~~CONFIDENTIAL~~

TM 32-220

TECHNICAL MANUAL

BASIC CRYPTANALYTICS (U)

This material contains information affecting the National Defense of the United States within the meaning of the Espionage Laws, Title 18, U.S.C., Sections 793 and 794, the transmission or revelation of which in any manner to an unauthorized person is prohibited by law.

HEADQUARTERS, DEPARTMENT OF THE ARMY

AUGUST 1970

~~CONFIDENTIAL~~

GROUP 1
Excluded From Automatic
Downgrading and Declassification

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

Serial: J9069-92
4 March 1993

Mr. William J. Neill
1231 Crescendo Drive
Roseville, CA 95678

Dear Mr. Neill:

This responds to your Freedom of Information Act (FOIA) request of 16 January 1992 for an original copy of TM 11-485 and the declassification and release of TM 32-220. Your request has been processed under the FOIA, and although we do not have an original of TM 11-485, a copy of that document is enclosed along with a copy of TM 32-220. Certain information, however, has been deleted from TM 32-220.

Some of the information deleted from the TM 32-220 was found to be currently and properly classified in accordance with Executive Order 12356. This information meets the criteria for classification as set forth in subparagraphs (a)(2), (a)(4) and (a)(8) of section 1.3 and remains classified CONFIDENTIAL as provided in section 1.1 of Executive Order 12356. The information is classified because its disclosure could reasonably be expected to cause damage to the national security. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. section 552(b)(1)).

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in TM 32-220. Accordingly, those portions are also exempt from disclosure pursuant to the third exemption of the FOIA which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 403(d)(3); and Section 6, Public Law 86-36 (50 U.S. Code 402 note).

Since these deletions may be construed as a partial denial of your request, you are hereby advised of this Agency's appeal procedures. Any person denied access to information may, within 60 days after notification of the denial, file an appeal to the NSA/CSS Freedom of Information Act Appeal Authority. The appeal shall be in writing addressed to the NSA/CSS FOIA Appeal Authority, National Security Agency, Fort George G. Meade, MD 20755-6000. The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes release of the information is required. The NSA/CSS Appeal Authority will respond to the appeal within 20 working days after receipt.

On 5 February 1993, you spoke to a member of my staff who advised you that we anticipated costs of $100.00 to process your request, and you agreed to pay that amount. The actual fees incurred total $96.80. The search for records responsive to your request took 4 hours, and 412 pages are being released to you. You are allowed 2 hours of search and the duplication of 100 pages at no cost pursuant to 5 U.S.C. 552 (4)(A)(iv)(II). The remaining charges are assessed in accordance with DoD Regulation 5400.7-R, which assesses $25.00 per hour for search and $.15 per page for duplication. A bill for the total due will be sent to you under separate cover.

Sincerely,

Linda S. Miller
for MICHAEL A. SMITH
Director of Policy

Encls:
a/s

~~CONFIDENTIAL~~

TM 32-220

TECHNICAL MANUAL

BASIC CRYPTANALYTICS (U)

This material contains information affecting the National Defense of the United States within the meaning of the Espionage Laws, Title 18, U.S.C., Sections 793 and 794, the transmission or revelation of which in any manner to an unauthorized person is prohibited by law.

HEADQUARTERS, DEPARTMENT OF THE ARMY

AUGUST 1970

~~CONFIDENTIAL~~

GROUP 1
Excluded From Automatic
Downgrading and Declassification

*TM 32-220

TECHNICAL MANUAL
No. 32-220

HEADQUARTERS
DEPARTMENT OF THE ARMY
WASHINGTON, D.C., *20 August 1970*

BASIC CRYPTANALYTICS (U)

*This manual supersedes TM 32-220, 5 April 1950.

ILLUSTRATIONS (U)

LIST OF TABLES (U)

PART ONE (C)
INTRODUCTION TO CRYPTANALYTICS

CHAPTER 1 (C)
INTRODUCTION

Section I. (U) GENERAL

1-1. (U) Purpose

This manual presents the basic principles of cryptanalytics and its relation to cryptography. Cryptography deals with the art of secret communications while cryptanalytics treats of their solution by those who do not have access to the plaintext communications. The manual is primarily a training text, designed to promote an understanding of the practical application of cryptanalytics to provide the student with the knowledge of the techniques and methods used in the cryptanalysis of common codes and ciphers.

1-2. (U) Scope

This manual has been organized into six parts. The first part deals with the fundamentals necessary to study the remaining five parts. In each subsequent part, the manual covers a type cryptographic system, its practical application, and the appropriate analysis methods. The material presented in each part represents a more complex cryptographic system than that preceding it and, therefore, requires a more detailed study. All parts except the last two are thorough in the scope of their study. The last two, due to the extreme difficulty of the subject matter, have been limited to an introductory study only. Note at the outset that each system presented has many possible variations. All the variants have not been included. The contents have been deliberately limited to those systems, methods, and techniques which offer the broadest possible application, and which, when mastered, will provide the greatest degree of understanding of the subject area.

1-3. (U) Changes or Revisions

Users of this publication are encouraged to submit recommended changes and comments to improve the publication. Comments should be keyed to the specific page, paragraph, and line of the text in which the change is recommended. Reasons will be provided for each comment to insure understanding and complete evaluation. Comments should be prepared using DA Form 2028 (Recommended Changes to Publications) and forwarded direct to the Commanding General, United States Army Security Agency, ATTN: IAFOR-RL, Arlington Hall Station, Arlington, Va. 22212.

1-4. (U) Developments

Cryptology, the branch of knowledge which treats of the principles of cryptography and cryptanalytics, is not a static art or science. Constant change, both in the systems used and in techniques of analysis, is its hallmark. What is regarded today as unnecessary, or as wholly impractical, may become possible and absolutely necessary tomorrow. The development of cryptology has a long history. Basic systems of cryptography and of cryptanalysis developed in the past, although relatively simple by today's standards, still are applicable. In some cases these same systems and techniques, or variations of them, are still in use today. These systems vary, from the relatively simple hand-generated ciphers and codes to the highly sophisticated and complex machine systems. Accordingly, the methods and techniques of their solution also vary from rather simple methods to highly involved studies requiring a great deal of time and skill. However, the basic techniques used in the solution of the less complex systems form the basis for the study and the analysis of the more complex systems. For this reason the following text progresses from the simple through the more complex.

Section II. (C) TERMINOLOGY

1–5. (U) Basic Definitions

In cryptology, as in any other art or science, a host of words and phrases exist, each having special meanings within the context of the subject area. These meanings may or may not relate to the common usage of the word or phrase. As forms of verbal shorthand, it is invaluable to state exactly what is meant with the minimum use of time and words. For the purpose of this manual it is necessary to understand some of the common definitions at the outset. Other definitions will be introduced and explained in detail as the subject is presented. For a complete list of definitions the NSA Basic Cryptologic Glossary, 1965, may be consulted.

a. Signal Communications. Any means of transmitting messages other than by direct conversation or mail. A commander uses signal communications to receive reports of hostile dispositions and activities, to receive reports of the progress and needs of subordinate and neighboring friendly units, to send orders to subordinate units, to receive orders from superior units, and to send to higher and adjacent units information necessary for the coordinated action of the whole command.

b. Means of Signal Communications. A medium, including equipment, used by a command for transmitting and receiving messages. The most important are:

(1) Wire.
- (*a*) Telephone.
- (*b*) Telegraph.
- (*c*) Teletypewriter.
- (*d*) Facsimile.

(2) Radio.
- (*a*) Radiotelephone.
- (*b*) Radiotelegraph.
- (*c*) Radio teletypewriter.
- (*d*) Radio facsimile.

c. Message Center. A communications facility, subordinate to and usually located within or nearby a command, having one or more of the above means of communications available. It serves as a point of origin, destination, and relay for messages within the command. Here messages are processed prior to transmission and after reception.

d. Writer. The person who actually prepares and signs the message. The writer may be the originator or his officially designated representative.

e. Originator. The command by whose authority a message is sent. A commander may delegate this authority to one or more subordinates, who originate messages as required in the commander's name.

f. Addressee. The office, headquarters, activity or individual to whom a message is directed by the originator.

g. Externals. Those elements appearing outside the body of the message placed on the message by the communications center for the purpose of routing. Examples of externals are callsigns, serial numbers, precedence indicators, times of file, and special routing instructions.

h. Message Text. That portion of a message which contains the communication. It may be in plaintext or in secret writing.

1–6. (~~C~~) Secret Communications

a. Intercommunications are any means susceptible to interpretation by one of the five senses. Those most commonly used are visual or auditory. Aside from the use of simple visual and auditory signals for intercommunication over relatively short distances, military communications depend upon the act of writing (messages), speaking (telephone and radiotelephone), and projecting a picture or illustration (TV and facsimile). Of these methods, our interest lies primarily with the first, and the latter two only insofar as the transmission of messages are concerned.

b. The origins and use of secret communications are unknown, but probably began in some form with man's ability to communicate. They originated in the earliest days of organized warfare and diplomatic relations where they were soon recognized as a necessity. The earliest reliable reference to the use of secret writing occurred in 900 A.D. when Plutarch reported the ancient Spartans as using a device called Scytale, a method of secret writing in which a narrow strip of parchment was wound round a wooden baton, the message written across the adjoining edges. History records the subsequent growth of the art, but the real beginnings of systematic modern cryptology is traced back to the early 13th century. During this period the science was developed and employed extensively in the diplomatic relations of the Papal States. From this period forward, its growth, although sporadic, has been constant. Systems of greater complexity have been introduced followed by the development of methods and techniques for their analysis.

c. Speech can be secured by electronic devices that distort, substitute, or change the electrical current of telephone and radiotelephone, rendering it unintelligible to all but those provided with similar electronic devices properly arranged for the purpose. The same thing is true in the case of facsimile transmission (the transmission of charts, maps, illustrations, messages, etc.), and simple forms of enciphered television transmissions currently used in conjunction with "pay-TV." In both instances, lacking the proper device to decipher the signal, one would be unable to receive intelligible information.

d. Writing can be secured by two general methods. It can be made invisible or unintelligible.

(1) Invisible writing is done with certain chemicals called invisible, sympathetic, or secret inks which are invisible to the naked eye. In order to make the writing visible, the message is first processed with a suitable reagent which in effect develops the message. Invisible writing is also produced by reducing the writing to microscopic size. This method requires special photographic equipment to reduce the writing, and later enlarge the writing to make it visible.

(2) Although invisible writing finds some application in military communications, by far the most important means of producing secret writing is by a cryptographic process, a far simpler and more effective method. The writing remains visible but its secrecy is protected by its unintelligibility.

1-7. ~~(C)~~ Plaintext and Encrypted Text

a. Visible writing which is intelligible, i.e. conveys an understandable or sensible meaning (in the language in which it was written) and does not intend to convey a hidden meaning is plaintext. A message in plaintext is termed a plaintext message, a cleartext message, or sometimes a message in the clear.

b. Visible writing which conveys no intelligible meaning in any recognized language is in encrypted text, and such writing is a cryptogram.

c. Visible writing may be intelligible, but the obvious meaning it conveys may not be the real meaning intended. Secret communications of this sort are impractical for field military use but are often encountered in espionage and counterespionage activities.

1-8. ~~(C)~~ Plain and Cipher Alphabets

a. A plain alphabet is a series of symbols constituting the speech sounds of a language, arranged in their normal sequence. A cipher alphabet is one in which the same elementary speech sounds are represented by symbols other than those used in the normal alphabet. A cipher alphabet is composed of two components, the plain component represented by a plain alphabet, and a cipher component, represented by a disarranged alphabetic sequence.

b. Basically the method of using a cipher alphabet involves finding a plaintext value in the plain component and then finding the cipher value which is substituted for it in the cipher component.

Section III. ~~(C)~~ CRYPTOGRAPHIC SYSTEMS

1-9. ~~(C)~~ Codes, Ciphers, and Enciphered Codes

A general cryptographic system is the sum total of all the basic invariable rules followed in converting the plaintext of a message to ciphertext, producing a cryptogram, and the reverse, drawn up between correspondents or furnished them by higher authority. All cryptographic systems can be classed in two basic systems, or one variation, according to the treatment the plaintext undergoes in its transformation to a cryptogram. The two basic systems are cipher systems and code systems.

a. In ciphers or cipher systems, cryptograms are produced by applying the cryptographic treatment (process whereby plain writing is changed to secret writing) to individual letters, or groups of individual letters, of the plaintext message. A cryptogram produced by this method is in cipher, and is called a cipher message or a cipher. The operation is called enciphering. Changing the cipher into plaintext is called deciphering. A cipher message may be produced by several processes. A cipher table, cipher device, or cipher machine may be used for the encipherment of a message. Any of the cipher systems involving only the use of paper and pencil are known as cipher tables. A cipher device is an apparatus or a simple machine for literal encipherment and decipherment, usually manually operated. A cipher machine is a more complex electromechanical device serving the same purpose but usually requiring an outside power source. It may be operated "off line" whereby a cryptogram is produced prior to transmission, or it may be operated "on line" whereby the process of encipherment-transmission-decipherment occurs simultaneously between correspondents.

b. In codes, or code systems, cryptograms are produced by applying the cryptographic treatment to entire words, phrases, or sentences of the plaintext message. A characteristic of codes is that the cryptographic element used as replacement of the plaintext elements is normally of constant length as opposed to the replaced plaintext element which varies in length. A cryptogram produced by means of a code system is called a code message, or more simply a code, the text being referred to as code text. Producing a cryptogram is called encoding. Breaking the code back into plaintext is called decoding. A code message may be produced through the use of several types of code systems. Common systems include code books, code charts, and code tables. All code systems are manually operated and are composed of listings of plaintext and corresponding cipher values. The foregoing classification of code systems is based on the manner in which the values are listed.

c. The variant class of systems previously mentioned are not encountered as often as the basic types, although still important. This class contains such quasi-systems as enciphered codes, systems where code groups are enciphered; encoded ciphers, systems wherein ciphertext is encoded; and superencipherment, systems wherein ciphertext is again enciphered in another cipher system different from that used to produce the original ciphertext. The complexity of these processes, the amount of time needed, the possibility of inducing errors, and the problematic increase of security created by these methods are factors which limit their use in most military communications.

1–10. (~~C~~) Discriminants (System Indicators) and Specific Keys

Cryptographic systems, regardless of type, normally include two elements, not part of the plaintext, to facilitate processing and handling. The elements may be a single number, a single letter, a group of letters or numbers, or a word or a phrase. The elements usually correspond in structure and external appearance to the cipher or code text in order to conceal them. However, to aid in their recognition by communications center personnel, they usually occur in a specific position within the text of a message. These two elements are the discriminant, or the system indicator, and the specific key.

a. The discriminant indicates the specific cryptographic system used to produce the cryptogram.

b. The specific key, used in conjunction with the discriminant, indicates "how" the cryptographic system was used. It may indicate the starting point in code books and manual cipher systems, the "set up" for a cipher machine or device, the manner in which the machine is prepared for the encipherment and decipherment of a specific message. The specific key is changed frequently, after a given number of characters have been enciphered, at the end of a time period, or after a message. Exact periods of usage of a given key may be dictated by higher authority or by agreement among correspondents. Derivation of specific keys involves the use of specially prepared tables, documents, or books.

1–11. (~~C~~) Ciphers, Transposition and Substitution

The two distinct types of cipher treatment, applied to plaintext to covert it to secret text, yield two different classes of cryptograms. In the first, transposition, the elements or units of the plaintext retain their original identity and only undergo a change in their relative position. In the second, substitution, a cipher element of varying length is substituted for a plaintext value, usually of the same length. Moreover all cipher elements within a given system are normally of the same length, though there are a few exceptions.

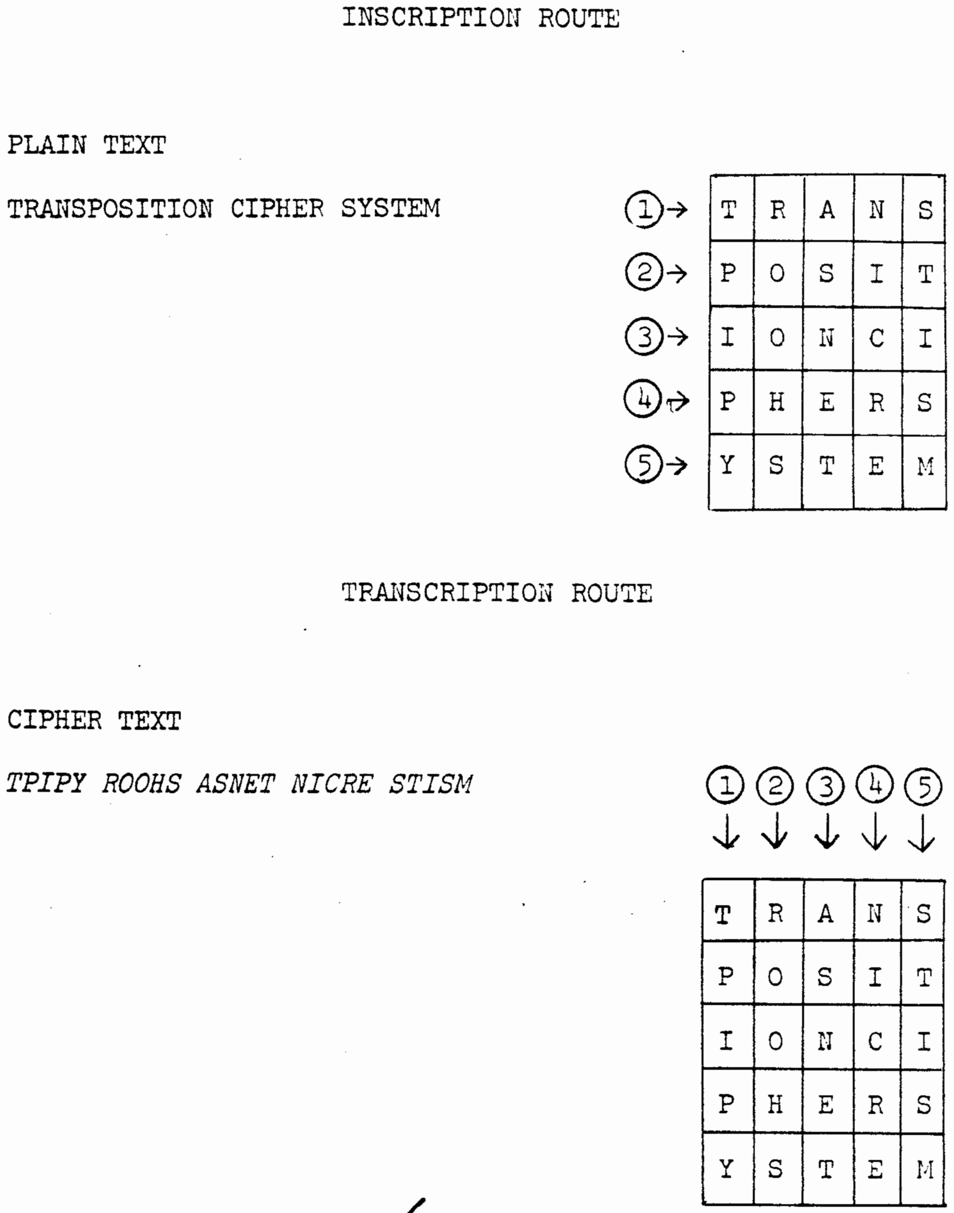
a. A simple form of a transposition cipher may be observed in figure 1–1. As the system's name implies, ciphertext is generated simply by the disarrangement of the letters of the plaintext. But note, this disarrangement is not a random process, rather it follows specific rules. In this case the plaintext is inscribed in the cells of a matrix as one would normally write, then extracted by columns from left to right and put into groups of five letters to form ciphertext.

b. The second class of treatment by which a written plaintext message can be converted to secret text is by substitution. In substitution systems, the elements of the plaintext retain their original relative positions to one another, but are replaced by other elements which have different values or meanings, with the result that the original text becomes unintelligible. A simple example of such a substitution system is one used by General Clinton during the American Revolution:

A	B	C	D	E	F	G	H	IJ	K	L	M	N	O	P	Q	R	S	T	UV	W	X	Y	Z
51	*52*	*53*	*54*	*55*	*60*	*61*	*62*	*63*	*64*	*65*	*66*	*67*	*68*	*69*	*70*	*71*	*72*	*73*	*74*	*75*	*76*	*77*	*78*

Using this system, a message was enciphered by substituting two numerical values for each literal value in the plaintext message. For example, the following message would be enciphered as shown below:

GEN	B	ARNOLD	AT	WEST	POINT
615567	*52*	*517167686554*	*5173*	*75557273*	*6968636773*



INSCRIPTION ROUTE

PLAIN TEXT

TRANSPOSITION CIPHER SYSTEM

①→	T	R	A	N	S
②→	P	O	S	I	T
③→	I	O	N	C	I
④→	P	H	E	R	S
⑤→	Y	S	T	E	M

TRANSCRIPTION ROUTE

CIPHER TEXT

TPIPY ROOHS ASNET NICRE STISM

①↓	②↓	③↓	④↓	⑤↓
T	R	A	N	S
P	O	S	I	T
I	O	N	C	I
P	H	E	R	S
Y	S	T	E	M

Figure 1-1 (~~C~~). *Transposition systems* (*U*).

1-12. (~~C~~) Divisions of Cipher Systems

Each of the two classes of cipher systems, transposition and substitution, are further subdivided based on the number of characters composing the textual elements of units undergoing treatment, and the number of cipher elements replacing the plaintext elements. A sharp line of demarcation cannot be drawn between systems in every case, for occasionally a given system may combine methods related to two differing systems. The descriptions given in the following paragraphs are for convenience in presenting the systems. Approved definitions may be found in NSA Basic Cryptologic Glossary.

a. Transposition System. A cryptographic system in which the elements of the plaintext (individual letters, groups of letters, syllables, words, phrases, sentences, or code groups or their components), undergo some change in their relative position without a change in their identity. The three major classes of transposition systems are:

(1) *Single transposition.* Those systems wherein the plaintext undergoes only one transposition.

(2) *Polyphase transposition.* Transposition systems wherein the plaintext undergoes two or more transpositions. Of this type transposition, double transposition is most common.

(3) *Grille transposition.* A transposition system involving the use of two devices; a matrix of given size, and a grille, a thin material in which perforations have been made. Normally the plaintext message is

inscribed in the cells of the matrix, one word or letter per cell, in normal left-to-right, top-to-bottom order. The grille is then placed over the matrix, the perforations exposing portions of the plaintext. These are extracted and recorded and the grille is revolved. Again more plaintext is exposed. This process is continued until all the plaintext has been extracted from the matrix, the process transposing the relative order of the words or letters of the plaintext.

b. Substitution System. A cryptographic system which involves the replacement of the plaintext value by one or more ciphertext values with no change between their relative order of occurrence. Both or either of the plaintext and ciphertext values may be of equal or different length and form the basis of the further subclassification of the system.

(1) *Monoalphabetic substitution.* A system of substitution involving a single fixed cipher sequence from which a cipher equivalent of one or more elements is drawn in all cases to represent one plaintext unit of equal length.

(*a*) *Monographic substitution.* Monoalphabetic substitution system in which the plaintext units replaced are always single units, letters, or numbers; but in which the length of the cipher unit may vary.

1. Uniliteral substitution. Monographic substitution in which single letters or numbers of the plaintext are replaced by single cipher equivalents.

2. Multiliteral substitution. Monographic substitution in which single letters of the plaintext are replaced by cipher units of two or more characters.

(*b*) *Polygraphic substitution.* Substitution systems in which the plaintext units treated are groupings of more than one element of regular length, replaced by cipher elements of similar length.

(2) *Polyalphabetic substitution.* A system of substitution in which successive plaintext elements of a message are replaced by cipher elements drawn from a succession of different cipher alphabets.

(*a*) *Periodic polyalphabetic substitution.* A method of polyalphabetic substitution in which a series of cipher alphabets are used cyclically, also called repeating key.

(*b*) *Aperiodic polyalphabetic substitution.* A method of polyalphabetic substitution in which the method of substitution results in the suppression of cyclical phenomena in the cryptographic text.

c. Application of Systems. Transposition systems, particularly the polyphase systems, excepting double transposition, although offering a greater degree of security than some substitution systems, find little application in military communications. Complexity of operation, time required for their use, the limitations on message length, and the practical difficulties encountered in producing and distributing the material required for their use, all serve to limit their effective use.

1–13. ~~(C)~~ Code System

a. Code systems differ from cipher systems in that the substitution of values does not involve a one-to-one ratio. A group of arbitrary length, usually three to five letters, figures, or combinations, is substituted for either letters, syllables, phrases, or sentences.

b. The mechanics of a code system are such that usually some method of listing the code groups and their associated plaintext values is required. A detailed explanation of code systems and their classification is given in Part Six.

CHAPTER 2 (C)

SECURITY OF CRYPTOGRAPHIC SYSTEMS

Section I. (C) GENERAL

2–1. ~~(C)~~ Practical Requirement of a Military Cryptographic System

Cryptographic systems must meet certain fundamental requirements of a practical nature for use in military communications. In order of importance, these requirements are: reliability, security, rapidity, flexibility, and applicability.

a. Reliability means that the cryptographic system, whether a code book, a cipher machine or device, or cipher table, will be on hand and in good working order, available for instant use. When used, it can be operative as long as needed. It also means that the cryptogram produced can be decrypted quickly, accurately, and without uncertainty as to meaning. Simplicity is implied in reliability; usually, the more simple the system the more reliable it is.

b. The needs for both security and rapidity in a military cryptographic system are often conflicting requirements. Security is the total protection afforded by a sound cryptographic system; rapidity is the speed of operation of the system. Maximum security at all times is the goal, but cannot always be met. Often a compromise between these differing requirements must be effected. In messages exchanged among higher headquarters, some speed may be sacrificed to attain greater security. Among lower headquarters and between units conducting active operations, security must often give way to the greater need for speed in communications.

c. Concerning flexibility, a cryptographic system should have as wide an application as possible. A system specifically adapted to a particular usage cannot serve as an all-purpose system. A code book designed for field operations can hardly serve the needs of a high headquarters, nor can a system designed for it serve the needs of small combat units.

d. The last factor concerns general application of the system.

(1) Cryptograms produced by the system must be in a form suitable for transmission by means available to the using unit.

(2) The system, especially that used at lower echelons, should be relatively simple in its operation and should be operable under different field conditions.

(3) The system must be such that errors in the cryptographic process can be either corrected easily and quickly by the operator or be of no consequence in the decipherment process.

(4) The system, if a device or a machine, must be light in weight, rugged in construction, and simple to operate, requiring the use of only one operator.

e. In order to satisfy the conflicting requirements posed by all the foregoing factors, several cryptographic systems are available to each unit or headquarters. This procedure permits the fulfillment by each unit of its own immediate needs for a system oriented to its mission, plus it provides a secure means of communications between adjacent units and higher and lower headquarters.

2–2. ~~(C)~~ Security Requirements of a Military Cryptographic System

a. The ideal cryptographic system for military purposes is a single all-purpose system which is practical for use by the highest headquarters and by the smallest troop unit in the combat area, and which also presents such a great degree of cryptographic security that, no matter how much traffic became available all in the same key, the cryptograms composing this traffic would resist solution indefinitely. Such an ideal system, however, is beyond the realms of possibility so far as present methods of cryptographic communications are concerned. For this reason, and those discussed in the preceding paragraph, a multiplicity of systems must be employed, each designed for a specific purpose, at a given level of security.

b. The best that can be expected for each system is that the degree of security be great enough to delay solutions for such a length of time that, when the solutions are finally reached, the information obtained by the enemy has lost all its "short term," immediate, or operational value, and much of its "long term," research or historical value.

2-3. (~~C~~) Exploitation of Cryptographic Systems

In theory, all cryptographic systems are vulnerable to analysis and exploitation, given sufficient time, organization, skill, and volume of traffic. Analysis can be accomplished even if the general system and the specific keys are unknown at the start. In actual practice, however, the security of a. cryptographic system, and therefore its degree of vulnerability to analysis, are correlated directly to:

a. The cryptographic soundness of the system. The degree of security of any system depends on this factor, and in turn determines the resistance to analysis which the system offers. A sound system, in the sense that the cryptographic process provides a maximum of variant values with little or no characteristic patterns subject to analytic attack, will resist analysis longer than a weak cryptographic system, all other factors being equal.

b. The adequacy and soundness of the operating instructions pertaining to a system and the extent to which the users follow these instructions. Security of a good cryptographic system can be almost completely destroyed by the users who, through carelessness or ignorance, fail to follow prescribed methods of operation or who change operating procedures in the mistaken belief that they are improving the system.

c. The volume of cryptographic text available for study. As a rule, the greater the volume of text, the more easily and speedily a system can be solved. A single cryptogram in a given system may present an almost impossible task to the cryptanalyst, but if many cryptograms are available in the same system in the same or in closely related specific keys, the solution may be reached in a very short time.

d. The number, skill, efficiency, and organization of personnel and units assigned to the analysis of communications. This factor plays a direct part in the analysis and exploitation of a system. The simplest system may resist cryptanalytic attack if the analysts are unskilled. Even if a system is solved, the information may not be fully exploited if it lacks proper organization for this purpose.

e. The amount and character of collateral information and intelligence available. Cryptograms between correspondents about whom no information is available may pose a very difficult problem. If, however, a certain amount of information is known, a solution may be readily obtained. The more information at hand concerning a given cryptogram (including particulars of the basic system, as well as knowledge of its possible contents, i.e. proper names, stereotyped beginnings and endings, and events or subjects referenced in the message), the easier the solution.

Section II. (C) THE CRYPTANALYTIC ATTACK

2-4. (~~C~~) Communications Intelligence Operations

Communications Intelligence (COMINT) operations study enemy communications for the purpose of obtaining information and intelligence. COMINT includes the collecting, processing, evaluating, and reporting of intelligence derived from raw data. COMINT attempts to answer three questions concerning enemy communications: Who, Where, and What; who are the originators and addressees, where are they located, and what do the messages say.

a. The two steps in the series of activities whose end objective is to answer these questions are the collection of raw data, and the study and analysis of this data.

(1) *Collection.*

✓(*a*) *Intercept operations.* Intercept operations include all activities and functions directly related to the intercepting and recording of enemy radio communications. Major functions which are a part of intercept operations are the mission assignment and control, the allocation of equipment and facilities; and the assignment and direction of personnel. As an adjunct to intercept operations, providing both support to the intercept effort and a source of information to their own right, two special collection techniques are available.

(*b*) *Radio fingerprinting* (*RFP*). RFP is the technique of identifying radio transmitters by recording on film, and later by analyzing the power and frequency variations of an on-off keyed Continuous Wave (CW) emission.

(*c*) *Radio direction finding* (*RDF*). RDF is the technique of determining the azimuth (bearing) of a transmitter from the point of interception. By establishing the bearing on a transmitter from several different points, it is possible to fix the geographic location of the emitter.

(2) *Study and analysis.* The second step in COMINT operations is the study and analysis of all data provided by the preceding intercept activities. The preliminary processing of this data normally occurs in a traffic analysis section. Traffic analysis is the study of the externals of signal communications by all means short of the cryptanalysis of the message text. Traffic analysis reconstructs radio communications networks by noting volume, direction, and routing of messages;

correlating transmission frequencies and schedules used among a network's various stations and nets; determining the location of radio stations by evaluating the results of radio direction finding; identifying radio station association by evaluating the results of radio fingerprinting; recovering the system or systems of generating, assigning, and changing radio callsigns; and studying all items that constitute messages originated by operators and exchanged among themselves on a radio net.

(*a*) Information gleaned by the traffic analyst serves two general purposes. First, it provides a basis for further interception of the enemy's communications. Second, it produces information that is of intelligence value in itself, and also of great value to the cryptanalyst in his attack upon the message text. Traffic analysis is able not only to ascertain the geographic locations and dispositions of troop units and headquarters, but also sometimes can predict, with varying degrees of reliability, the areas and extent of immediately pending or future activities of the enemy. This can be done without reading the text of the intercepted message. Specifically, enemy plans and operations may be revealed by:

1. Movement, appearance, and disappearance of radio stations.

2. Changes in volume and routing of messages.

3. Characteristics of messages and any changes thereto.

4. Redeployment and changes in communications networks.

5. Allusion to operations in radio operator chatter.

(*b*) On the basis of the foregoing studies it is possible to accurately answer the first two questions, Who and Where, and, in some cases find a partial answer to the third question, What. However, the final answer to the third question can only be found with certainty in the message text itself. This is a task of the cryptanalyst.

b. Cryptanalysis is the process involved in converting encrypted messages into plaintext without initial knowledge of the system or key employed in the encryption process. The solution of practically every cryptogram under these conditions involves four fundamental operations:

(1) The determination of the language used in the plaintext version.

(2) The determination of the general system of cryptography used.

(3) The reconstruction of the specific key in the case of a cipher system; or the reconstruction, partial or complete, of the code book, in the case of a code system, or both in the case of enciphered codes.

(4) The reconstruction or establishment of the plaintext.

2–5. (C) Determination of Language

a. The determination of the language employed seldom comes into question where studies are made of the cryptograms of an organized enemy. During conventional war when the enemy is known, the language employed in messages will most likely be in the enemy's native tongue. Where this is not the case, i.e. when cryptograms of unknown origin must be studied, the cryptanalyst looks for indications of the language in the cryptogram itself. Addresses, signatures, and other data in plaintext in the preamble, in the body, or in the postamble of the cryptogram may reveal the language used, as well as those external elements associated with the transmission of the message.

b. In special cases, the nature and composition of the cryptographic text may reveal the language used. For example, if the letters K and W are absent, the language may be Spanish or Portuguese, as these letters are used only to spell foreign words. The presence of special characters in the text may also indicate the language where the alphabet exceeds the Morse code equivalents. For example, KATA KANA, a Japenese syllabic writing having 72 syllabic sounds, requires 48 Morse code characters for radio transmission, creating a form of Morse code called Kana Morse code.

c. Knowledge of the language used in a given cryptogram is important in two respects. First, the frequency of occurrence and distinctive pecularities of combining individual letters, vowels, consonants, digraphs, and trigraphs, varies with different alphabetic based languages, but individually are rather constant, a feature that becomes the basis for analysis. Second, final solution and translation of the message depends upon the ability to make valid assumptions of word usage.

d. In some cases it is possible to perform certain steps before the language of the cryptogram is known. Frequency studies may be made and certain analytic processes begun without this knowledge. Final solution, however, usually depends on the analyst knowing valid combinations of letters, syllables, and some common military terminology in that language, or having available a translator who can aid him in making necessary assumptions based upon his special knowledge of the characteristics of the language in question.

2–6. (~~C~~) Isolation of the General System

a. Determining the general system in which a given cryptogram has been enciphered is the most difficult step in its solution, except for some of the simpler basic systems. The solution of every cryptogram involving a form of substitution depends upon its reduction to monoalphabetic terms. This is also true of combined substitution-transposition ciphers and enciphered codes. In the case of transposition ciphers, recognition of the system, followed by determination of the method of transposition is required.

b. To achieve these ends, however, a degree of prior knowledge is required; knowledge of how a given cryptographic system operates, its characteristics, and its limitations. The analyst must be able to identify the cryptogram under study as one of the basic systems. The knowledge of cryptographic systems comes from training and experience; identification of a cryptographic system is a matter of analytic determination.

c. Cryptanalysis offers few tests that may be applied to a cryptogram to determine positively to which class it belongs, particularly in the case of two systems yielding externally similar results. However, the analyst, if he can identify a system to a general class, can usually determine by trial and error the exact class to which it belongs. Sooner or later most systems can be identified, either because of blunders or carelessness on the part of the cryptographic clerks, or because the accumulation of a volume of traffic makes possible its identification by cryptanalytic and statistical studies. In the case of isolated cryptograms, identification of a system is sometimes a matter of a shrewd guess.

2–7. ~~(C)~~ Reconstruction of the Specific Key

Most cryptographic systems use a specific key to guide, control, or modify the processing steps of the general system. Once the system is known, the next step in the solution of a cryptogram is to determine the specific key, if used, employed to produce the cryptogram. This determination may not be required in complete detail; it may be sufficient to know the number of alphabets involved in a substitution system, or the number of columns in a transposition system, or that a code system is one-part. In other cases, a complete recovery may be desirable for use as a clue to the operation of an unsolved related system. In many cases, the reconstruction of the specific key and the recovery of the plaintext may be simultaneous operations. The primary requirement for specific key recovery in most cases is to provide the basis for the rapid solution of cryptograms enciphered in the system using the same key or similar key.

2–8. (C) Recovery of the Plaintext

a. In the case of substitution ciphers, this process involves establishing equivalency between specific letters of the ciphertext and the plaintext, letter by letter, pair by pair, etc., depending upon the type of substitution cipher involved. In the case of transposition ciphers, the process involves rearranging the elements of the ciphertext, according to the peculiarities of the system, until the plaintext has been recovered. In the case of codes, the process is one of determining the meaning of each code group.

b. The above processes for any system are not sequential. The identification of plaintext values comes at very irregular intervals. At first, only one or two values are recovered and appear scattered throughout the ciphertext. These letters form the "skeletons" of words, upon which further work, continuing the reconstruction process and assuming words to be tested, recovers the complete text. The recovery of the plaintext is a long tedious process involving a great deal of work and analysis.

2–9. ~~(C)~~ Steps of Cryptanalysis

Any scheme of analysis is based upon successive elimination of alternatives, therefore the cryptanalyst can only progress as far as the extent of his own knowledge of the possible alternatives. Additionally, the general procedures and techniques of analysis will differ from one system to another due to the characteristics of each system that lends itself to analytic attack. For these reasons it is difficult to specify which exact steps will be followed in all cases. The most important steps of practical, operational cryptanalysis are listed below in outline form. These steps appear in the order in which they are usually followed, but in particular cases, some of these steps may be interchanged or omitted entirely.

a. The study of the characteristics of the message text.

b. The study of any available collateral information.

c. The search for and study of indicators in the message text.

d. The determination of the type cryptographic system used.

e. The separation and classification of messages into common groups determined by general system or related specific keys.

f. The search for repetition of groups, symbols within and between messages of the same system.

g. The study of the beginnings and endings of messages for stereotypes.

h. The preparation of statistical counts of message elements.

i. The reduction of the encrypted text to the simplest terms.

j. The test for probable words, stereotypes, and isologs.

k. The recovery of the plaintext.

Section III. ~~(C)~~ ANALYTIC AIDS

2-10. ~~(C)~~ Introduction

a. Several different statistical tests, tables, and many different data listings, are available to the analyst as analytic aids. The tests are generally used for the initial identification of a system, enabling the analyst to identify a system to its particular class, substitution or transposition, and in some cases allowing the determination of type, monoalphabetic or nonmonoalphabetic substitution. However, the analyst should understand at the outset that the results given by these tests are not always absolutely reliable. In certain cases, the inherent characteristics of the ciphertext may be such that the test results are misleading if not totally false. The significance is that the analyst should not accept at face value the results of one test. Rather, identification should be based on several factors.

b. In the following paragraphs, the more common and immediately useful tests are introduced and explained. In subsequent chapters where the tests have specific application, they will again be explained in terms of each case. Also in the same areas, other tests which serve a purpose only in a given set of circumstances will be explained and the techniques of their application discussed.

c. The lists of data used by the analyst in the analysis of a cryptogram, and which have general application in this context only are contained in the appendixes. As they become applicable they will be discussed and their use illustrated.

2-11. ~~(C)~~ Uniliteral Frequency Distribution

a. The individual letters of any alphabetic-based language, when used in intelligible text, occur with greatly varying frequency. If, for example, a tabulation is made of the occurrence of the individual letters in the preceding sentence, shown in figure 2-1, the variation in frequency is strikingly demonstrated.

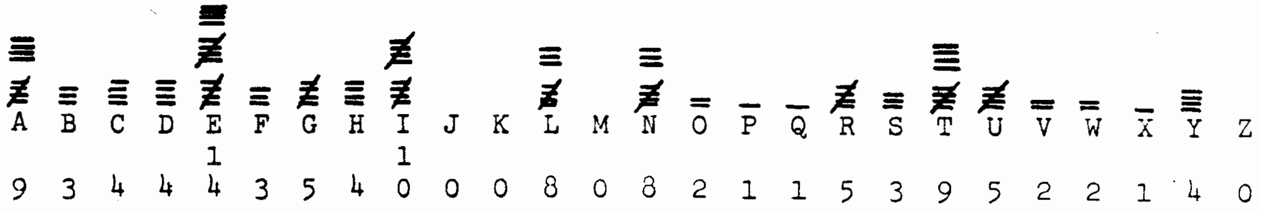


Figure 2-1 (U). Frequency tabulation 1 (U).

If the letters of the second sentence in the preceding paragraph are tabulated as shown in figure 2-2, the following occurrence of individual letters will be found.

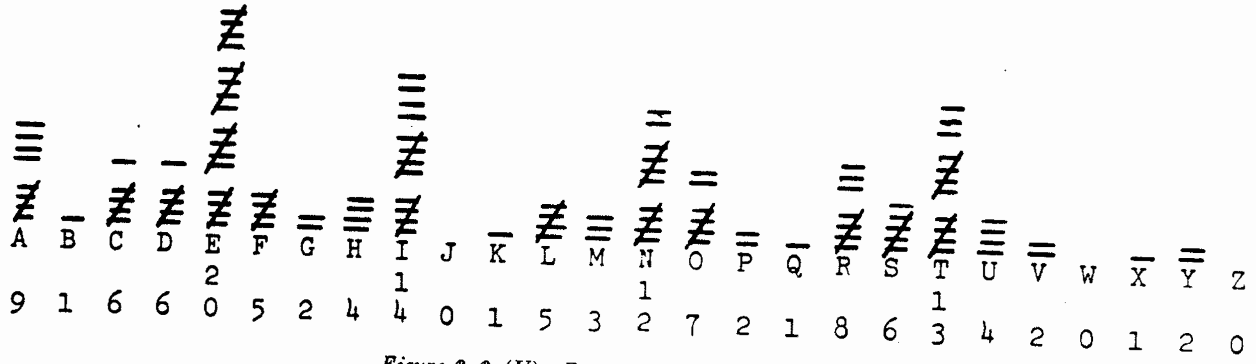


Figure 2-2 (U). Frequency tabulation 2 (U).

Although a difference in the frequency of occurrence of single letters, as reflected in peaks and troughs of each distribution, is observable in both distributions, very little difference is observed when the frequency of occurrences of given letters in both distributions is compared.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
9	3	4	4	14	3	5	4	10	0	0	8	0	8	2	1	1	5	3	9	5	2	2	1	4	0
9	1	6	6	20	5	2	4	14	0	1	5	3	12	7	2	1	8	6	13	4	2	0	1	2	0

In both of the distributions, note that certain letters occur much more frequently than others. The letters A, E, I, N, O, R, and T occur with the greatest frequency. The letters C, G, H, L, P, and S occur less often. The letters F, J, K, Q, V, X, and Z occur infrequently, or not at all. A degree of similarity between the two distributions is greater if the two texts used in the tabulation are longer. In fact, when two different texts of 1,000 or more letters are compared, the frequencies of occurrence of individual letters show only the slightest variation. Beyond that, the practical gain in accuracy does not warrant further increase in the amount of text.

b. The standard uniliteral frequency distribution for English telegraphic plaintext, derived from a tabulation of 50,000 letters, and reduced to a base of 1,000 which may be used as a tool in the analysis of cryptograms in the English language, is given in figure 2–3.

c. The preceding figures reveal several facts of great importance to the cryptanalyst and cryptographer.

(1) The standard uniliteral frequency distribution is quite irregular, having marked peaks and troughs, points of high and low frequency.

(2) The relative position within the standard uniliteral frequency distribution of the peaks and troughs is relatively fixed, determined by the sequence of the letters of the alphabet and their frequency of usage.

(3) The relative height and depth of the peaks and troughs are also relatively fixed, varying only slightly, and this is determined largely by the size of the sample tabulated.

(4) The most prominent crests are marked by the vowels A, E, I, and O, and the consonants N, R, S, and T. The deepest troughs are the consonants J, K, Q, X, and Z.

(5) The four vowels, A, E, I, and O, and the four consonants, N, R, S, and T, representing a combined frequency of 666 of 1,000 letters, approximately one-third of the alphabet, are used in writing two-thirds of normal plaintext messages.

d. Should an alphabet be so changed, or used in such a manner as to either change the sequence of the alphabetic values, or the frequency of usage of individual letters, the peaks and troughs would be changed accordingly, both in relative order and in total value. However, these changes, as will be shown in following paragraphs, can be directly related to the use of plaintext, as the true values must remain constant.

e. The data given above is based on English telegraphic text derived from government administrative messages. A similar distribution drawn from another source can be expected to show some

In Alphabetic Order

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
74	10	31	42	130	28	16	34	74	2	3	36	25	79	75	27	3	76	61	92	26	15	16	5	19	1

In Relative Order of Frequency

E	T	N	R	O	A	I	S	D	L	H	C	F	P	U	M	Y	G	W	V	B	X	Q	K	J	Z
130	92	79	76	75	74	74	61	42	36	34	31	28	27	26	25	19	16	16	15	10	5	3	3	2	1

	frequency	percent	percent in round numbers
Vowels:			
A E I O U Y	398	39.8	40
Consonants:			
High Freq D N R S T	350	35.0	35
Med Freq B C F G H L M P V W	238	23.8	24
Low Freq J K Q X Z	14	1.4	1
	1,000	100	100

Figure 2–3 (U). Standard uniliteral frequency distribution (U).

variation, the degree of variance being dictated by the source. For example, a distribution tabulated from messages pertaining to international shipping activities is markedly different, caused by the use of words peculiar to the business. Also, a distribution of a message in a foreign language is different, due to the nature of that language's alphabet, spelling, and word usage. However, for any given set of circumstances, which remain constant, a standard uniliteral frequency distribution can be derived. Variations may occur in each, because of volume available for tabulation or subject matter, but given sufficient volume, a normal distribution can be derived which forms a basis for the initial study of a cryptogram.

2–12. (~~C~~) Use of the Standard Uniliteral Frequency Distribution

Three facts can be determined by a comparison of the standard uniliteral frequency distribution to a uniliteral frequency distribution drawn from a cipher message composed of letters. First, whether the cipher belongs to the substitution or transposition class. Second, if substitution, whether the cipher is monoalphabetic or polyalphabetic. Third, if the cipher is monoalphabetic, whether the cipher component is a standard (direct or reversed) or a mixed sequence.

a. The difference between a transposition system and a substitution system is that in transposition, the plaintext has been rearranged, conventional values remaining the same in all cases. In substitution, the identities or values of the letters of the plaintext have been changed giving rise to the ciphertext of the message. Consequently in a transposition cipher, a count of the letters should correspond closely to the standard uniliteral frequency distribution, both in frequency of occurrence of the individual letters and in their spatial relationship, i.e. the location of the peaks and troughs.

For example, a frequency count of the following cryptograms produced by transposition ciphers appears in figure 2–4.

```
Cryptogram No. 1    HAMEA EROSY ATUTS DEEET QRDRU USYDP

Cryptogram No. 2    NPRIO IRXCC PMTIS SSLEL VCTEE
                    NEEAC OOSOO ANFSE OEOYI NSIAT
                    SSSYA HRARN LIRWN ATNNT OTIRN
                    TIODR

Cryptogram No. 3    VAAEI TZZMO HNEUE APDEF TOXIL
                    YNTRT OORTS PLORO ARRON ECTZL
                    REEEA RFAXI OUTER OTSEK JUPPE
                    ZSDII IOERE QOOSJ EOLSO SYEIO
                    WNILN ROFUF HTUSF TIFTS SVUOC
                    XWERE LERRA DE
```

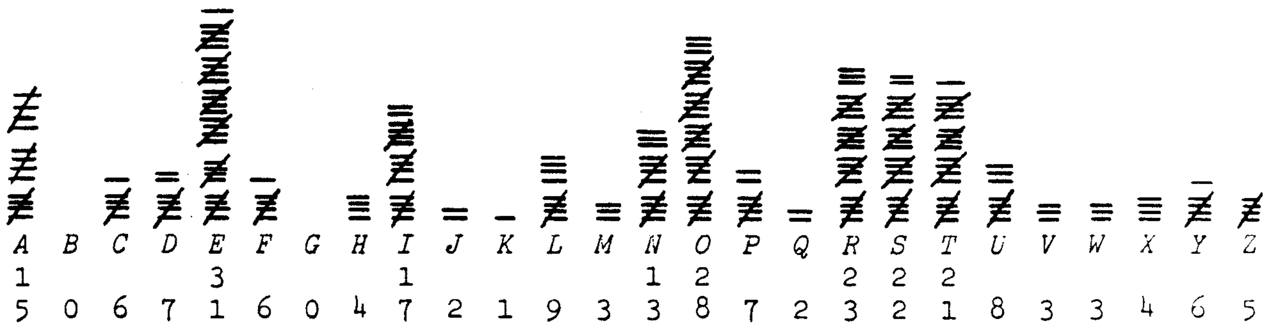


Figure 2–4 (~~C~~). *Uniliteral frequency distribution, transposition cipher* (*U*).

Converted to an equal base and compared to the standard uniliteral frequency distribution, it appears in figure 2-5. On this basis one assumed with a certain degree of security that the cipher in question is a transposition system rather than a substitution system.

b. In monoalphabetic substitution ciphers, the identities of the letters are changed on a one-to-one basis, i.e. Ap may become *Xc* and Xp may become *Ac*; Ap by definition cannot be represented by more than one cipher value. Since the identities of the letters are changed, the frequency of appearance of the letters are changed. The frequency of appearance of vowels, and high-, medium-, and low-frequency consonants are quite different from what they were in the plaintext. This may be seen in figure 2-6 depicting a message enciphered in a monoalphabetic substitution system, and its accompanying uniliteral frequency distribution.

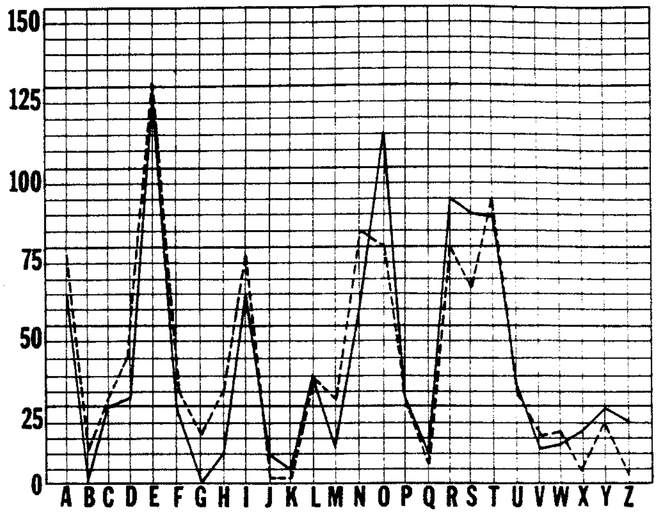


Figure 2-5 (U). Comparison, standard uniliteral frequency distribution and transposition ciphertext (U).

```
YHYGS UWNCP CNSCH KOUHA HAUCJ LIPCH WYWIH MCHOC HAQCN BYHYG

GCHCN CUNCH AWIHN UWNMV SMHCJ YLZCL YGLIN ULUNN UWEMU HXCHN

YLXCW NCIHI ZFIWM VSGCH YMUHX VIIVS NLUJM WUJNO LYXJQ CHUIM

NUNYX NBUNN QIIHY LYACG YHNWO LLYHN FSYHA UAYXC HLYMO JJFSU

WNCPC NCYMU HXJFU HMZIL IZZYH MCPYU WNCIH CHUOA OMNNB CMULY
```

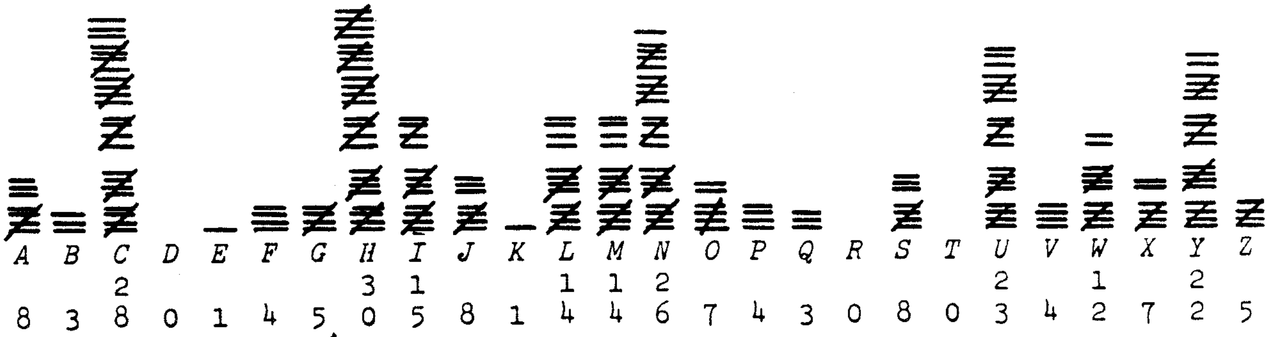


Figure 2-6 (~~C~~). Uniliteral frequency distribution, monoalphabetic substitution cipher (U).

Enlarged to a base of 1,000 by multiplication and compared to a standard uniliteral frequency distribution, it appears as in figure 2-7. A comparison of the two shows that it does not correspond to the expected norm. Expected high-frequency letters appear as low-frequency letters, low-frequency letters become medium-frequency, and medium-frequency letters are both high and low. Close inspection will show that the ciphertext still exhibits marked peaks and troughs, and a definite spatial relationship exists between them; both are characteristics of monoalphabetic substitution where only the value of the letters are changed, and consequently the frequencies of occurrence of individual letters are not suppressed. If the system is nonmonoalphabetic, where the possibility exists that

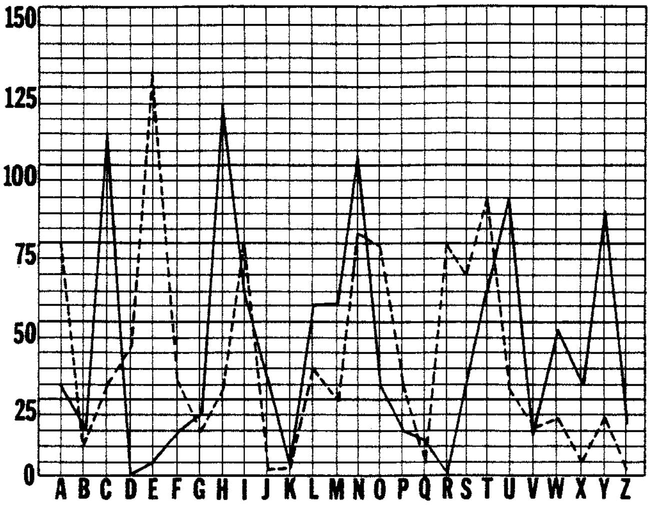


Figure 2-7 (U). Comparison, standard uniliteral frequency distribution and monoalphabetic substitution cipher (U).

one plaintext letter is represented by a number of different cipher letters, the peaks and troughs are suppressed and leveled off.

c. Once it has been determined that a given cipher alphabet is monoalphabetic, represented by the text of a cryptogram, the type alphabet (direct or reversed standard, or mixed) can be identified by comparing the spatial relationships of its peaks and troughs with those of the standard uniliteral frequency distribution. For example, if the frequency distribution for the cipher shown above is moved seven places to the right, where *Uc* corresponds to Ap, the peaks and troughs of the two distributions can be brought into alinement. This relationship is shown more clearly in figure 2–8 where each alphabet and its associated frequency distribution is inscribed on two wheels which can be moved against one another.

d. Identification of the use of direct standard reversed cipher alphabets and mixed sequence cipher alphabets employs the same techniques of comparing the peaks and troughs of the cipher alphabets in question against those of the standard uniliteral frequency distribution. For example, compare the cipher alphabets shown below to their associated standard uniliteral frequency distributions. In figure 2–9①, note that the spatial relationships are the same, except that the one representing the ciphertext is directly reversed, indicating that the alphabetic values it represents are also reversed. In figure 2–9②, no matter how the two alphabets are placed against one another, alinement is impossible, without a rearrangement of the letters of the ciphertext. Once this is done, however, peaks and troughs can be alined.

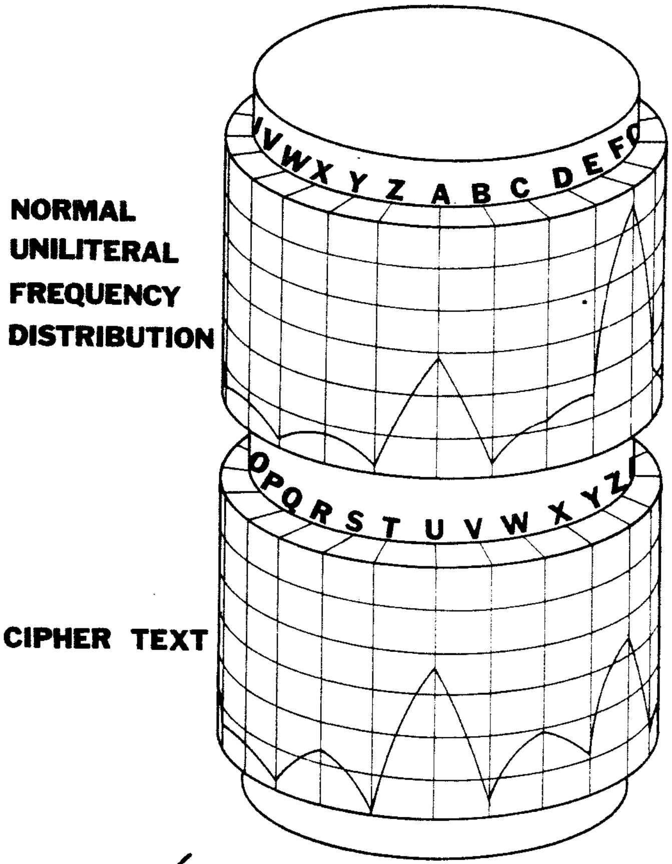


Figure 2-8 (Ø). Point of coincidence, normal uniliteral frequency distribution and ciphertext (U).

2–13. (Ø) Variations in a Uniliteral Frequency Distribution

a. In the preceding paragraphs, identification is predicated on the fact that usually the frequency distribution of a transposition cipher is very close to that of normal plaintext, while usually in a substitution cipher they are far different, making identification of either a simple matter. This is not always the case, however, for as messages decrease in length, there may be greater and greater departure from the normal proportion of vowels, and high-, low-, and medium-consonants used. This situation will limit the use of the standard uniliteral frequency distribution for identification purposes.

b. Statistical studies show the theoretical deviation from the norm. The following charts, one for each vowel (fig. 2–10), and for high-frequency (fig. 2–11), medium-frequency (fig. 2–12), and low-frequency (fig. 2–13) consonants, illustrate expected variations in frequency of occurrence by message length. The time of occurrence is shown on the vertical line, message length on the horizontal line, and maximum and minimum occurrences indicated

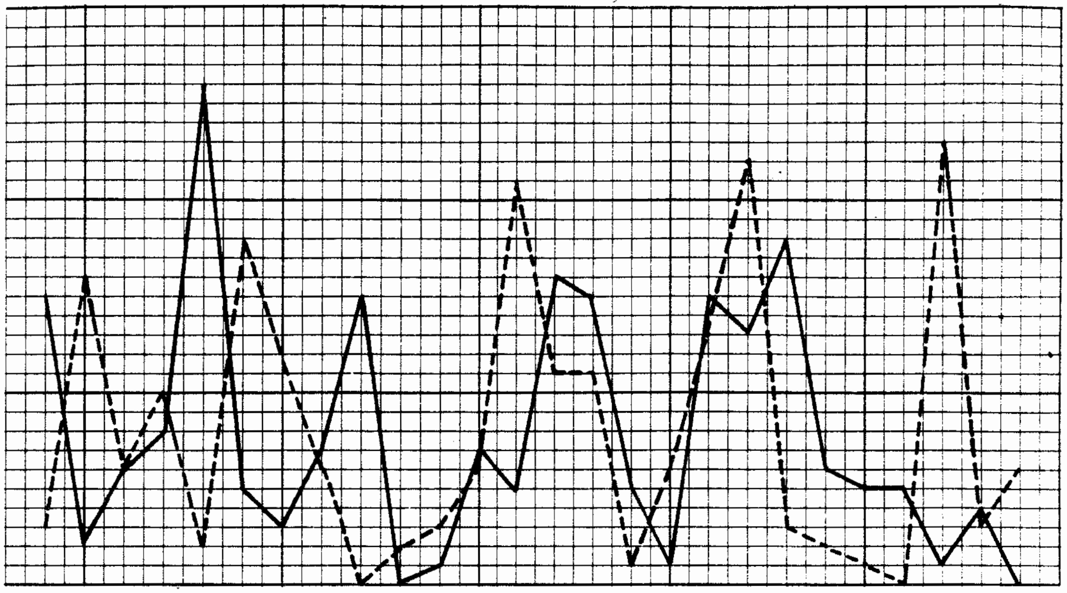


Figure 2–9① (U). Comparison, standard uniliteral distribution and reversed standard cipher alphabet (U).

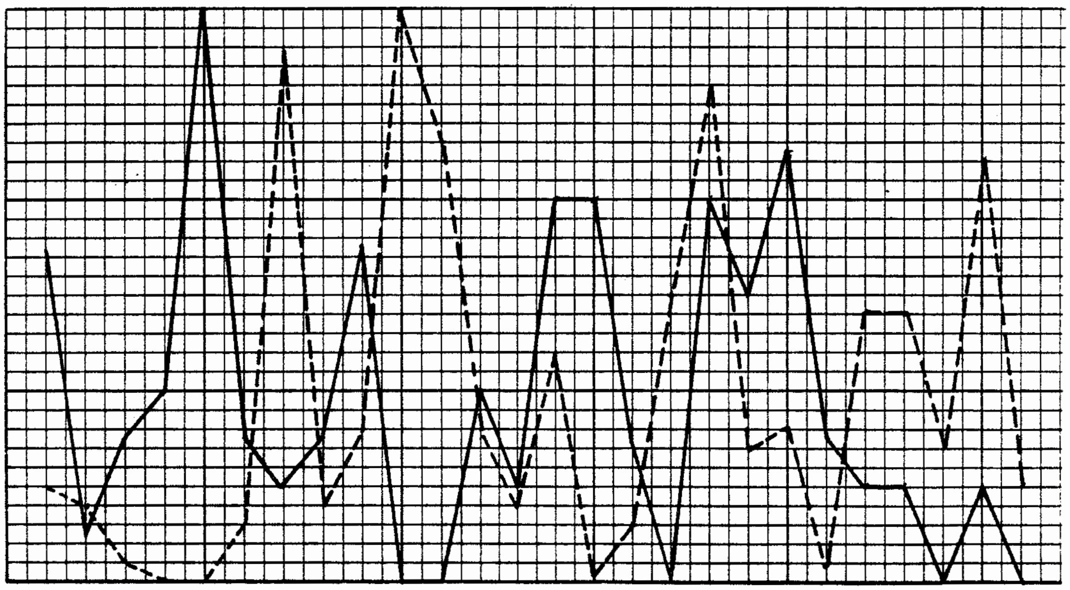


Figure 2–9② (U). Comparison, standard uniliteral distribution and mixed cipher alphabet (U).

by the upper and lower lines of the graph respectively. For example, in a plaintext message of 100 letters, the combined number of vowels appearing in it should fall within the range of 32 to 48 letters.

2–14. (~~C~~) The Lambda (λ) Test

a. The Lambda or blank expectation test is another means of determining whether a cipher message is monoalphabetic or nonmonoalphabetic. It is normally used on messages of 200 letters or less, assuming that messages of greater length can be identified easier by other methods. The test is based on the number of nonoccurrences of letters in a message. Statistical studies show that a predictable number of blanks will occur in plaintext messages, the exact number varying with the length of the message. Statistical studies also show that the theoretical numbers of blanks that will occur in a completely random assortment of letters differ from the expected number of blanks occurring in plaintext messages of equal length. From this information the blank expectation chart (fig. 2–14) has been devised which compares the expected number of blanks in plaintext and in random text, which in

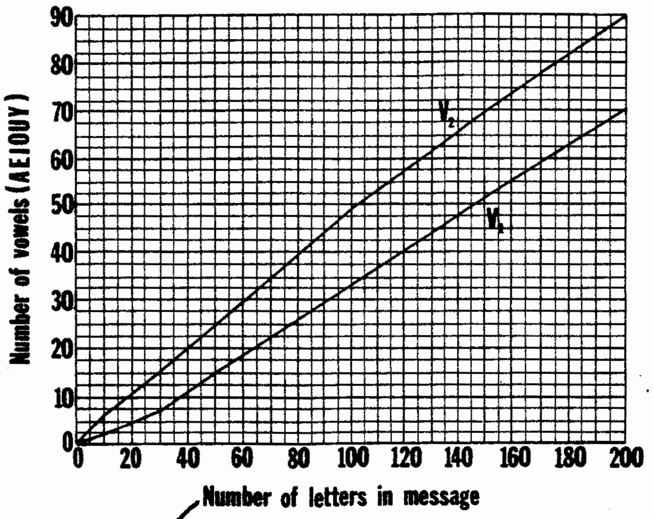


Figure 2-10 (~~C~~). *Expected occurrence of vowels, English plaintext* (*U*).

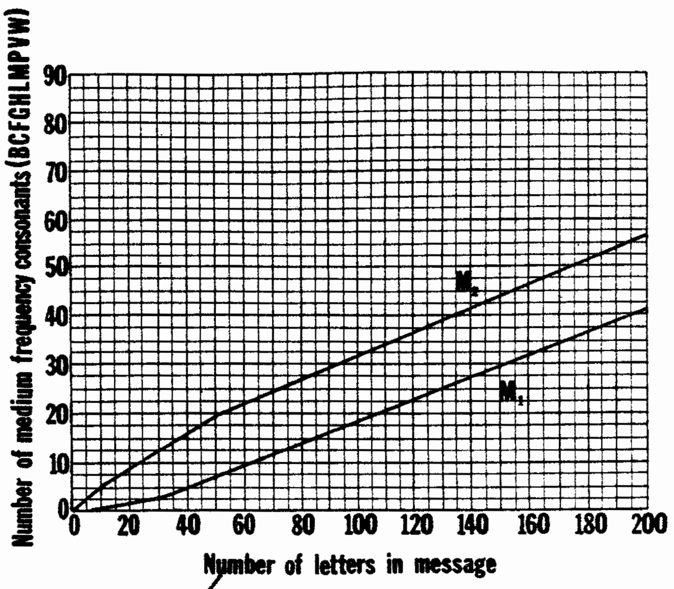


Figure 2-12 (~~C~~). *Expected occurrence of medium-frequency consonants, English plaintext* (*U*).

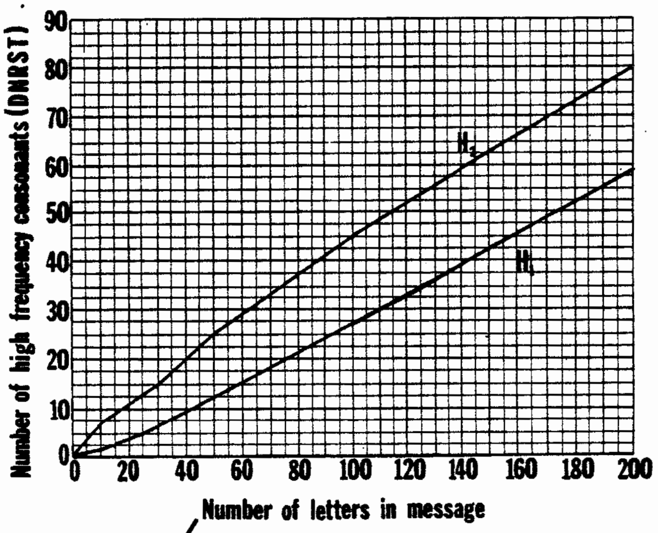


Figure 2-11 (~~C~~). *Expected occurrence of high-frequency consonants, English plaintext* (*U*).

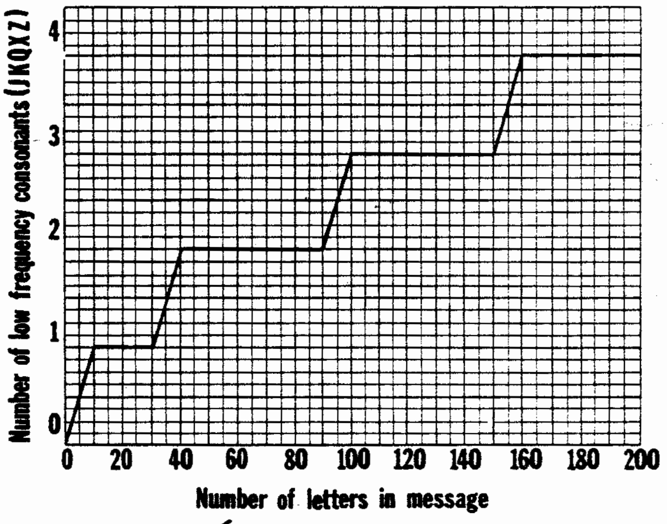


Figure 2-13 (~~C~~). *Expected occurrence of low-frequency consonants, English plaintext* (*U*).

effect is the same as the number of blanks expected in a cipher message based on a nonmonoalphabetic cipher.

b. Curve P in the chart indicates the number of expected blanks in a plaintext message and curve R the number of expected blanks in a random (nonmonoalphabetic cipher message) assortment of letters. To use the chart, find the number of blanks in the message under study. Locate this number on the vertical line indicating the number of expected blanks, locate the total number of letters in the message on the horizontal line, and then locate the point of intersection of these two points on the chart. Should the point of intersection fall closer to the P curve than to the R curve it is probably either a simple substitution or a transposition cipher. If, however, the point of intersection falls closer to the R curve, the message is probably enciphered in a nonmonoalphabetic system.

c. These charts may be used to identify the class of a cipher in addition to supplementing the standard uniliteral frequency distribution. If the count of a class of letters, vowels or consonants, falls within the expected range shown by the upper and lower lines, it is assumed to be a transposition cipher; if outside, it is assumed to be a substitution cipher. Basis of reasoning for these identifications is the same as used previously, i.e. transposition

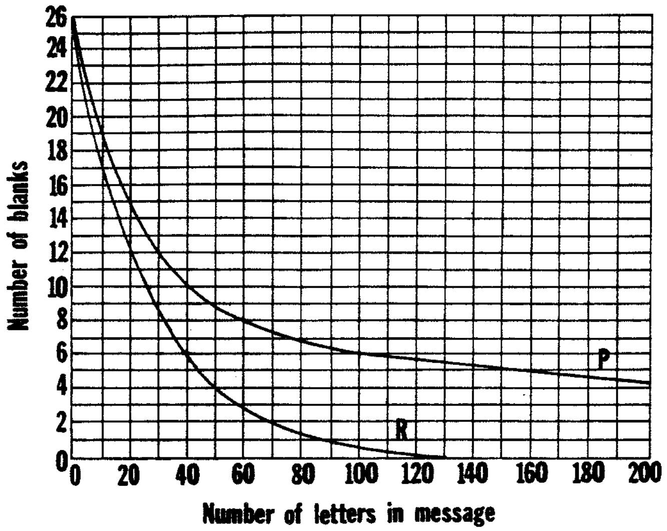


Figure 2-14. (U). The Lambda (λ) test, expected number of blanks occurring in English plaintext (U).

does not change the values of the letters while substitution does. The degree of accuracy of the identification is correlated to the distance that the point of intersection of the number of letters and message-length falls from or within the delimiting maximum-minimum lines.

2-15. (~~C~~) The Phi (φ) Test

a. In the preceding examples, identification is based largely upon visual observation of characteristics present because sufficient depth, that is quantity of messages in a given cipher, is available. However, depth is not always available. Often an analyst must work with an extremely small volume of traffic, in which case a frequency distribution is likely to be inaccurate, due to the insufficiency of traffic as well as the normally expected variations of occurrence. For such cases, a mathematical test has been developed which allows identification of monoalphabetic or nonmonoalphabetic quality.

b. This test is based upon the known frequency of occurrence of the specific letters of an alphabet, and the premise that these characteristic frequencies will be repeated in certain ciphers, even though the identity of the letters involved might be changed. For example, in English the letter E is normally one of the most frequently used letters. If in a cipher the letter X was substituted for the letter E, X then would appear in the ciphertext as often as E did in the plaintext. Also given an alphabet, the frequency of random occurrence of each of its letters can be calculated by statistical means. This frequency, random occurrence, represents the number of times a letter is liable to appear through pure chance alone where the text is solely a random mixture of all letters of the alphabet. Thus, two standards are available, the plaintext frequency of occurrence, and the random frequency of occurrence, for all alphabets.

c. The φ test then is a comparison between the observed occurrences of the letters, of a cipher represented by φo, with the expected value of random occurrence, represented by φr, and the expected plaintext occurrence, represented by φp. The use of the φ test can be seen in figures 2-15 and 2-16.

```
OWQWZ AEDTD QHHOB AWFTZ WODEO

TUWRQ BDQRO XHQDA GTBDH PZRDK
```

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3	3	0	7	2	1	1	4	0	0	1	0	0	0	4	1	6	3	0	4	1	0	5	1	0	3

Figure 2-15 (C). The Phi (φ) test, tabulation of frequencies (F) of letters (U).

```
3 3 0 7 2 1 1 4 0 0 1 0 0 0 4 1 6 3 0 4 1 0 5 1 0 3 ΣF = N
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
      4       1             1   3     1     2
6 6 0 2 2 0 0 2 0 0 0 0 0 0 2 0 0 6 0 2 0 0 0 0 0 6 ΣF (F-1) = ϕo

                        N = 50
                       ϕo = 154
```

Figure 2-16 (~~C~~). The Phi (φ) test, calculation of φo (U).

d. Observed values of occurrence (ϕo) for this distribution are calculated by applying the formula F(F–1) to the frequency of occurrence (F) of each letter and then totaling the sums of all. This is expressed mathematically as $\phi o = F(F-1)$. For example, F(F–1) ϕo of *A*=3(3–1)=3×2=6. This calculation is applied to each in turn, the individual sums then summed to derive the observed values of occurrence, ϕo. To determine the values of ϕr and ϕp, the formulas $\phi r = .0385N(N-1)$ and $\phi p = .0667N(N-1)$ are used, where N is the sum of F of the distribution. ϕr gives the value of expected random occurrence; ϕp gives the expected plaintext value for English military telegraphic text. The constants .0385 and .0667 are valid for English plaintext. The former (.0385) is the decimal equivalent of 1/26, the reciprocal of the number of letters in the alphabet. The constant .0667 is the sum of the squares of the probabilities of occurrence of the individual letters in English plaintext. Where a different alphabet is involved, these constants are different, though the formulas remain the same. The calculations are:

$$\phi r = .0385N(N-1) = .0385 \times 50 \times 49 = 94$$
$$\phi p = .0667N(N-1) = .0667 \times 50 \times 49 = 163$$

e. Once the calculations are completed, the values for observed occurrence, random expected occurrence, and expected plaintext occurrence are compared.

$$\phi o = 154$$
$$\phi r = 94$$
$$\phi p = 163$$

Since the value of ϕo (154) is closer to the value of ϕp (163) than to the value of ϕr (94), the cipher is probably monoalphabetic. If it were closer to ϕr, a nonmonoalphabetic cipher is indicated. Nonmonoalphabetic in this sense refers to the cipher being any one of the systems listed previously in paragraph 1–11 which are not monoalphabetic. If, however, the value of ϕo were just halfway between ϕr and ϕp no assumption would be made on the basis of this test.

f. The basis for identification whether a message is monoalphabetic or nonmonoalphabetic is similar to the basis in preceding tests, i.e. the nonsuppression of frequencies of occurrence when monoalphabetic ciphers are used, and their suppression by nonmonoalphabetic ciphers. The value of ϕo approaches the value ϕp in cases of nonsuppression, while the value of ϕo approaches the value of ϕr where suppression occurs. The underlying reason for the latter is that nonmonoalphabetic systems tend to randomize the frequencies of observed occurrences in ciphertext.

PART TWO (C)

TRANSPOSITION SYSTEMS

CHAPTER 3 (C)

GENERAL TRANSPOSITION SYSTEMS

Section I. (C) GENERAL

3–1. (~~C~~) Transposition Ciphers

All transposition ciphers are alike in several respects. First, and most important, all the elements of the original message are present in their original identities, only disarranged in sequence. Second, the individual bits into which the original plaintext message is divided by the transposition process are normally of equal length. They may be either single letters, pairs of letters, sets of letters, or in exceptional cases, whole words. Third, practically all transposition ciphers involve the use of matrices, a geometric design usually a square or a rectangle, with specific routes of inscription and transcription. The importance of these factors is the degree of constancy which they impart to cryptograms produced by transposition systems which form the basis of their analysis.

3–2. (U) Monoliteral, Polyliteral, and Word Transposition

Transposition ciphers are classified by the structure of the elements manipulated in the transposition processes. Those that deal with individual letters of the plaintext are monoliteral transposition. Those that deal with a component of two or more letters are polyliteral transposition. Those wherein the elements are word length are termed word transposition systems. It is possible to use any length element, as the length of the element does not affect the process of transposition. However, the monoliteral transposition systems are favored due to their practicality and security.

3–3. (U) Single and Double Transposition

Single and double transposition, also called monophase and polyphase, are transposition processes a plaintext message may undergo to become ciphertext. In single transposition, the elements transposed go through only one cycle: inscription into a matrix, and transcription to ciphertext. In double transposition the elements undergo two cycles. The letters resulting from the first transposition cycle are again submitted to a transposition process. Triple and quadruple transpositions are possible but impractical for common use. Double transposition, while limited in its use due to the same practical considerations, does provide a great deal of security; often more security than that provided by certain much more complicated substitution methods.

3–4. (~~C~~) Geometric Designs

Most transposition systems use matrices for the inscription and transcription of the plaintext and ciphertext. Squares and rectangles are most commonly used, although other geometric figures, e.g. triangles, trapezoids, and other polygons, are occasionally used. The square and rectangle are far superior to the other forms, being easier to use and less subject to error in transposition, and, therefore, of more practical application. The other geometric figures provide a greater degree of security in that the relative sequence of the elements comprising the plaintext is more completely disarranged leaving little positional pattern. However, due to their own complexity, they find little use in military communications.

3–5. (~~C~~) Transposition Routes

a. Just as the size and the shape of the matrix must be predetermined by the correspondents using a transposition system, so must the method of inscribing and transcribing the plain and ciphertexts. Depending to some degree upon the configuration of the matrix used, there are two general methods that may be followed: route, or columnar method.

b. In route transposition, the plaintext message is inscribed within a matrix in the usual manner of writing, from left to right, top to bottom. Then to

(1) Simple horizontal:

(1)	(2)	(3)	(4)
ABCDEF	FEDCBA	STUVWX	XWVUTS
GHIJKL	LKJIHG	MNOPQR	RQPONM
MNOPQR	RQPONM	GHIJKL	LKJIHG
STUVWX	XWVUTS	ABCDEF	FEDCBA

(2) Alternate horizontal:

(1)	(2)	(3)	(4)
ABCDEF	FEDCBA	XWVUTS	STUVWX
LKJIHG	GHIJKL	MNOPQR	RQPONM
MNOPQR	RQPONM	LKJIHG	GHIJKL
XWVUTS	STUVWX	ABCDEF	FEDCBA

(3) Simple diagonal:

(1)	(2)	(3)	(4)
ABDGKO	OKGDBA	GKOSVX	XVSOKG
CEHLPS	SPLHEC	DHLPTW	WTPLHD
FIMQTV	VTQMIF	BEIMQU	UQMIEB
JNRUWX	XWURNJ	ACFJNR	RNJFCA

(5)	(6)	(7)	(8)
ACFJNR	RNJFCA	JNRUWX	XWURNJ
BEIMQU	UQMIEB	FIMQTV	VTQMIF
DHLPTW	WTPLHD	CEHLPS	SPLHEC
GKOSVX	XVSOKG	ABDGKO	OKGDBA

(4) Alternate diagonal:

(1)	(2)	(3)	(4)
ABFGNO	ONGFBA	GNOUVX	XVUONG
CEHMPU	UPMHEC	FHMPTW	WTPMHF
DILQTV	VTQLID	BEILQS	SQLIEB
JKRSWX	XWSRKJ	ACDJKR	RKJDCA

(5)	(6)	(7)	(8)
ACDJKR	RKJDCA	JKRSWX	XWSRKJ
BEILQS	SQLIEB	DILQTV	VTQLID
FHMPTW	WTPMHF	CEHMPU	UPMHEC
GNOUVX	XVUONG	ABFGNO	ONGFBA

(5) Spiral clockwise:

(1)	(2)	(3)	(4)
ABCDEF	LMNOPA	DEFGHI	IJKLMN
PQRSTG	KVWXQB	CRSTUJ	HUVWXO
OXWVUH	JUTSRC	BQXWVK	GTSRQP
NMLKJI	IHGFED	APONML	FEDCBA

(6) Spiral counterclockwise:

(1)	(2)	(3)	(4)
APONML	FEDCBA	NMLKJI	IHGFED
BQXWVK	GTSRQP	OXWVUH	JUTSRC
CRSTUJ	HUVWXO	PQRSTG	KVWXQB
DEFGHI	IJKLMN	ABCDEF	LMNOPA

Figure 3-1 (~~C~~). *Matrix routes* (*U*).

form the ciphertext, the letters in the design are taken out of the matrix transcribed by following one of many different routes. Each route may have a different starting point and follow a different path through the matrix, with the only consideration being that it be orderly and fixed. Dependent upon the agreement among the correspondents, the use of routes are either fixed or varied at a given interval. A few typical routes which are used are shown in figure 3–1, and for ease in following their paths, the normal sequence of the alphabet is used.

c. Columnar transposition differs from route transposition in that the path of extraction is based upon the columns of the matrix. Again inscription is normally in the usual form of writing, although it may be varied by any route other than vertical, and then transcribed vertically from the cells of the matrix to obtain ciphertext. The sequence in which the columns are extracted from the matrix may be varied: either by following preassigned directions; top to bottom, bottom to top, etc.; or by the use of special keys which determine columnar order; or even by a combination of the two. Two of the more common vertical routes are illustrated in figure 3–2.

d. The indication for the correspondents of the

(1) Simple vertical:

(1)	(2)	(3)	(4)
AEIMQU	UQMIEA	DHLPTX	XTPLHD
BFJNRV	VRNJFB	CGKOSW	WSOKGC
CGKOSW	WSOKGC	BFJNRV	VRNJFB
DHLPTX	XTPLHD	AEIMQU	UQMIEA

(2) Alternate vertical:

(1)	(2)	(3)	(4)
AHIPQX	XQPIHA	DELMTU	UTMLED
BGJORW	WROJGB	CFKNSV	VSNKFC
CFKNSV	VSNKFC	BGJORW	WROJGB
DELMTU	UTMLED	AHIPQX	XQPIHA

Figure 3-2 (*C*). *Columnar extraction routes* (*U*).

use of a given transposition system (single or double), the type transpositions (route or columnar), and the specific route or key used are functions of the discriminant and specific key. In most cases, the discriminant refers to the use of a given transposition system and its type, while the specific key refers to the specific route or key used in the inscription and transcription processes. As required, either or both may appear in the message. They usually occur at a specific point in the message text, sometimes so constructed that to the outsider they appear as a legitimate part of the text. At other times they are easily recognizable for what they are.

Section II. (~~C~~) ROUTE TRANSPOSITION SYSTEMS

3–6. (~~C~~) Encipherment and Decipherment

a. The encipherment and decipherment steps in route transposition are based upon the use of fixed matrices and routes; the latter process is a reversal of the former. To illustrate how the system is used, the following steps are illustrated. The system in this case, to be indicated by a discriminant, is single route transposition. The specific key indicates the following elements are required.

(1) A completely filled matrix of 5 rows and 8 columns.

(2) A route of inscription following an alternate diagonal, as shown in figure 3–1, route (4)–(3).

(3) A route of transcription following an alternate diagonal, as shown in figure 3–1, route (3)–(6).

b. Inscription of the plaintext is as follows:

ATTACK HAS BEEN POSTPONED UNTIL TOMORROW TWO AM

O	S	T	I	O	W	A	M
H	P	T	N	L	R	T	O
K	A	N	P	U	T	R	W
T	C	S	E	O	D	O	O
A	T	A	B	E	N	E	M

c. Transcription to obtain ciphertext is as follows:

O	*S*	*T*	*I*	*O*	*W*	*A*	*M*
H	*P*	*T*	*N*	*L*	*R*	*T*	*O*
K	*A*	*N*	*P*	*U*	*T*	*R*	*W*
T	*C*	*S*	*E*	*O*	*D*	*O*	*O*
A	*T*	*A*	*B*	*E*	*N*	*E*	*M*

MOAWT WORRO MOTLI EDUNT NOPTS
EENPO BSAHA CKTTA

d. Decipherment is merely a reversal of the preceding steps. The cipher message is inscribed in a 5 x 8 matrix following route (3)–(6), then transcribed following route (4)–(3), thus regenerating the plaintext. Using this system requires both remembering a series of rules, and following these rules explicitly. Any deviation in either process creates some difficulty in deciphering the message with the difficulty proportional to the error.

e. Of all the transposition systems, route transposition of this type probably offers the least resistance to the cryptanalyst. This remains true despite the apparent variability afforded by changing the dimensions of the matrix, the routes of inscription and transcription, and the starting points. For example, observe the cryptogram just produced. The briefest examination would quickly reveal three words, ATTACK, HAS, and TOMORROW. In all cases the plaintext would not be so readily identifiable, but sufficient fragments would occur to enable the analyst to solve the cryptogram with little difficulty.

3–7. (~~C~~) The Use of Nulls

a. Nulls are symbols appearing in cryptographic texts which have no plaintext value. They are usually similar in appearance to the other elements of the cryptographic text. Nulls may be used to complete a matrix in transposition systems, to pad a text for purposes of security, or where service regulations require, to form groups of equal length. It is common to find that a transposition system provides a greater number of cells than letters in the message to be enciphered; or that the number of letters in the message are not divisible equally by group length. In either case nulls are often used. When nulls are used in transposition systems they must be inserted in the matrix at the same time as the plaintext, and extracted with the plaintext to form the ciphertext. Adding the nulls after the ciphertext has been generated will result in changing the sequence so that the message is either difficult or impossible to decipher.

b. As transposition ciphers are only rearranged plaintext, exhibiting all the normal frequencies of plaintext, the letters chosen for nulls are limited. Letters of very low frequency, such as J, K, Q, X, or Z in English, are normally avoided, as their overuse may make them recognizable for what they are. High- and medium-frequency letters serve best as nulls, but they are limited in their placement. To avoid the possibility of misinterpretations or errors in spelling in the text proper, nulls are generally placed in the last positions.

c. When nulls are employed solely for the purpose of making cryptanalysis more difficult, they may appear at any position within the message text. To insure the identification by concerned correspondents nulls are usually placed in prearranged positions, although the placement may be random if the system permits. For all practical purposes, however, the use and placement of nulls concern the cryptographer more than the cryptanalyst. They add to the length of the text to be enciphered, possibly induce errors, and cause the user, whose time is of the essence, difficulty in deciphering. Increase in security by their use is questionable.

3-8. ~~(C)~~ Special Cases of Route Transposition

a. The effects of route transposition may be obtained by methods other than those previously shown. Two examples are reversed writing and vertical writing; the latter in horizontal form is also known as the rail-fence cipher. Both systems are extremely simple from the cryptanalytic viewpoint, but they illustrate that a given method of encipherment may duplicate the results produced by another method. Thus, the cryptanalyst may be able to solve messages accurately, yet not have recovered the original system that produced it. Also, a solution devised for one type system may be equally valid applied to another type.

b. The procedures of reversed writing are illustrated in figure 3-3 by enciphering this message:

BRIDGE DESTROYED AS DIRECTED

(1) Reversed retaining original word length.
DETCERID SA DEYORTSED EGDIRB

(2) Regrouping the words in cipher text of five letters.
DETCE RIDSA DEYOR TSEDE GDIRB

(3) Reversing words retaining their original length.
EGDIRB DEYORTSED SA DETCERID

(4) Regrouping the reversed words in cipher text of five letters.
EGDIR BDEYO RTSED SADET CERID

Figure 3-3 ~~(C)~~. *Reversed writing* (*U*).

c. The ciphertext produced by method (2) above is duplicated by:

Inscription 1	*B*	*R*	*I*	*D*	*G*	5	
2	*E*	*D*	*E*	*S*	*T*	4	
3	*R*	*O*	*Y*	*E*	*D*	3	
4	*A*	*S*	*D*	*I*	*R*	2	
5	*E*	*C*	*T*	*E*	*D*	1	Transcription

d. The method of achieving the same message text through the use of route transposition illustrates that, although the external appearance of the two methods differ, their products are the same.

e. During the Civil War an interesting form of reversed writing, involving the use of phonetics shown in figures 3-4 and 3-5, was employed on several occasions. The following message, allegedly sent from President Lincoln to General Burnside, is an example:

Washington, D.C.

November 25, 1862

BURNSIDE, Falmouth, Virginia: Can Inn Ale me withe
2 oar our Ann Pas Ann me flesh ends N.V. Corn Inn
out with U cud Inn heaven day nest Wed roe Moore
Tom darkey hat Greek Why Hawk of Abbot Inn B chewed
I if.

Bates

Figure 3-4 ~~(C)~~. *Reversed phonetic writing* (*U*).

Reading the message backward with the stress on the phonetics the recipient reads the message as:

If I should be in boat off Aquia Creek at dark
tomorrow (Wednesday) evening, could you, without inconvenience, meet me and pass an hour
or two with me?

A. Lincoln

Figure 3-5 ~~(C)~~. *Plaintext, reversed phonetics* (*U*).

f. A system of more practical worth, when compared to that above, is vertical writing or the rail-fence cipher. The message, "BRIDGE DESTROYED AS DIRECTED," when enciphered in these systems appears as in figure 3–6.

Variation is extended simply by increasing the length of each diagonal rail:

```
B         S         S         D
 R       E T       A D       E
  I     D   R     D   I     T
   D E       O E       R C
    G         Y         E
```

Although different groups would be generated (*BSSDR ETADE* etc.), the system produces the same results as route transposition and is susceptible to the same security failures.

```
(1)  Vertical writing:  BR    BIGDS RYDSI ETDRD
                        ID    EETOE ADRCE
                        GE
                        DE
                        ST
                        RO
                        YE
                        DA
                        SD
                        IR
                        EC
                        TE
                        D

(2)  Rail-fence cipher:

     B   I   G   D   S   R   Y   D   S   I   E   T   D
       R   D   E   E   T   O   E   A   D   R   C   E
```

Figure 3–6 (Ø). *Vertical writing* (*U*).

Section III. (Ø) COLUMNAR TRANSPOSITION SYSTEMS

3–9. (Ø) General

Columnar transposition differs from route transposition in that the transcription of the plaintext from the matrix is based exclusively upon column order. One of the most common types of columnar transposition involves the use of a key to randomize the transcription of the columns. The purpose of columnar transposition is to introduce a greater degree of security than is afforded by either the route or straight sequential columnar methods. The use of a key, either numeric or alphabetic, provides a wider latitude for variation in the vertical route, yet serves as a controlling factor to coordinate the transposition process between several correspondents. Of primary interest to the analyst is that it also serves to limit the width of the matrix; the height then being the product of dividing the approximate message length by matrix width.

3–10. (Ø) Keywords and Numerical Keys

a. A numerical key is composed of a sequence of numbers, either sequential or random and is used to control certain cryptographic operations. To preclude the necessity of carrying a long sequence of random numbers in written form, cryptographers have devised a simple method of deriving such sequences from words, phrases, or sentences, which can be remembered much more easily than the sequence of numbers. This memory aid is known as a keyword or keyphrase, whichever the case may be; and from a prearranged key, a series of numbers can be derived, as shown below:

KEYWORD	H	E	A	D	Q	U	A	R	T	E	R	S
NUMERICAL KEY	6	4	1	3	7	12	2	8	11	5	9	10

The numerical key is derived by assigning numbers in sequential order to the letters of the keyword in their alphabetic order. Thus A is assigned the number 1, and since A is repeated in the keyword, it is assigned 2 at its next position. Alphabetically D follows A, so it is assigned the next available number, 3. The process is continued until each letter has been assigned a number, no number being repeated.

b. The method of deriving a numerical key from a literal key as shown above is only one of a number of methods, but it is the most commonly used. The same technique may be applied to phrases or to sentences so that a very long numerical key, impossible to remember ordinarily, may be generated at will. So far as the cryptanalyst is concerned it is not essential to know how a key was derived in a specific case, except when this knowledge will enable him to generate additional keys for the solution of other messages. Often, as will be demonstrated in subsequent paragraphs, he may be unaware that a literal key has been used as the basis for a numerical key, or if aware of this, be unable to recreate the true literal key by analysis of available information alone.

c. Several general factors enter into the selection of literal keys which are of interest to the cryptanalyst, and which can under certain circumstances prove of value.

(1) It is usually such that it can be remembered easily.

(2) Normally it contains as few repeated letters or words as possible.

(3) It usually consists of one or more simple familiar words or phrases, which admit only one spelling and one order.

(4) It should present no direct association with the special situation in which it is used, so as not to be easily assumed.

3-11. (~~C~~) Use of Keys With Completely Filled Matrices

a. In keyed columnar transposition, where a completely filled matrix is used, the letters are written into a matrix, a square or a rectangle with nulls being added to complete the matrix or to provide the requisite number of characters to form complete groups; then transcribed vertically by following the sequence of columns as determined by the numerical key. For example, in figure 3-7, a message is enciphered by this method.

```
Message         REPORT LOCATION OF SECOND BATTALION COMMAND POST TODAY

Keyword                                 L I B E R T Y
Numerical Key                           4 3 1 2 5 6 7
                                        R E P O R T L
                                        O C A T I O N
                                        O F S E C O N
                                        D B A T T A L
                                        I O N C O M M
                                        A N D P O S T
                                        T O D A Y D N

Cipher Text                  PASAN DDOTE TCPAE CFBON OROOD
                             IATRI CTOOY TOOAM SDLNN LMTN
```

Figure 3-7 (~~C~~). *Keyed columnar transposition* (*U*).

b. To decipher such a message, a matrix of the proper size must first be constructed. In this case, since the key contains 7 numbers and the message has 49 letters, the matrix must be a 7 x 7 square if the rectangle is completely filled. After constructing the matrix, the message is inscribed in it, starting with the first group of the message and following the sequence of columns indicated by the numerical key. Once the inscription is completed, the message can be read horizontally.

c. The results produced by this method may be varied by one or a combination of changes in the keyword and in the routes of inscription and transcription. However, all things being equal, variation is most often introduced by changes in the key. A change of key on a daily basis, or for each message, is possible by preparing a whole list of keys for a given period, a different key being used in each case. It is also possible to designate the specific key to be used from a prepared list of keys through the use of an indicator in the message, inserted in a prearranged position of the message text. This last procedure has one disadvantage, however. If the indicator is erroneously transmitted, the message may be impossible to decipher, in which case the recipient must either ask that the message be retransmitted or ask that the key indicator be confirmed. In both cases the indicator may be revealed.

3-12. (~~C~~) Use of Keys With Incompletely Filled Matrices

a. The degree of cryptographic security of keyed columnar transposition is increased if the matrix is not completely filled, the number of cells in the matrix exceeding the total number of letters in the message. This increased security creates more difficulty for the cryptanalyst in determining the dimensions of the matrix, and the corresponding length of individual columns once width is assumed or proved. Where this system is used, cells which will be left blank must be specified.

b. Normally the system operates as shown in figure 3-8.

c. To decipher the message the cryptographer must know the key and the position where cells will be left blank. Knowing that the key contains 7 letters and the message 30 letters, he can determine the dimensions of the matrix to be 7 x 5, 35 cells, 5 more than needed. Constructing a matrix of this size, he crosses off the blank cells and inscribes the cryptogram in the remaining open cells in the order predetermined by the key.

```
Message:            REQUEST IMMEDIATE REINFORCEMENTS
Keyword:                         P R O D U C T
Numerical Key:                   4 5 3 2 7 1 6
                                 R E Q U E S T
                                 I M M E D I A
                                 T E R E I N F
                                 O R C E M E N
                                 T S
Cipher Text:        SINEU EEEQM RCRIT OTEME RSTAF NEDIM
```

Figure 3–8 (C). Keyed columnar transposition with incompletely filled matrix (U).

```
4  5  3  2  7  1  6
–  –  Q  U  –  S  –
–  –  M  E  –  I  –
–  –  –  E  –  N  –
–  –  –  E  –  E  –
–  –  #  #  #  #  #
```

d. To illustrate the importance of adding nulls in transposition systems prior to the transcription stage, figure 3–9 depicts what could occur if nulls were added after the encipherment process.

e. Note that the addition of three nulls to complete the last group results in the destruction of the orderly sequence of the reencription process, compounded by the use of keys, thus making the message indecipherable. The cryptographer has two options, ask for a retransmission of the message or attempt solution by eliminating the nulls, which requires their identification first. The former case provides clues for the cryptanalyst.

3–13. (C) Variations on Columnar Methods

A variation of columnar methods, either straight or keyed, may be obtained by writing the message out and extracting cryptographic text by decimation or by assigning the numerical key to individual letters, repeating its sequence as required.

```
KEY  4 5 3 2 7 1 6 4 5 3 2 7 1 6 4 5 3 2 7 1 6 4 5 3 2 7 1 6 4 5
     R E Q U E S T I M M E D I A T E R E I N F O R C E M E N T S
```

The letters are taken out in order, all those with the same number at the same time, in the order of their appearance in the text.

```
1 1 1 1 2   2 2 2 3 3   3 3 4 4 4   4 4 5 5 5  etc.
S I N E U   E E E Q M   R C R I T   O T E M E  etc.
```

The process results in the same text as derived from the incompletely filled matrix illustrated in figure 3–8. If the letters are extracted by decimation, i.e. every letter which occurs at a given interval, the results are the same as straight columnar transposition, the width of the matrix equal to the interval of the decimation.

Message: COMMAND POST LOCATED AT ROAD JUNCTION

Matrix:

A	L	P	H	A	B	E	T
1	6	7	5	2	3	4	8
C	*O*	*M*	*M*	*A*	*N*	*D*	*P*
O	*S*	*T*	*L*	*O*	*C*	*A*	*T*
E	*D*	*A*	*T*	*R*	*O*	*A*	*D*
J	*U*	*N*	*C*	*T*	*I*	*O*	*N*

Cipher Text: *COEJA ORTNC OIDAA OMLTC OSDUM TANPT DNROH*

Nulls: *ROH* added after transcription to complete last group.

A	L	P	H	A	B	E	T
1	6	7	5	2	3	4	8
C	*S*	*A*	*L*	*O*	*C*	*A*	*N*
O	*D*	*N*	*T*	*R*	*O*	*A*	*R*
E	*U*	*P*	*C*	*T*	*I*	*O*	*O*
J	*M*	*T*	*O*	*N*	*D*	*M*	*H*
A	*T*	*D*					

Decipherment produces unintelligible plaintext:
CSALOCA NODN TROAR ... etc.

Figure 3–9 (~~C~~). *Addition of nulls after encipherment* (*U*).

CHAPTER 4 (~~C~~)

SOLUTION OF SINGLE TRANSPOSITION SYSTEMS

Section I. (~~C~~) PRINCIPLES OF SOLUTION

4–1. (~~C~~) Review of Characteristics

a. Prior to attempting the solution of any cryptogram, the analyst reviews exactly what is known concerning the basic operation and characteristics of the system which produced that cryptogram. This general information, plus any foreknowledge of the possible contents or subject matter of the message, will determine to a great degree methodology and rapidity of solution. The general characteristics covered to this point are:

(1) Transposition ciphers are a rearrangement of plaintext, therefore they will exhibit all the frequency characteristics of plaintext.

(2) The process of encipherment consists of two stages, inscribing the plaintext into a matrix, and transcribing ciphertext from the matrix.

(3) The routes of inscription and transcription are fixed, and each differs from the other.

(4) Normally the matrix is either a square or a rectangle, and if the latter, not remarkably distorted.

(5), The dimensions of the matrix are determined by either the message length or by the length of message divided by key length. In those cases where an incomplete matrix is used, the dimension may be slightly larger in the vertical plane.

(6) Nulls may be inserted to complete a matrix or to even group lengths, thus usually limiting their number.

(7) Nulls are inserted prior to the encipherment process; accordingly their identification is not, except in rare cases, critical to the solution of the message.

b. With these known characteristics, the analysis of transposition systems becomes one of initial identification, determination of the matrix dimensions, anagramming to recover the plaintext, and finally, key and route recovery.

4–2. (~~C~~) Identification

Transposition systems as a class are not difficult to identify since cryptograms produced reflect the characteristic frequencies of plaintext. The standard uniliteral frequency distribution, given in paragraph 2–13, usually suffices to identify one composed of English letters. For other languages special frequency distributions drawn up for them would serve the same purpose. As a matter of course, one of the first things the cryptanalyst does when attempting solution of any unknown system is to make a frequency distribution or test of the cryptogram under study.

4–3. (~~C~~) Determination of Matrix Dimensions

a. Once it is established that a given cryptogram is produced by a transposition system, the second step toward solution is the determination of the matrix dimensions. Where completely filled matrices are involved this is a relatively simple matter, for the dimensions, width times height, must equal message length. The only problem incurred is to determine which factors to select.

For example, if the message contains 96 letters, possible dimensions of the matrix are: 8 x 12, 12 x 8, 6 x 16, 16 x 6, 4 x 24, 24 x 4, or 48 x 2 and 2 x 48. In actual practice, the matrix dimensions probably would be a combination of the factors 12 and 8, or 6 and 16, rather than the other possibilities. The distorted rectangles represented by combinations of 24 x 4 and 48 x 2 produce a cryptogram similar to the vertical writing or rail-fence cipher discussed previously. In most cases the final solution to this problem lies in limiting the choices, and then eliminating incorrect assumptions by trial and error.

b. Where incompletely filled matrices are used, an additional problem of determining the dimensions of the matrix is introduced. Determination may be based upon finding two factors which will equal message length plus a number, corresponding to the blank cells, which is not greater than the assumed value of matrix width. For example, note the sequence of letters, indicated by number for clarity, and the occurrence of blank cells in figure 4–1.

c. Matrix 1 contains a total of 64 cells, of which only 60 are required, leaving 4 as blanks. Matrix

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60				

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60				

Figure 4-1 (U). Letter sequence, incompletely filled matrices (U).

2 contains a total of 72 cells, a surplus of 12. Following the normal procedure for inscription, the last row and the four cells at the extreme right of the next-to-last row in matrix 2 are left blank; and the last four at the extreme bottom right of matrix 1 are left blank. In both cases, assuming the same key, the cryptograms produced from either matrix are similar in all respects to the other.

d. Therefore, in those cases where blank cells occur in a matrix, a greater variation in dimensions is expected. However, as extra rows equal to the width of the matrix are of no consequence in the encipherment process, a certain limitation does exist. For example, in the case of a message of 60 letters, matrix dimensions could be 8 x 8, 9 x 7, 7 x 9, 11 x 6, 13 x 5, 14 x 5, 16 x 4, 17 x 4, etc. In each case dimensions give an excess of 60 cells, yet the total number of blank cells does not exceed the total cells in a row. Final determination of the correct matrix is one of trial and error starting with the square and nearly-square rectangles.

4–4. (~~C~~) Anagramming

a. Having determined possible matrix dimensions and possible column length, the analyst attempts recovery of the plaintext through a process termed anagramming, which simply returns the plaintext letters to their normal position within the matrix.

b. The process of anagramming uses the following factors:

(1) The column totals times number of letters in each column is equal to message length. Therefore, if the analyst's assumption of matrix dimensions is correct, he can reconstruct the original columns simply by dividing the message in letter length elements that are equal to the height of the matrix.

(2) All letters in a given column follow one another in an orderly fixed sequence, a result of the horizontal inscription, and thus cannot be changed without changing the length of the column. In this case, the sequence of the letters are not disturbed. Only the column in which a letter or a series of letters might appear is changed.

(3) The letters that appear in a given row, when a number of assumed columns are brought together, can be changed in only two ways. First, the letters may be changed only by a change in column length. Otherwise they must remain fixed. Second, the sequence of their appearance in a given row can be changed only by the rearrangement of the order in which the columns are juxtaposed; a change which will result in changing the sequence of the letters in all the rows.

c. As anagramming involves the spelling out of complete words from fragments and individual letters that appear at random in each row, the analyst can use the vowel-consonant ratio, a stable characteristic exhibited by all alphabetic languages. In English, this ratio is 40 to 60, 40 percent vowels to 60 percent consonants. As the plaintext is inscribed horizontally, the vowel-consonant ratio will occur in the rows of a matrix. This phenomenon then serves as a check of the accuracy of the assumed matrix dimensions. A count of vowels and consonants in each row is made and compared to the expected ratio. Should all the ratios fall well outside that expected, the rows may be changed, but only by changing the column length, until reasonable ratios appear. It must be expected that the exact vowel-consonant ratio will not always appear, particularly where such small samples are involved; but, on the other hand, the ratios should not be extremely distorted either.

4–5. (~~C~~) Recovery of the Key

Recovery of the key is not essential to the solution of transposition systems. In fact, it is possible and is usually the case that when a given cryptogram is solved, the key recovery never proceeds further than the recovery of the numeric key. This is the literal key from which it was drawn and is either unrecognized or unrecoverable with the information available to the analyst. Where variations of a basic key are involved, recovery becomes possible and, in terms of speeding subsequent solutions of related cryptograms, very profitable.

4–6. (~~C~~) System Identification

a. System identification is always the first step unless the basic system is known without a doubt. As a matter of course, where the identity of a system is suspect but not assured, a test is used to confirm its identity. This may take time but, when considered in relation to the time spent in attempting to solve a system with completely inappropriate methods, it is time well spent. Prior to conducting any test, any element not part of the text must be eliminated to avoid the possibility of distorting test results.

Message:

```
VASCO  UOUTE  QFVRM  OCSWH  RRERG
SMPET  ARNTR  IIERY  EERON  RNAMA
ESOER  ESLUR  ABSZO  IELFO  RETON
IRPBD  UOEOO  TDIOM  TZHMI  QFSSD
DEEEW  VASCO
```

An examination of the message reveals a repeated group "VASCO" appearing in the first and last position. Although it is similar structurally to the other groups, its separate appearance and the positions in which it occurs, are indicative of a specific key. Therefore, these groups are immediately eliminated. Using the remaining 20 groups, a uniliteral frequency distribution is made of the ciphertext, see figure 4–2.

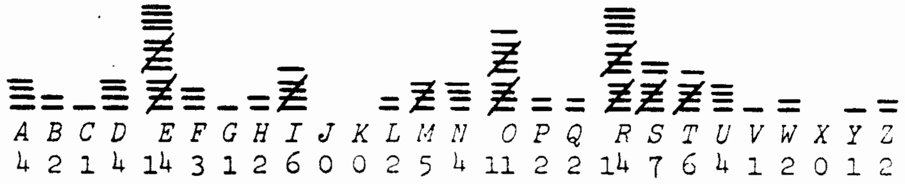


Figure 4–2 (U). Uniliteral frequency distribution, ciphertext (U).

b. Comparing this uniliteral frequency distribution with the standard uniliteral frequency distribution (based on 100 English plaintext letters) reveals similar characteristics, see figure 4–3.

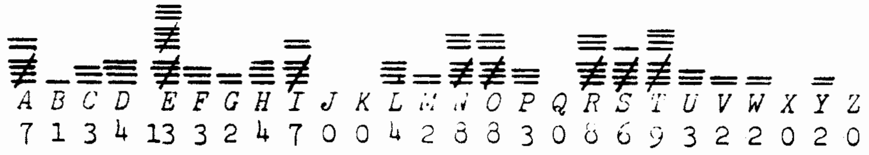


Figure 4–3 (U). Standard uniliteral frequency distribution (U).

The deviations that exist are not radical and can be accounted for by the smallness of the sample. The sample exhibits the same characteristic peaks and troughs of English plaintext, and the vowel consonant ratio appears very good. Therefore, the assumption that the cryptographic system is transposition is quite safe, unless proven contrary in the analytic stages.

4–7. (~~C~~) Recovery of Matrix Dimensions

a. Presuming the system under study is a completely filled matrix, the dimensions are easily determined. The combination of 10 x 10 is the most likely one which will provide a matrix of the proper size, though combinations of 20, 25, and 50 are possible. A matrix of 10 x 10 dictates that there be 10 columns, each containing 10 letters. Accordingly, the message is divided into 10-letter lengths and transcribed to the vertical position, each corresponding to an assumed column. Just as the ciphertext is originally removed from the matrix by columns, this process is merely a reversal of the enciphering process. For ease in identifying the columns during later manipulation, they are numbered as they are withdrawn from the message.

1	2	3	4	5	6	7	8	9	10
U	*O*	*S*	*I*	*R*	*E*	*I*	*I*	*T*	*Q*
O	*C*	*M*	*I*	*N*	*S*	*E*	*R*	*D*	*F*
U	*S*	*P*	*E*	*A*	*L*	*L*	*P*	*I*	*S*
T	*W*	*E*	*R*	*M*	*U*	*F*	*B*	*O*	*S*
E	*H*	*T*	*Y*	*A*	*R*	*O*	*D*	*M*	*D*
Q	*R*	*A*	*E*	*E*	*A*	*R*	*U*	*T*	*D*
F	*R*	*R*	*E*	*S*	*B*	*E*	*O*	*Z*	*E*
V	*E*	*N*	*R*	*O*	*S*	*T*	*E*	*H*	*E*
R	*R*	*T*	*O*	*E*	*Z*	*O*	*O*	*M*	*E*
M	*G*	*R*	*N*	*R*	*O*	*N*	*O*	*I*	*W*

b. At this stage, if the message is enciphered by a straight columnar route transposition, it could be read out of the matrix along the horizontal rows. Therefore, since it is unreadable in its present form, it is assumed that the system is keyed columnar transposition. The plaintext would not then appear without first rearranging the sequence of the columns.

4-8. (~~C~~) Anagramming To Recover Plaintext

a. Before attempting to anagram, the analyst must examine the matrix he has constructed, particularly the letter values appearing in each row. If the anagramming is to be successful and plaintext is to appear, each row must exhibit a good vowel-consonant ratio. This ratio does not have to be exact; the prime requirement is that it be possible. If the ratio is unacceptable, the analyst has but one recourse, to change the dimensions of the matrix in order to change row letter values.

b. A check of the individual rows in the matrix above reveals the following vowel-consonant ratios.

1	2	3	4	5	6	7	8	9	10	Vowels	Consonants
U	*O*	*S*	*I*	*R*	*E*	*I*	*I*	*T*	*Q*	6	4
O	*C*	*M*	*I*	*N*	*S*	*E*	*R*	*D*	*F*	3	7
U	*S*	*P*	*E*	*A*	*L*	*L*	*P*	*I*	*S*	3	7
T	*W*	*E*	*R*	*M*	*U*	*F*	*B*	*O*	*S*	3	7
E	*H*	*T*	*Y*	*A*	*R*	*O*	*D*	*M*	*D*	3	7
Q	*R*	*A*	*E*	*E*	*A*	*R*	*U*	*T*	*D*	4	6
F	*R*	*R*	*E*	*S*	*B*	*E*	*O*	*Z*	*E*	4	6
V	*E*	*N*	*R*	*O*	*S*	*T*	*E*	*H*	*E*	4	6
R	*R*	*T*	*O*	*E*	*Z*	*O*	*O*	*M*	*E*	5	5
M	*G*	*R*	*N*	*R*	*O*	*N*	*O*	*I*	*W*	3	7

These ratios, while not perfect, do not exhibit any unusual abnormalities such as rows almost exclusively composed of vowels or consonants. Further, note that the first row composed of 6 vowels and 4 consonants, a reversal of the expected norm, is followed by a number of rows where the vowel count if slightly lower than normal. This is not an unusual condition. Therefore, there being nothing to disprove the original assumption as to the dimension of the matrix at this stage, the anagramming can be started.

c. Several factors will aid the analyst in the anagramming process. Among these are the characteristic combinations of certain letters to form digraphs and trigraphs, the frequency with which they are used, and the types of terminology common to the correspondents using the cipher system. These factors will form the basis by which the anagramming process can be continued.

(1) In column 10, row 1, a letter *Q* appears, a letter of low frequency usage, but when used in English is, almost without exception, followed by a *U*. Scanning row 1 of all adjacent columns reveals a *U* in column 1. By placing these columns side by side in the order 10–1 the following digraphs are formed:

	10	1	
Row 1	*Q*	*U*	(15)
2	*F*	*O*	(40)
3	*S*	*U*	(11)
4	*S*	*T*	(63)
5	*D*	*E*	(42)
6	*D*	*Q*	(02)
7	*E*	*F*	(18)
8	*E*	*V*	(20)
9	*E*	*R*	(87)
0	*W*	*M*	(00)

Comparing the digraphs so formed against those in table A–1, Frequency Distribution of Digraphs, the frequencies shown in brackets are obtained. All with the exception of *WM*, *DQ*, and *SU* are medium to high-frequency digraphs, which gives weight to the juxtaposition of these columns. The occurrence of *WM* and *DQ* in particular may be explained as word endings and beginnings. Therefore, these columns may be accepted and the anagramming process continued.

(2) The *Q* appearing in row 6, column 1 can be matched to the *U* in the same row, column 8 for the same reason as the preceding match. Thus the columns appear as:

	10	1	8
1	*Q*	*U*	*I*
2	*F*	*O*	*R*
3	*S*	*U*	*P*
4	*S*	*T*	*B*
5	*D*	*E*	*D*
6	*D*	*Q*	*U*
7	*E*	*F*	*O*
8	*E*	*V*	*E*
9	*E*	*R*	*O*
0	*W*	*M*	*O*

The trigraphs formed by the addition of column 8 are not unusual. In fact, *FOR* and *EVE* are quite common, and *QUI*, *SUP*, and *ERO* offer several possibilities for good word fragments. The next step then is to scan the remaining columns for a letter or combination of letters of significance. Another low-frequency letter is the letter *Z* in row 9 column 6. It is not often used, though in military communications it is used for the word "zero." The trigraph *ERO* above could be combined with the *Z* to form the word *ZERO*. Accordingly the columns are juxtaposed.

	6	10	1	8
1	*E*	*Q*	*U*	*I*
2	*S*	*F*	*O*	*R*
3	*L*	*S*	*U*	*P*
4	*U*	*S*	*T*	*B*
5	*R*	*D*	*E*	*D*
6	*A*	*D*	*Q*	*U*
7	*B*	*E*	*F*	*O*
8	*S*	*E*	*V*	*E*
9	*Z*	*E*	*R*	*O*
0	*O*	*W*	*M*	*O*

(3) At this point, one word (*ZERO*) plus several other word fragments emerge. *SEVE* in row 8 suggests *SEVEN; BEFO* in row 7 may be *BEFORE.* If these initial word assumptions are valid, we need only find a column with the letter *R* and *N* in the 7th and 8th row positions respectively. Checking the remaining columns, this combination is found in column 3. An *R* also is found in the 7th position of column 2, but as an *E* appears in the 8th position. it is rejected. Column 3 is then placed in the matrix to the right of column 8.

	6	10	1	8	3
1	*E*	*Q*	*U*	*I*	*S*
2	*S*	*F*	*O*	*R*	*M*
3	*L*	*S*	*U*	*P*	*P*
4	*U*	*S*	*T*	*B*	*E*
5	*R*	*D*	*E*	*D*	*T*
6	*A*	*D*	*Q*	*U*	*A*
7	*B*	*E*	*F*	*O*	*R*
8	*S*	*E*	*V*	*E*	*N*
9	*Z*	*E*	*R*	*O*	*T*
0	*O*	*W*	*M*	*O*	*R*

(4) From this point on the solution is quite simple. Only five columns remain to be placed, and sufficient word fragments appear in the partially recovered matrix to affect this easily. For example, in row 1 the fragment *EQUIS* must be preceded by a consonant; and there are only two unplaced, the *R* in column 5 and the *T* in column 9. Column 5 then is placed before column 6.

	5	6	10	1	8	3
1	*R*	*E*	*Q*	*U*	*I*	*S*
2	*N*	*S*	*F*	*O*	*R*	*M*
3	*A*	*L*	*S*	*U*	*P*	*P*
4	*M*	*U*	*S*	*T*	*B*	*E*
5	*A*	*R*	*D*	*E*	*D*	*T*
6	*E*	*A*	*D*	*Q*	*U*	*A*
7	*S*	*B*	*E*	*F*	*O*	*R*
8	*O*	*S*	*E*	*V*	*E*	*N*
9	*E*	*Z*	*E*	*R*	*O*	*T*
0	*R*	*O*	*W*	*M*	*O*	*R*

(5) In row 1, the word fragment *REQUIS* suggests the word *REQUISITION*. A quick glance at the remaining values in row 1 of the unplaced columns reveals the letters *I, T, I*, and *O*, which combined with the *N* in column 5 row 2 completes the word. If at this point it could be determined which column, 7 or 4, containing the *I* follows column 3, the entire matrix could be written out. The word *BEFORE* in row 7 has yet to be completed, but here again the same situation is found; an *E* appears in row 7 of both columns 7 and 4. The assumed word *REQUISITION* hints at the subject of the message. Considering this, the word fragment *SUPP* in row 3 may possibly be the word *SUPPLY, SUPPLIES, SUPPLIED*, etc., all with the letter *L* following the last *P*. An *L* appears only in column 7 row 3, so it is assumed that column 7 follows column 3. If this is the case, the remaining columns must be placed in order 9—4—2 to complete the word *REQUISITION*, the *N* appearing at the first position of the second row. To confirm this assumption, the entire matrix is written out and the plaintext read off horizontally.

5	6	10	1	8	3	7	9	4	2
R	*E*	*Q*	*U*	*I*	*S*	*I*	*T*	*I*	*O*
N	*S*	*F*	*O*	*R*	*M*	*E*	*D*	*I*	*C*
A	*L*	*S*	*U*	*P*	*P*	*L*	*I*	*E*	*S*
M	*U*	*S*	*T*	*B*	*E*	*F*	*O*	*R*	*W*
A	*R*	*D*	*E*	*D*	*T*	*O*	*M*	*Y*	*H*
E	*A*	*D*	*Q*	*U*	*A*	*R*	*T*	*E*	*R*
S	*B*	*E*	*F*	*O*	*R*	*E*	*Z*	*E*	*R*
O	*S*	*E*	*V*	*E*	*N*	*T*	*H*	*R*	*E*
E	*Z*	*E*	*R*	*O*	*T*	*O*	*M*	*O*	*R*
R	*O*	*W*	*M*	*O*	*R*	*N*	*I*	*N*	*G*

d. As illustrated above, the process of anagramming results in the recovery of the key used in extracting the cipher message from the matrix. Only in those situations where the key exhibits characteristics of being generated by some recoverable system, either through a manipulation of the key values themselves or through derivation from a literal key, is this of significance. Usually the recovery of the key is left at this point.

Section II. (~~C~~) SOLUTION OF INCOMPLETELY FILLED MATRICES

4–9. (~~C~~) General

The techniques of solution given previously represent those which are generally applicable to all columnar transposition systems. However, where the matrix is incompletely filled, a slightly different approach is required and is somewhat more involved. There are some instances where special conditions are present, and quick and convenient solutions can be reached, circumventing some of the more difficult process required for a general solution. In the following paragraphs a type of general solution is treated, followed by some of the special cases where a modified technique may be used. In all cases the basic method is based upon the characteristics of transposition systems dealt with in preceding paragraphs.

4–10. (~~C~~) A Solution for Incompletely Filled Matrices

a. When dealing with cryptograms produced by this method, the most critical phase is identifying the system as such. If the cryptographic text contains an odd number of letters not equally divisible, it is obvious that this system is employed. Where the text is even or equally divisible, as is most often the case considering the norm of padding out the message to obtain groups of equal length, identification is more difficult and usually comes only after attempting to solve it as a completely filled matrix. If this attempt fails, it is assumed that it is an incompletely filled matrix. But, assuming that the system has been identified, the next problem is to determine the dimensions of the matrix.

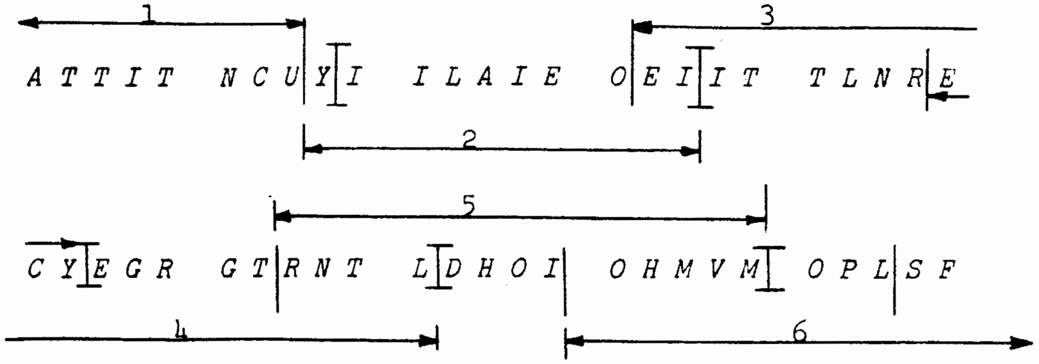
b. Wherever an incompletely filled matrix is suspected, the dimensions are assumed to be the factors of message letter length, plus a number of cells not to exceed the width of the matrix, which are evenly divisible.

For example, examine the following cryptogram which contains 50 letters.

ATTIT NCUYI ILAIE OEIIT TLNRE
CYEGR GTRNT LDHOI OHMVM OPLSF

Were it derived from a completely filled matrix, a 5 x 10 or a 10 x 5 matrix is immediately assumed. But as an incompletely filled matrix is suspected, several assumptions leading to the dimensions are first considered. First, the product of the dimensions will exceed 50 cells. Second, nulls, if used to round out the groups, will appear in the matrix. Third, the cells left blank will not exceed matrix width. Given these generalities, the combination of 6 x 9 or 7 x 8 appears as possible dimensions. Other combinations such as 4 x 13, or 5 x 11 are not be be rejected completely. Since the former gives a more proportional rectangle, it is tried first. In any case, the final determination of the correct matrix size, unless there is prior knowledge available, is largely a matter of trial and error.

c. Assuming a dimension of 6 x 9, the message may now be broken into columns in such a manner as to fit the matrix, blank cells included. Thus, in a matrix of this dimension, there are two columns 9 letters long and four columns 8 letters long. If the extraction is determined by a key, any specific column cannot be given a definite length. General parameters can be established based on the limitations of column length present. Any column can only be 8 or 9 letters long. Using this limitation, columns of maximum-minimum length are ascertained by decimating the message at intervals as shown in figure 4–4 first by 8's, then by 9's, starting at the first letter of the message. Possible columns thus generated can be arranged in the vertical position, numbered in the order of their extraction. The columns above represent the minimum and maximum lengths of any column in that particular position of the matrix, as determined by its position in the message.


1
3
A T T I T N C U Y I I L A I E O E I I T T L N R E
2
5
C Y E G R G T R N T L D H O I O H M V M O P L S F
4
6

```
1 2 3 4 5 6

  Y E E R O
A I I C N H
T I I Y T M
T L T E L V
I A T G D M
T I L R H O
N E N G O P
C O R T I L
U E E R O S
Y I C N H F
    Y T M
      L V
        M
```

Figure 4-4 (~~*C*~~). *Determination of column length* (*U*).

For example, column 1 being in the first position of the message, must start at a known position. Thus, it can only be, at the maximum, 9 letters long. The second column may begin at the 9th or 10th letter, depending upon the length of the first column, and thus will contain 10 letters of which only 8 or 9 represent the true column length.

d. As these columns represent minimum-maximum length, a vertical movement against one another, as well as shifting of their relative order, is required to aline the rows in their proper sequence. A simple way of doing this is to write each column on a strip of paper so that it may be slipped or shifted as required. The extra letters appearing at the top and bottom of the columns can then be struck off, or added as required. The surest entry into a system is usually by way of some peculiarity of the system or the message, an example being the appearance of Q's or Z's in the text. There being none in this particular message, entry is sought through an analysis of digraphs produced by column juxtaposition. Of the columns extracted, 1 and 6 contain the least number of letters. Therefore, since possible combinations are limited, either could be used as a starting point. Selecting column 6, it is written vertically:

6
O
H
M
V
M
O
P
L
S
F

(1) Once a column has been selected as a base, the next step is to isolate possible adjacent columns. The problem consists not only of selecting the right column, but also selecting its relative vertical position in respect to the base column. In this process, the vertical relationship of the letters in any given column cannot be disturbed except by moving letters from the top of one column to the bottom of the

preceding column; or, from the bottom of one column to the top of the next succeeding column. The letter *Y* may appear in either columns 1 or 2 in the example above. If in column 1, it must follow *U;* if in column 2, it must precede *I*. Using the table of digraphic frequencies (table A–1), the possible identities of letters lying to the right of column 6 are attempted. The letters *J*, *K*, *Q*, *V*, and *Z* are noted as being rarely combined with other letters to form digraphs. Thus the *V* appearing in the columns represents either the start of a word, the end of a word, or probably a part of one of five common digraphs. If it represents the start of a word, it must still be part of the digraphs listed. Therefore, using this as an initial limitation, those letters which are most often combined with the *V* can be written to the right of it, underlining the letters most often used.

6					
O					
H					
M					
V	$\underline{A}$	*E*	*I*	*O*	*T*
M					
O					
P					
L					
S					
F					

Noting that similar limitations exist in respect to combining letters with *F* and *P* to form digraphs, these letters are also listed:

6						
O						
H						
M						
V	$\underline{A}$	*E*	$\underline{I}$	*O*	*T*	
M						
O						
P	$\underline{A}$	$\underline{E}$	*L*	*O*	*P*	$\underline{R}$
L						
S						
F	*E*	*F*	$\underline{I}$	$\underline{O}$	*T*	

(2) Using these possible combinations as a base, the remaining columns are scanned for these letters occurring at the same relative intervals. With the exception of the letters forming combinations with the letter *V*, only those high-frequency combinations are selected for letters *P* and *F*, leaving the low-frequency combinations open. In some cases, the low-frequency letters form the correct combination. However, it is better to start with the most common combinations; then, if no matches are found, check the low-frequency combinations. Column 1 is set aside immediately as it offers no good combinations. Column 2 contains an *I*, *A*, and *O* sequence in the same relative positions. Therefore, it is considered. Columns 3 and 5 offer nothing; they too, are set aside. Accordingly, columns 6 and 2 are juxtaposed.

6	2	
O		
H		
M	*Y*	(02)
V	*I*	(12)
M	*I*	(09)
O	*L*	(19)
P	*A*	(14)
L	*I*	(27)
S	*E*	(49)
F	*O*	(40)
	E	
	I	

(3) As a check, all digraphs formed by the juxtaposition of the two columns are compared with those listed in the table of digraph frequencies, and are found acceptable as a group, since none are unlikely. If possible word fragments are lacking, and if there are no particular letter combinations which suggest the next letter to be added to any of the digraphs, the next possibility is to attempt to expand the digraphs to trigraphs, using tables B–1 and B–2 as a guide. As trigraphs, with column 6 forming the first letter, only *FOR* or *FOU* appear likely. In the cryptogram, only one *U* appears. Therefore, if *FO* represents the first two letters of the trigraph *FOU*, only column 1 will fit, forming the third letter of the trigraph. Placing column 1 to the right of columns 6 and 2, the pseudo matrix appears.

6	2	1
O		
H		
M	*Y*	*A*
V	*I*	*T*
M	*I*	*T*
O	*L*	*I*
P	*A*	*T*
L	*I*	*N*
S	*E*	*C*
F	*O*	*U*
	E	*Y*
	I	

ING INE
SECOND SECRET SECTION
OUR FOUR FOUND FOUL

(4) Examination of the rows reveals several possible word bits—*SEC* can be expanded to *SECOND*, *SECRET*, *SECTION* and *FOU* to *FOUR*, *FOUND*, *FOUL*. Also considering the digraphs formed by columns 2 and 1, the possible trigraphs *ING* and *INE* are suggested. These possible words and trigraphs offer a means of placing the next column. If the above assumptions are correct, the next adjacent column must contain one of the following sequence of letters, in the order shown:

G	G	G	G	G	G	G	G	G	E	E	E	E	E	E	E	E	E
O	O	O	R	R	R	T	T	T	O	O	O	R	R	R	T	T	T
R	N	L	R	N	L	R	N	L	R	N	L	R	N	L	R	N	L

Checking each column in turn for any of the above sequences, only column 4 contains a proper sequence, that being GTR. Therefore, column 4 is placed next to column 1.

6	2	1	4
O			
H			*E*
M	*Y*	*A*	*C*
V	*I*	*T*	*Y*
M	*I*	*T*	*E*
O	*L*	*I*	*G*
P	*A*	*T*	*R*
L	*I*	*N*	*G*
S	*E*	*C*	*T*
F	*O*	*U*	*R*
	E	*Y*	*N*
	I		*T*
			L

(5) There being only two columns unplaced, the solution is greatly simplified; the columns must fall either in the sequence 3–6–2–1–4–5–3–6 etc., or 5–6–2–1–4–3–5–6–2–1, etc. Establishing which is the correct sequence is done quickly by placing each strip in the possible position in which it might appear, slipping it up and down against the columns previously placed, to look for plaintext. By this method, the following sequence would be quickly discovered:

3	6	2	1	4	5
	O				*R*
O	*H*			*E*	*N*
E	*M*	*Y*	*A*	*C*	*T*
I	*V*	*I*	*T*	*Y*	*L*
I	*M*	*I*	*T*	*E*	*D*
T	*O*	*L*	*I*	*G*	*H*
T	*P*	*A*	*T*	*R*	*O*
L	*L*	*I*	*N*	*G*	*I*
N	*S*	*E*	*C*	*T*	*O*
R	*F*	*O*	*U*	*R*	*H*
E		*E*	*Y*	*N*	*M*
C		*I*		*T*	*V*
Y				*L*	*M*

(6) By rearranging columnar order, not changing the sequence, using column 4 as the starting point, and by striking off the letters duplicated at the top and bottom which were generated in establishing minimum-maximum column lengths, the matrix is reconstructed and thus completes the solution.

4	5	3	6	2	1
E	*N*	*E*	*M*	*Y*	*A*
C	*T*	*I*	*V*	*I*	*T*
Y	*L*	*I*	*M*	*I*	*T*
E	*D*	*T*	*O*	*L*	*I*
G	*H*	*T*	*P*	*A*	*T*
R	*O*	*L*	*L*	*I*	*N*
G	*I*	*N*	*S*	*E*	*C*
T	*O*	*R*	*F*	*O*	*U*
R	*H*	*X*	*X*	*X*	*X*

4-11. (C) A Solution Using Literal Characteristics

a. On occasion a cryptographic text will exhibit an outgrowth of the language used, which will enable the analyst to reach a rapid solution by a less involved process. In the English language for example, the use of the letters X, Q, K, J, and Z is rather limited. Moreover, the use of any of these letters immediately suggests words common to the military.

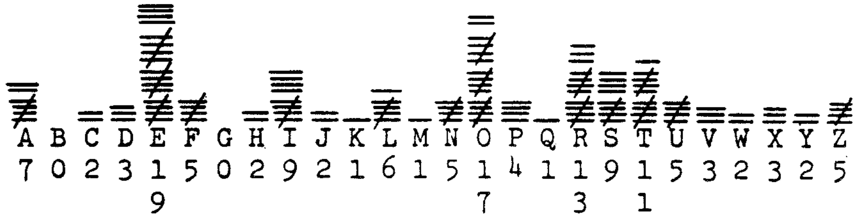
K	Kilo Kilometer Kill KIA
Q	QU as in Request Requisition Quota
J	Juliett, June, July, Junction, Join
X	Xray, Six, Fix, Axis
Z	Zulu Zero

Depending on the service and function of the correspondents, other words of limited use could be found. Similar limitations and associated words are found in all alphabetic languages and give a rather quick entry into a system.

b. Taking one such characteristic, the analyst can move directly into the anagramming stage with reasonable certainty that as the recovery of the plaintext progresses, the matrix and its keys will fall out.

```
VAAEI  TZZMO  HNEUE  APDEF  TOXIL
YNTRT  OORTS  PLORO  ARRON  ECTZL
REEEA  RFAXI  OUTER  OTSEK  JVPPE
ZSDII  IOERE  QOOSJ  EOLSO  SYEIO
WNILN  RORUF  HTUSF  TIFTS  SVUOC
XWEZE  LERRA  DE
```

Examination of the above text reveals a number of low-frequency letters which may be used as an entry into the system. To begin, a frequency distribution is made, see figure 4-5.



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7	0	2	3	19	5	0	2	9	2	1	6	1	5	17	4	1	13	9	11	5	3	2	3	2	5

Figure 4-5 (U). Transposition ciphertext, uniliteral frequency distribution (U).

(1) Any low-frequency letter may be used, but since the *Q* appears only once, it will be used. With the *Q* as a center point, a sequence of letters is withdrawn from the message, the exact number of letters depending upon a presumed approximate size for the matrix. The message contains a total of 137 letters indicating that its dimensions possibly lie in the general area of 10 x 14 to 12 x 12. This is just a guess serving only to place some limitation on the number of letters extracted, and to some degree to duplicate the determination of minimum-maximum column length by decimation. On this basis 13 letters are extracted, 6 preceding and 6 following the letter *Q*, and inscribed vertically to form a column.

```
I
I
O
E
R
E
Q
O
O
S
J
E
O
```

Since there are five U's in the cryptogram, five additional columns (each centered about a U, and of equal length) are now withdrawn from the message and compared individually against column 1. Determination of which column should be paired with column 1 depends on which pair produces the most acceptable digraphs. In this particular case, additional comparative basis is provided by the *J* which also appears in column 1.

(1)	(2)	(3)	(4)	(5)
I Z (02)	*I R* (27)	*I I* (00)	*I O* (41)	*I I* (00)
I M (09)	*I F* (10)	*I L* (28)	*I R* (27)	*I F* (10)
O O (06)	*O A* (07)	*O N* (77)	*O U* (37)	*O T* (19)
E H (07)	*E X* (07)	*E R* (87)	*E F* (17)	*E S* (54)
R N (07)	*R I* (30)	*R O* (28)	*R H* (30)	*R S* (31)
E E (42)	*E O* (12)	*E R* (87)	*E T* (37)	*E V* (20)
Q U (15)	*Q U* (15)	*Q U* (15)	*Q U* (15)	*Q U* (15)
O E (03)	*O T* (19)	*O F* (25)	*O S* (14)	*O O* (06)
O A (07)	*O E* (03)	*O H* (03)	*O F* (25)	*O C* (08)
S P (10)	*S R* (05)	*S T* (03)	*S T* (02)	*S X* (00)
J D (00)	*J O* (02)	*J U* (02)	*J I* (00)	*J W* (00)
E E (42)	*E T* (37)	*E S* (54)	*E F* (18)	*E E* (42)
O F (03)	*O S* (14)	*O F* (25)	*O T* (19)	*O Z* (00)

Initially combinations (1) and (5) can be rejected, as the digraphs produced by the juxtaposition of the columns produce impossibly low-frequency digraphs (frequency shown in parentheses). Combinations (2) and (4) contain a fair number of medium-frequency digraphs. Combination (4) also has the digraph *JI* with a frequency of zero. Combination (3) has several high-frequency digraphs, in addition to a number of medium-frequency digraphs. It also has one with zero frequency, but since it occurs at the top of the column it may not be a true match, not occurring in adjacent rows at all. Of all the combinations (3) offers the best possibilities, and it will be used as a base for further analysis.

(2) Assuming that the selected combination is the correct arrangement, the digraphs can be considered for possible expansion. For example, the digraph *IL* can be expanded to *HILL* or *WILL*, *QU* can be expanded to *QUE*, or *QUI*, and *JU* to *JUN* or *JUL*, all fairly common trigraphs. A column to complete these trigraphs must contain one of the following combinations of letters in rows as shown below:

1	*I I*				
2	*I L*	*L*	*L*	*L*	*L*
3	*O N*				
4	*E R*				
5	*R O*				
6	*E R*				
7	*Q U*	*E*	*E*	*I*	*I*
8	*O F*				
9	*O H*				
10	*S T*				
11	*J U*	*N*	*L*	*N*	*L*
12	*E S*				
13	*O F*				

By starting with the letter which precedes each of the six L's found in the text, the following columns are pulled out quickly.

	1	2	3	4	5	6
1	*Z*	*O*	*I*	*E*	*I*	*P*
2	*L*	*L*	*L*	*L*	*L*	*L*
3	*R*	*S*	*N*	*E*	*Y*	*O*
4	*E*	*O*	*R*	*R*	*N*	*R*
5	*E*	*S*	*O*	*R*	*T*	*O*
6	*E*	*Y*	*R*	*A*	*R*	*A*
7	*A*	*E*	*U*	*D*	*T*	*R*
8	*R*	*I*	*F*	*E*	*O*	*R*
9	*F*	*O*	*H*	*V*	*O*	*O*
10	*A*	*W*	*T*	*A*	*R*	*N*
11	*X*	*N*	*U*	*A*	*T*	*E*
12	*I*	*I*	*S*	*E*	*S*	*C*
13	*O*	*L*	*F*	*I*	*P*	*T*

Of these possible columns, only the second sequence will complete the assumed trigraphs. Therefore, it is placed to the right of the two columns previously placed, which in turn forms a basis for additional anagramming. The placement of the columns, and possible expansions are shown below:

	I	*I*	*O*	
(H/W)	*I*	*L*	*L*	
	O	*N*	*S*	
(Z)	*E*	*R*	*O*	
	R	*O*	*S*	
	E	*R*	*Y*	
(RE)	*Q*	*U*	*E*	(ST)
	O	*F*	*I*	
	O	*H*	*O*	
	S	*T*	*W*	(O)
	J	*U*	*N*	(E/C/)
	E	*S*	*I*	
	O	*F*	*L*	

(3) Once an entry has been made into a transposition system, the complete solution follows rapidly, and in most instances it is merely a mechanical process of making assumptions and then testing their validity by using appropriate frequency tables. Further progress is then made by expanding upon

word fragments. Following this technique the columns shown below could be matched with little trouble.

```
  X I I O F
E W I L L T
C E O N S I
T Z E R O F
Z E R O S T
L L E R Y S
R E Q U E S T
E R O F I V E
E R O H O U R
E A S T W O
A D J U N C T I O N
R E E S I X
    O F L W
          E
```

(4) In addition to the many obvious words and word fragments in the matrix above, evidence also indicates the dimensions of the matrix. Considering the letters in the top row, they can hardly be part of a word in their present sequence, and they are repeats of letters appearing in the bottom row. Therefore, true column length may start in either the first or the second row (in the first row if the repeated letter is located there, or in the second row if the repeated letter falls in the bottom row). Consider also the letter *E* which ends the column starting *XWE*, and which appears as the last letter of the cryptogram. As it ends the cryptogram, it must be the last letter of the column in question. Note also that the *W* which ends the last column of the matrix is also the same *W* that appears in the start *XWE*. Therefore, it must belong to this column and not to the last column of the matrix, the *X* then ending this column. On this basis, there are two column lengths; one of 11 starting with *W* and ending with *E*; the other starting with F and ending with X. Thus the F which ends column *ILNR* must be deleted. The columns ending *WNIL* and that beginning *ILNR* share in common the letters *I* and *L*. This is impossible. If short and long columns are 11 and 12 letters or rows in length, neither column can contain both letters, as they would then be 13 letters long. Therefore, they must be shared between the two, and to preserve the sequence of letters one must end *WSI*, and the other start *LNR*.

(5) Since the cryptogram contains 137 letters, the assumption of long columns of 12 letters and short columns of 11 letters is very good. For example, 12×12=144, 144−137=7, and 12−7=5; therefore, in a matrix with 12 rows and columns in which 137 letters have been inscribed, there will be 5 long columns and 7 short. This can be confirmed by going back to the cryptogram and marking off those sequences used. Also, knowing the length of some columns will serve to isolate additional columns of the correct lengths, speeding the recovery process.

```
VAAEI TZZMO HNEUE APDEF TOXIL
YNTRT OORTS PLORO ARRON ECTSL
REEEA RFAXI OUTER OTSEK JVPPE
ZSDII IOERE QOOSJ EOLSO SYEIO
WNILN RORUF HTUSF TIFTS SVUOC
XWEZE LERRA DE
```

Figure 4–6 (~~C~~). Isolation of columns in ciphertext (U).

Counting the number of unused letters lying between those columns previously extracted, as underlined in figure 4–6, the following combination of column lengths can be established.

First, unused sequence of 45 letters=one 12-row column and three 11-row columns.

Second, unused sequence of 24 letters=two 12-row columns.

Third, unused sequence of one letter must be assigned to either the preceding or following column. Since it is unlikely that the preceding columns could start with *IIOE*, the *O* belongs to the following column making it 12 letters in length.

(6) The assumption as to column length seems valid, but still there are only six identified as to length, three short and three long. An additional bit of information, which will aid in further recovery is that long columns appear on the left and short on the right. Accordingly the columns can be moved, long columns to the left and short columns to the extreme right to maintain word symmetry.

```
O F-------E W I L
L T-------C E O N
S I-------T Z E R
O F-------Z E R O
S T-------L L E R
Y S-------R E Q U
E S-------E R O F
I V-------E R O H
O U-------E A S T
W O-------A D J U
N C-------R E E S
I X
```

(7) Having established the parameters of the matrix, and having placed the columns in their correct sequence, recovery of the remaining columns becomes quite easy, using the same methods previously covered. In this case the many word fragments are readily apparent and measurably aid in the process. The completed matrix appears as follows, the keys being derived by the order in which the columns are extracted from the matrix.

```
   1                   1     1
9  1  6  7  2  4  3  1  5  2  8  0
O  F  F  E  N  S  I  V  E  W  I  L
L  T  A  K  E  P  L  A  C  E  O  N
S  I  X  J  U  L  Y  A  T  Z  E  R
O  F  I  V  E  O  N  E  Z  E  R  O
S  T  O  P  A  R  T  I  L  L  E  R
Y  S  U  P  P  O  R  T  R  E  Q  U
E  S  T  E  D  A  T  Z  E  R  O  F
I  V  E  Z  E  R  O  Z  E  R  O  H
O  U  R  S  F  R  O  M  E  A  S  T
W  O  O  D  T  O  R  O  A  D  J  U
N  C  T  I  O  N  T  H  R  E  E  S
I  X  S  I  X
```

4-12. (~~C~~) Stereotypes and Service Terminology

a. A characteristic of military cryptograms, particularly at the lower echelons, is the presence of stereotypes and characteristic terminology common to military operations. These elements may occur at any position in a message although those at the beginning and the ending are more readily identifiable. These elements may be any of the following types:

(1) Phonetic alphabets.

(2) Ranks, titles, unit designations, and nicknames.

(3) Map reference data, grid coordinates, reference lines, hill numbers, geographic place-names, etc.

(4) Weapons, caliber, short titles, model numbers, etc.

(5) The 24-hour time system when spelled out.

(6) Addressee and signature lines.

(7) Message reference components (such as part one of two parts, reference your message, etc.).

b. These elements may be either spelled out or abbreviated. The above list is not all inclusive. Once the use of specific stereotypes and certain service terminology has been identified, the analyst is provided with an invaluable aid in the solution of cryptograms, particularly in the case of transposition systems. Not only is this of importance in anagramming, but also, in certain instances, the use of stereotypes can lead to the rapid solution of a number of messages simultaneously.

4-13. (~~C~~) Special Solutions

a. On occasion, depending on the security consciousness of the correspondents, a series of messages are enciphered in a transposition system of the same width. If this is coupled with stereotyped beginnings or endings, regardless of whether or not different keys are used, the resulting ciphertext will exhibit a number of similarities which the analyst can quickly exploit. As an example of how these similarities are produced, observe the encipherment shown in figure 4-7.

```
5 1 2 3 4          2 4 1 5 3
R E Q U E          R E Q U E
S T I N F          S T I N F
O R M A T          O R M A T
I O N C O          I O N O N
N C E R N          L O C A T
I N G E N          I O N O F
E M Y A C          C O M M A
T I V I T          N D P O S
Y                  T
```

```
                          Message A

ETROC  NMIQI  MNEGY  VUNAC  REAIE  FTONN  CTRSO  INIET  Y
  A        B           C         D             E

                          Message B

QIMNC  NMPRS  OILIC  NTEFT  NTFAS  ETROO  OODUN  AOAOM  O
  B        E             D           A           C
```

Figure 4-7 (~~C~~). Repeated sequences, cipher message A and B (U).

The repeated sequences that appear in both messages, underlined above, are the result of two factors: stereotyped beginnings and matrices of the same width. Given these two factors, repetition in text will occur as a result of the enciphering process. Additionally, the number of repetitions is determined by the number of columns. The length of the repetition is determined by the number of rows occupied by the stereotype. The sequence in which the repetitions occur in the message are the result of the order of extracting the cryptographic text from the matrix, i.e. the particular key used. Thus, matrix width (number of columns), depth (number of rows), and order of extraction (key sequence) can be found. For example, consider figure 4–8.

```
                               Message A

ASOLI  LBOAE  WDLIR  ACIEL  NSAIR  IEDLS  NDWND  TQNIH  UAOTL  FMLIF
  1              2                    3              4               5
AMPES  DBREU  SCEPV  NELOM  YEODC  SHCAI  TIELT  MNAEE  IDERA
                6                   7                  8

                               Message B

QNILB  TSROI  RRIEP  LIHUE  OZYAS  OLSUT  ARZEO  LTMUI  MTQBR  OAUSC
  1             2                     3             4                5
IEEHT  RXOLI  RSWBO  DSERD  EODPL  TIAFS  EIFAE  SDEEE  ZT
               6                   7              8
```

Figure 4–8 (~~C~~). *Stereotypes as repeated sequences* (*U*).

(1) Each cryptogram contains 8 sequences which are repeated in the other. Therefore, 8 columns can be assumed, each repetition marking the beginning of a column.

(2) Message A contains 95 letters; as 8×12=96, we assume a matrix depth of 12 rows containing seven columns of 12 letters and one column of 11 letters, the column beginning with IFA. Being the shortest column, it must appear at the right of the matrix.

(3) Message B contains 92 letters; as 8×12=96, we assume again a depth of 12 rows, four columns of 12 letters, and four columns of 11 letters.

(4) All repeated sequences, with the exception of *ASOL* are of the same length. As the longer columns of an incompletely filled rectangle occur on the left, the column beginning with *ASOL* is placed to the left.

(5) As the repeats do not appear sequential in both messages, a different key has been used in each case.

(6) The keys, which determine the order of extraction of the column from the matrix, are reflected by the order of the repeats in each message.

(7) Row sequence, i.e. the order of the letters across the matrix, are similar in both matrices for the stereotype; therefore, a column placement of 1 in one matrix can be applied to that column exhibiting the same repeat in the other matrix.

b. With these generalities, two matrices can be constructed as follows, one for each message:

```
A                 B
A - - - - - - I   A - - - - - - I
S             F   S             F
O             A   O             A
L             M   L             E
I             P   S             S
L             E   U             D
B             D   T             E
O             D   A             E
A             B   R             E
E             R   Z             Z
W             E   E       - - - T
D - - - - -       O - -
```

With the parameters of the matrices established, anagramming can be commenced playing the recovery of one column's placement against the placement of columns in the other matrix. The two columns of each message that start with a *Q* and *U* respectively can be withdrawn and paired:

A		B	
Q	*U*	*Q*	*U*
N	*S*	*N*	*S*
I	*C*	*I*	*C*
H	*E*	*L*	*I*
U	*P*	*B*	*E*
A	*V*	*T*	*E*
O	*N*	*S*	*H*
T	*E*	*R*	*T*
L	*L*	*O*	*R*
F	*O*	*I*	*X*
M	*M*	*R*	*O*
L	*Y*		

The digraphs formed by pairing the columns appear valid, and can be placed in the matrices. Examination of matrix B shows only 3 columns of 11 letters remaining. Therefore, the pair above for matrix B must fit in two of those three spaces. Also, message B contains only 1 remaining column of 11 letters, that beginning with the repeated sequence *EOD*, which means that these three columns must be joined. Considering the letters available, the sequence *EQUI* appears to be better than the sequence *QUEI*. As the first row, therefore, it is placed in matrix B. Since the column placement found for one matrix can be applied to the other, the same columns that start with the same repeated letters are also placed in matrix A, producing the following matrices. At this time, key values are also assigned to each matrix in the order of its column's appearance in the message.

A

1	- - - -	7	4	6	5
A		*E*	*Q*	*U*	*I*
S		*O*	*N*	*S*	*F*
O		*D*	*I*	*C*	*A*
L		*C*	*H*	*E*	*M*
I		*S*	*U*	*P*	*P*
L		*H*	*A*	*V*	*E*
B		*C*	*O*	*N*	*S*
O		*A*	*T*	*E*	*D*
A		*I*	*L*	*L*	*B*
E		*T*	*F*	*O*	*R*
W		*I*	*M*	*M*	*E*
D		*E*	*L*	*Y*	

B

	- - - -	7	1	5	8
A		*E*	*Q*	*U*	*I*
S		*O*	*N*	*S*	*F*
O		*D*	*I*	*C*	*A*
L		*P*	*L*	*I*	*E*
S		*L*	*B*	*E*	*S*
U		*T*	*T*	*E*	*D*
T		*I*	*S*	*H*	*E*
A		*A*	*R*	*T*	*E*
R		*F*	*O*	*R*	*E*
Z		*S*	*I*	*X*	*Z*
E		*E*	*R*	*O*	*T*
O					

c. Using familiar anagramming techniques to place one column in one matrix, and then transferring its location to the other matrix, both messages can readily be solved, resulting in the recovery of the following matrices:

A

1	2	8	3	7	4	6	5
A	*L*	*L*	*R*	*E*	*Q*	*U*	*I*
S	*I*	*T*	*I*	*O*	*N*	*S*	*F*
O	*R*	*M*	*E*	*D*	*I*	*C*	*A*
L	*A*	*N*	*D*	*C*	*H*	*E*	*M*
I	*C*	*A*	*L*	*S*	*U*	*P*	*P*
L	*I*	*E*	*S*	*H*	*A*	*V*	*E*
B	*E*	*E*	*N*	*C*	*O*	*N*	*S*
O	*L*	*I*	*D*	*A*	*T*	*E*	*D*
A	*N*	*D*	*W*	*I*	*L*	*L*	*B*
E	*S*	*E*	*N*	*T*	*F*	*O*	*R*
W	*A*	*R*	*D*	*I*	*M*	*M*	*E*
D	*I*	*A*	*T*	*E*	*L*	*Y*	

B

3	6	4	2	7	1	5	8
A	*L*	*L*	*R*	*E*	*Q*	*U*	*I*
S	*I*	*T*	*I*	*O*	*N*	*S*	*F*
O	*R*	*M*	*E*	*D*	*I*	*C*	*A*
L	*S*	*U*	*P*	*P*	*L*	*I*	*E*
S	*W*	*I*	*L*	*L*	*B*	*E*	*S*
U	*B*	*M*	*I*	*T*	*T*	*E*	*D*
T	*O*	*T*	*H*	*I*	*S*	*H*	*E*
A	*D*	*Q*	*U*	*A*	*R*	*T*	*E*
R	*S*	*B*	*E*	*F*	*O*	*R*	*E*
Z	*E*	*R*	*O*	*S*	*I*	*X*	*Z*
E	*R*	*O*	*Z*	*E*	*R*	*O*	*T*
O	*D*	*A*	*Y*				

d. The methods of solving cryptograms enciphered by matrices of the same width, but where the stereotypes occur in the endings of the messages, are the same as those given above. The only difference is that since the repetitions occur in the last few rows of the matrices, the analyst deals with column endings rather than the beginnings of each column. All other conditions being equal, the analyst need only anagram using the bottom row rather than the top using essentially the same techniques as given for message beginnings.

4–14. (~~C~~) Solution of Messages of Identical Length

a. When several messages of identical length have been enciphered using the same key, implying an equal width matrix, a solution can be obtained without recourse to stereotypes or literal patterns by using a process known as multiple anagramming. In this process, the anagramming is applied across several messages, rather than attempting to recover the individual columns of each message. This process is predicated on the premise that the letters of two or more messages which occur in the same relative position in a given matrix will undergo exactly the same change in position.

b. Also used in this process are the characteristics of a progressive key. A progressive key is a series of numbers which correspond to the sequence in which letters can be extracted from a transposition cipher in order to read plaintext. The key may be divided into sections or sequences of numbers, each corresponding to a row of the matrix used to produce the cipher, and each bearing a definite relationship to other sequences. This relationship is exhibited by a one-digit difference between the numeric values of each sequence; the difference being minus for a preceding sequence and plus for a succeeding sequence. Figure 4–9 illustrates this concept. The matrix contains both numbers and letters, the former corresponding to the sequence of extraction, and the latter to the plaintext.

1	4	2	5	3	6
A 1	*R* 15	*T* 6	*I* 20	*L* 11	*L* 24
E 2	*R* 16	*Y* 7	*F* 21	*I* 12	*R* 25
E 3	*H* 17	*E* 8	*A* 22	*V* 13	*Y* 26
I 4	*N* 18	*Z* 9	*O* 23	*N* 14	*E* 27
O 5	*N* 19	*E* 10			

Figure 4–9 (~~C~~). *Row sequences in a progressive key* (*U*).

c. The cipher text extracted in normal key sequence will appear as:

AEEIO TYEZE LIVNR RHNNI FAOLR YE

To reflect the sequence caused by the extraction process, the analyst could assign numerical values to each letter of the message in its order of appearance:

A	*E*	*E*	*I*	*O*	*T*	*Y*	*E*	*Z*	*E*	*L*	*I*	*V*	*N*	*R*	*R*	*H*	*N*	*N*	*I*	*F*	*A*	*O*	*L*	*R*	*Y*	*E*
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

Plaintext could be read from this sequence of letters by using the progressive key:

1–15–6–20–11–24–2–16–7–21–12–25
3–17–8–22–13–26–4–18–9–23–14–27
5–19–10

Note that the progressive key is only a repeat of row sequences, each section of the key corresponding to a row of the matrix. The origin of the progressive key lies in the horizontal inscription of plaintext followed by the vertical transcription to form ciphertext.

d. The relationship of each sequence of the progressive key is such that if the two letters represented by key values 15–6 could be anagrammed in one sequence, one could logically assume the juxtaposition of 16–7 and 17–8. Although a valuable tool, this process does have some limitations. By continued generation of possible juxtaposition, one could lap over into another sequence of the progressive key. For example, a continued expansion of the key values 15–6 would soon produce the juxtaposition of values 20–11; but note that 20–11 appears in the first sequence. In this case it just happens that they, too, are juxtaposed, but quite often they are not associated in any manner. Therefore, juxtaposition by expansion is not always infallible. As anagramming progresses, changes are sometimes required. Within limits, anagramming is very useful.

e. Using this technique, the initial step in the solution of a number of messages is to superimpose the messages and assign to each column so formed, a number in the normal sequence, as follows:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
L	*P*	*Q*	*R*	*Y*	*T*	*T*	*L*	*P*	*U*	*A*	*R*	*R*	*S*	*I*	*U*	*E*	*D*	*E*	*O*	*E*	*T*	*S*	*R*	*E*	Message A
Q	*S*	*N*	*E*	*T*	*B*	*B*	*U*	*H*	*B*	*H*	*R*	*S*	*M*	*D*	*R*	*E*	*D*	*A*	*A*	*O*	*A*	*E*	*E*	*E*	Message B
A	*O*	*E*	*E*	*W*	*O*	*V*	*G*	*U*	*C*	*M*	*T*	*N*	*I*	*S*	*F*	*R*	*D*	*E*	*R*	*E*	*S*	*O*	*T*	*E*	Message C
I	*O*	*O*	*O*	*E*	*O*	*D*	*N*	*R*	*N*	*N*	*N*	*P*	*O*	*H*	*T*	*T*	*Y*	*G*	*E*	*T*	*T*	*W*	*R*	*A*	Message D
J	*N*	*U*	*O*	*T*	*E*	*K*	*U*	*F*	*R*	*R*	*C*	*V*	*A*	*D*	*O*	*O*	*N*	*N*	*I*	*T*	*A*	*I*	*F*	*A*	Message E

Anagramming is started using any element of any row, each representing a message; and since each is inherently similar in respect to the movement of the individual letters, the process is applied to all other letters in the same column. Consequently, selecting the *Q* and *U* columns, 1 and 8 of message B, as point of departure, they may be juxtaposed and expanded as follows, carrying along all other elements of columns:

1–8	2–9	3–10	4–11	5–12
L L	P P	Q U	R A	Y R
Q U	S H	N B	E H	T R
A G	O U	E C	E M	W T
I N	O R	O N	O N	E N
J U	N F	U R	O R	T C

Although the above anagrams give two doublets (*LL* and *PP*), generally they are acceptable and the process may be continued. It is at this stage that the relationship between segments of a progressive key come into play, for any column selected for a given pair should produce, by adding or subtracting one to its number, a column that can be anagrammed to the other columns. Thus, column 17 is juxtaposed to columns 1–8, columns 18, 19, 20, and 21 could be anagrammed with the pairs 2–9, 3–10, 4–11, and 5–12. The following diagram, illustrating the foregoing expansion of one sequence of a progress key, shows how it may serve as a check on the analyst's assumption.

(1)	(2)	(3)	(4)	(5)
1 - 8 -17	2 - 9–18	3 - 10–19	4 - 11–20	5 - 12–21
L L E	P P D	Q U E	R A O	Y R E
Q U E	S H D	N B A	F H A	T R O
A G R	O U D	E C E	E M R	W T E
I N T	O R Y	O N G	O N E	E N T
J U O	N F N	U R N	O R I	T C T

f. Further study of the message reveals that column 19 could be anagrammed to columns 1–8; to check this assumption and to generate additional anagrams, all segments of the key are expanded and juxtaposed:

(1)	(2)	(3)	(4)	(5)
1 - 8 -19	2 - 9 -20	3 - 10–21	4 - 11–22	5 - 12–23
L L E	P P O	Q U E	R A T	Y R S
Q U A	S H A	N B O	F H A	T R E
A G E	O U R	E C E	E M S	W T O
I N G	O R E	O N T	O N T	E N W
J U N	N F I	U R T	O R A	T C I

The trigraphs generated by the juxtaposition of the columns above appear to be valid, except those of the last segment, particularly the trigraphs *YRS* and *TCI*. For the moment, rather than rejecting them, it would be best to work with those showing the better combinations, in this case segments 1, 2, and 3. Note that *QU* in the first and third segments are now followed by an *A* and *E* respectively which are likely combinations. If they are valid, then because of the relationship between sequences, segment 2 must also be valid. Scanning all remaining columns in the message, including those just rejected, column 12 seems a likely candidate for matching to the sequence 1–8–19. Inscribing those columns the following combination is found:

1 - 8 -19 -12
L L E R
Q U A R
A G E T
I N G N
J U N C

By placing columns 13 and 14 to the second and third sequences, the following combinations are derived:

2 - 9 - 20–13	3 - 10–21–14
P P O R	Q U E S
S H A S	N B O M
O U R N	E C E I
O R E P	O N T O
N F I V	U R T A

As several word fragments are now quite plain (artillery, requested, headquarters, received, five), the recovery of all the plaintext can be affected easily, still generating additional portions of each sequence on the basis of anagramming a single column to one sequence. When completed, the messages and accompanying progressive key would appear as:

1		2	1			1	1		2	1			2	1		2	1		1	2	1		2	1
1	4	2	5	1	8	9	2	5	3	6	2	9	0	3	6	4	7	3	0	1	4	7	5	8
A	*R*	*T*	*I*	*L*	*L*	*E*	*R*	*Y*	*S*	*U*	*P*	*P*	*O*	*R*	*T*	*R*	*E*	*Q*	*U*	*E*	*S*	*T*	*E*	*D*
H	*E*	*A*	*D*	*Q*	*U*	*A*	*R*	*T*	*E*	*R*	*S*	*H*	*A*	*S*	*B*	*E*	*E*	*N*	*B*	*O*	*M*	*B*	*E*	*D*
M	*E*	*S*	*S*	*A*	*G*	*E*	*T*	*W*	*O*	*F*	*O*	*U*	*R*	*N*	*O*	*T*	*R*	*E*	*C*	*E*	*I*	*V*	*E*	*D*
N	*O*	*T*	*H*	*I*	*N*	*G*	*N*	*E*	*W*	*T*	*O*	*R*	*E*	*P*	*O*	*R*	*T*	*O*	*N*	*T*	*O*	*D*	*A*	*Y*
R	*O*	*A*	*D*	*J*	*U*	*N*	*C*	*T*	*I*	*O*	*N*	*F*	*I*	*V*	*E*	*F*	*O*	*U*	*R*	*T*	*A*	*K*	*E*	*N*

g. Nothing now remains to be done except to recover the numeric key used in extracting the columns from the matrix. Since the progressive keys reflect columnar and row order, they are used for this purpose. By setting them down to show their row and columnar sequence, the following matrix and keys can be recovered, see figure 4–10.

11	4	22	15	1	8	19
12	5	23	16	2	9	20
13	6	24	17	3	10	21
14	7	25	18			

4	2	7	5	1	3	6
11	4	22	15	1	8	19
12	5	23	16	2	9	20
13	6	24	17	3	10	21
14	7	25	18			

Figure 4–10 (~~C~~). Recovered matrix and keys (U).

CHAPTER 6 (C)

GRILLE TRANSPOSITION SYSTEMS

Section I. (C) GENERAL

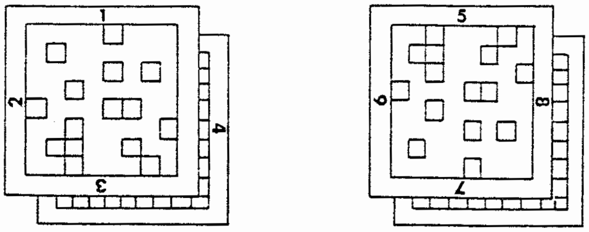
6–1. U (~~C~~) Cryptographic Grilles

a. Grille systems are basically transposition systems which involve the use of two elements, a thin material in which perforations have been made according to a definite pattern, and a matrix, usually of ruled paper, of the same dimensions as the grilles. The grille placed over the matrix serves to uncover its cells in a systematic order, thus providing space for the insertion or extraction of letters, groups of letters, or entire words of the plaintext, thereby generating ciphertext.

[redacted]

6–2. (C) Simple Grilles

a. These consist usually of a square in which perforations have been cut in prearranged positions. When the grill is superimposed upon the matrix, the apertures disclose cells of the matrix. There are eight possible positions in which the grilles may be placed upon the matrix as shown in figure 6–1.



ROTATE THRU FOUR POSITIONS (1-4)

REVERSE AND ROTATE THRU FOUR POSITIONS (5-8)

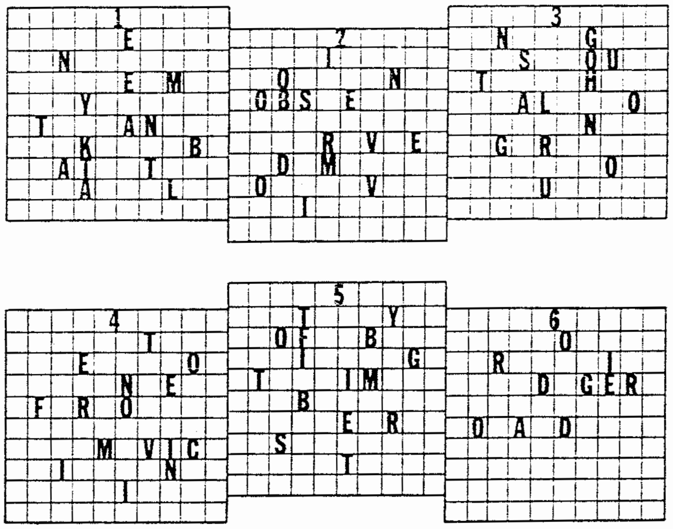
Figure 6–1 (~~C~~). Simple cryptographic grille (U).

In encrypting a message, the grille is placed upon the matrix in one of the eight possible positions. The letters of the plaintext then are inscribed in the open cells, following any prearranged route. The grille is then removed and a ciphertext produced by transcribing the letters, again following any prearranged route.

b. If the number of letters of the plaintext exceed the capacity of the grille, the process is continued on a fresh matrix, this time the grille being placed on the matrix at its next position. Thus by repeatedly using fresh matrices and progressively repositioning the grille, the entire message is encrypted. The several sections of the cipher letter, resulting from each grille placement on successive matrices, merely follow one another in the final cryptogram. In this manner it is only necessary for the correspondents to agree upon the initial position of the grille and its successive positions or placement. The example in figure 6–2 depicts a method of using the simple grille to encipher a message.

Plain text message.

```
ENEMY TANK BATTALION OBSERVED MOVING SOUTH
ALONG ROUTE ONE FROM VICINITY OF BIG TIMBERS
TO RIDGE ROAD.
```



Encrypted Text.

```
TNAYK TAEEA NTMLB OOOBD SIIRM EVVNE TNGSA
LRUGO HNUOO FIERM NOITV EINOC TOSTF IBIET
BNYRG ORADO EGIER
```

Figure 6–2 (~~C~~). Use of simple cryptographic grille (U).

PART THREE (~~C~~)

MONOGRAPHIC SUBSTITUTION SYSTEMS

CHAPTER 7 (~~C~~)

UNILITERAL MONOALPHABETIC SUBSTITUTION SYSTEMS USING STANDARD CIPHER ALPHABETS

Section I. (~~C~~) BASIS OF SUBSTITUTION SYSTEMS

7-1. (~~C~~) General

a. The methods of cryptography to be covered in this part differ from those previously presented in which the plaintext elements are transposed, but always retain their identity. In substitution systems the elements or textual units composing the original plaintext retain their relative position, one to the other, but not their identities. Cipher elements replace, or are substituted for plaintext and for this reason, these systems are called substitution. They may deal with individual letters, combinations of letters, or even words and sentences. When the cryptographic process deals with single letters, or combinations less than words and sentences, the system is termed a substitution cipher system. When the process involves primarily the treatment of whole words, phrases, and sentences, the system is known as a code system.

b. The differentiation of systems, basically similar in that a cryptogram is produced by substituting one value for another, may seem somewhat arbitrary. However, the difference in the length of the elements directly affects the manipulation process of cryptography. Generally, the smaller the element, the better it lends itself to complex manipulation. Substitution systems are also further classified by the number of alphabets involved, and by the number of elements used and manipulated from each alphabet. A detailed definition of common substitution systems is found in paragraph 1-12*a*.

c. A fundamental characteristic of monoalphabetic substitution, the first substitution system to be considered, is that each individual plaintext unit, one character or a number of characters, is always represented by the same cipher unit, again one or a number of characters. This rigid rule is one of the inherent weaknesses of this class of system, for cipher units must inevitably occur with the frequency of use of the plaintext equivalents, and analysis of the system is thereby greatly simplified.

7-2. (U) Nature of Alphabets

a. In the study of cryptanalytics, the dual nature of the alphabet becomes apparent. In order to write a polysyllabic language with facility, it is necessary to establish and maintain, by common agreement or convention, a national equivalency between two sets of elements, a set of elementary sounds, and a set of elementary symbols to represent the sounds. Theoretically, in an ideal alphabet, each symbol or letter denotes only one elementary sound, and each elementary sound is invariably represented by the same symbol.

b. The English language is written by means of 26 simple symbols or letters which, taken together and considered in a sequence, constitute the alphabet of the language. The Dutch and German alphabets are similar in length, French has 25 characters, Italian has 27, and Russian has 31. Not all systems of writing are of this nature. Chinese writing is composed of about 44,000 complex characters, each representing one sense of a word. Japanese writing has a syllabary consisting of 72 syllabic sounds, which can be expressed by 48 characters, singly and in combination.

c. Written plain language consists of words, i.e. combinations and permutations of the letters of the alphabet which represent visually, and call forth vocally, the elementary speech sounds of which the spoken language is composed. In the case of polysyllabic alphabetic languages, the principles on which substitution ciphers rest may be applied in all cases. In the encipherment of the Japanese and Chinese languages, these principles cannot apply directly to the language. They first require a conversion to other values that can be understood. This method of conversion and its implications will be demonstrated in future chapters.

7–3. (~~C~~) Normal and Cipher Alphabets

a. Good cryptography demands that there exist at all times a definite relationship between the plaintext and the cipher values. How this relationship is developed is determined by the particular system, but if it does not exist and is not constant, decryption of the message enciphered by that system is an impossibility. This relationship is brought about by the construction of a cipher alphabet. The primary difference between a cipher alphabet and a normal alphabet is that in the former the elementary speech sounds are represented by characters other than those used in the normal alphabet. There is no real limitation other than practicability on what these characters may be. They may be letters, figures, signs, symbols, or even a combination of any one of these.

b. A cipher alphabet is an ordered arrangement of the letters of a written language and the characters which replace them in the cryptographic process of substitution. It consists of two components, a plain component and a cipher component. The plain component is the normal alphabet of that language, in which the letters of the plaintext are found. The cipher component is the sequence of characters from which the cipher equivalents are drawn. For brevity and for clarity, a letter of the plain component is designated by suffixing a small "p" to it, and a letter of the cipher component designated by suffixing a small "c" to it. Thus Ap means A of the plaintext, and *Xc* means *X* of the ciphertext. The expression Ap=*Xc* means that A of the plaintext, or plain component, is represented by *X* in the ciphertext, or cipher component.

7–4. (~~C~~) Standard and Mixed Cipher Alphabets

a. The plain component of a cipher alphabet is a normal alphabetical sequence, an alphabet where letters represent their commonly associated speech sounds and which appear in their normal order. This normal sequencing of the plain component is the norm. If the plain component is omitted, it is understood to be the normal sequence. The sequence of the cipher component, which may be either standard or mixed, determines the classification of the cipher alphabet.

b. Standard cipher alphabets are those alphabets in which the cipher sequence is the same as the normal sequence. For obvious reasons, a standard cipher alphabet must eithe be reversed in direction or shifted from its normal point of coincidence with the plain component; otherwise, Ap would equal *Ac* and all succeeding letters would equal themselves.

c. Mixed cipher alphabets are those alphabets in which the cipher component no longer demonstrates the normal sequencing in part or in whole. Rather it is disarranged by either some systematic process, an example of which will be treated later, or is generated by some arbitrary and unmethodical process which results in a completely random sequence.

Section II. (~~C~~) UNILITERAL MONOALPHABETIC SUBSTITUTION

7–5. (~~C~~) Standard Cipher Alphabets

a. If a message is enciphered, letter for letter, by using one cipher component, the resulting cryptogram is said to be enciphered by a uniliteral (one-unit) monoalphabetic (one-cipher alphabet) cipher. A standard cipher alphabet used for this purpose is of two types, a direct standard or a reversed standard. In direct standard alphabets, both the plain and the cipher sequence are normal alphabets, i.e., letters follow one another in normal sequence and are individual from left to right. Only their points of coincidence are shifted to the right or left of the normal point of coincidence.

Example:

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*

Key Ap=*Vc*.

b. Reversed standard cipher alphabets also contain normal plain and cipher sequences except the latter sequence is inscribed backward, from right to left.

Example:

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	*O*	*N*	*M*	*L*	*K*	*J*	*I*	*H*	*G*	*F*	*E*	*D*	*C*	*B*	*A*	*Z*	*Y*	*X*	*W*	*V*	*U*	*T*	*S*	*R*	*Q*	*P*

Key Ap=*Oc*.

c. Because of the difference in the direction of the sequence in the two alphabets, the number of possible cipher alphabets produced by each method differs. Where direct standard cipher alphabets of 26 characters are moved against one another, there are only 25 combinations which are different, the 26th being a repeat of the first, i.e. Ap=*Ac*. In reverse standard cipher alphabets, the number of possible combinations equals the number of letters in the alphabet, as the direction of the sequences provides no one point of coincidence where the whole alphabets are exactly the same.

7–6. ~~(C)~~ Reciprocity of Standard Alphabets

a. The reversed standard cipher alphabet illustrated above is also a reciprocal alphabet, i.e. the equivalents show reciprocity and are reversible in pairs. For example, Ap=*Oc* and *Ac*=Op, but note also that Hp=*Hc* and Up=*Uc*. The reciprocity, and the identities shown, are a result of the method by which it was formed. Reciprocal alphabets may be formed by juxtaposing two alphabetic sequences which are identical, but which run in different directions. The occurrence of equal identities is dependent upon the point of juxtaposition. In the alphabet above, *Ac* coincides with Op, the 15th letter of the alphabet. In the example below note that *Ac* is moved to a point below Pp. Further note that equal identities no longer occur.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	*P*	*O*	*N*	*M*	*L*	*K*	*J*	*I*	*H*	*G*	*F*	*E*	*D*	*C*	*B*	*A*	*Z*	*Y*	*X*	*W*	*V*	*U*	*T*	*S*	*R*	*Q*

Juxtaposition at every second interval produces two equal identities, and juxtaposition at even intervals does not produce identities. Note also that the two identities occur at an interval of 13 letters. Both of these numbers, 2 and 13, may be recognized as the factors of the number of letters in the English alphabet (26). Other alphabets of different length also exhibit this characteristic, the points of juxtaposition producing identities and the distances between identities determined by their factors.

b. A reciprocal alphabet which provides complete reciprocity and no identities may be produced in one of two ways:

(1) By arbitrarily constructing a reciprocal alphabet by the random assignment of values in pairs. For example, Ap is made to equal *Kc*: then Kp is made to equal *Ac*. In such an alphabet, the two components thus constructed cannot be slid against one another to produce additional reciprocal alphabets.

(2) By juxtaposing a sequence of an even number of characters against the same sequence shifted exactly halfway to the right or left as below.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
             ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Key Np=*Ac*
Ap=*Nc*

c. Reciprocal alphabets are inverse alphabets, since they may serve either as enciphering or deciphering alphabets.

7–7. ~~(C)~~ Method of Encipherment and Decipherment

a. When a message is enciphered using a uniliteral monoalphabetic substitution system, one plaintext value is replaced by one ciphertext value. For example, using the cipher alphabet of paragraph 7–5*a*, the following message can be enciphered (fig. 7–1):

```
Message:  LISTENING POSTS REPORT TANK MOVEMENT

Enciphering alphabet:  Ap - Vc

P   A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
C   V W X Y Z A B C D E F G H I J K L M N O P Q R S T U

Letter for letter encipherment:

     LISTENING POSTS REPORT TANK MOVEMENT
     GDNOZIDIB KJNON MZKJMO OVIF HJQZHZIO

Cipher text rearranged into five-letter groups, indicator

and nulls added:

     ZYZYZ GDNOZ IDIBK JNONM ZKJMO OVIFH JQZHZ IOXXX
```

Figure 7–1 (*C*). *Monoalphabetic encipherment* (*U*).

b. The procedure for decipherment is the reverse of encipherment. Using the indicator, the cryptographer constructs the cipher alphabet, and since it is nonreciprocal, he rearranges it on the cipher sequence for ease in deciphering.

Deciphering alphabet:

C	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
P	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

The message deciphered:

GDNOZ IDIBK JNONM ZKJMO OVIFH JQZHZ IO
LISTE NINGP OSTSR EPORT TANKM OVEME NT

Message rewritten into word length:

LISTENING POSTS REPORT TANK MOVEMENT

7–8. (~~C~~) Use of Monoalphabetic Ciphers

a. Because of the extreme simplicity of uniliteral monoalphabetic substitution in general, and direct or reversed standard cipher alphabet in particular, its use for practical purposes is quite limited. Solution of these systems is generally very easy, involving two basic methods of analysis, one based entirely upon a frequency distribution and the other based upon a quicker mechanical process. The analysis and solution of messages enciphered by mixed-cipher sequences may be somewhat involved and tedious, but not impossible. Again, the practical use of this type monoalphabetic substitution is also limited.

b. For the cryptanalyst, the study of these systems is important not from the likelihood that he will encounter them in use, but from the basic techniques and skills he will acquire. Moreover, the basic principles of the operation of the system, and the method of its analysis, are incorporated and expanded in the more advanced and complicated manual systems he may encounter.

Section III. (~~C~~) SOLUTION OF UNILITERAL MONOALPHABETIC CIPHERS USING STANDARD CIPHER ALPHABETS

7–9. (~~C~~) Basis for Solution Using a Uniliteral Frequency Distribution

a. The solution of uniliteral monoalphabetic ciphers where standard alphabets are used follows directly from two factors.

(1) The fundamental characteristic is the one-for-one substitution.

(2) The sequence of the letters of the cipher component is merely displaced if it is a direct standard or, if it is a reversed standard, it is reversed and displaced. Because of this, a uniliteral frequency distribution of a cryptogram produced by standard cipher components will show crests and troughs whose relative spatial position and vertical

dimensions will be the same as a uniliteral frequency distribution for the plaintext of that cryptogram.

b. If the cryptogram was enciphered by a reversed standard alphabet there will be one exception to the exact spatial correspondence between the two frequency distributions. That is, the progression of the successive peaks and troughs will be in opposite directions. To observe this, note the plaintext messages and their accompanying cipher alphabets, cryptograms, and uniliteral frequency distributions in figures 7-2 and 7-3.

(1) Encipherment by a direct standard cipher alphabet.

Message:

ENEMY ATTACKING ALONG ROUTE ONE WITH ESTIMATED INFANTRY BATTALION SUPPORTED BY TANKS FORWARD POSITIONS OVERRUN REQUEST IMMEDIATE REINFORCEMENT

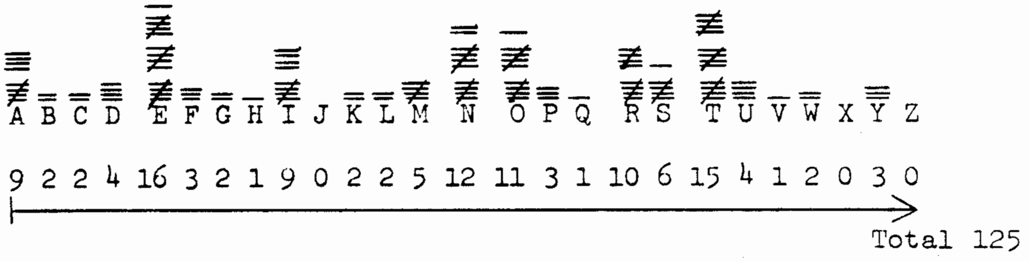
Direct standard cipher alphabet: Ap = *Tc*

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*

Ciphertext:

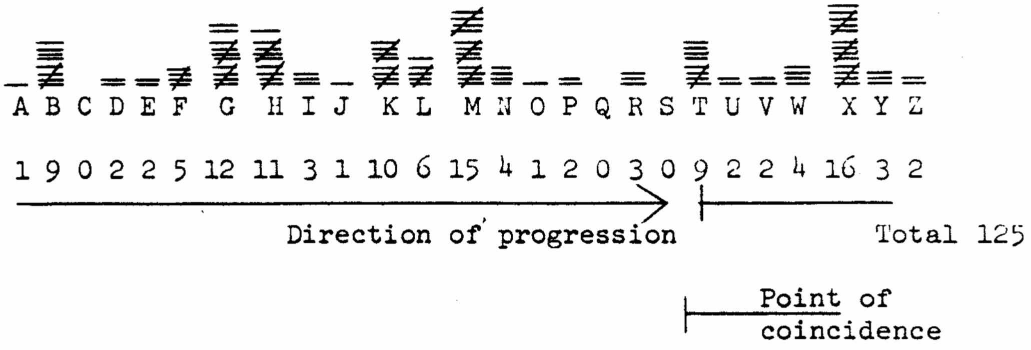
```
X G X F R   T M M T V   D B G Z T   E H G Z K   H N M X H   G X P B M
A X L M B   F T M X W   B G Y T G   M K R U T   M M T E B   H G L N I
I H K M X   W U R M T   G D L Y H   K P T K W   I H L B M   B H G L H
O X K K N   G K X J N   X L M B F   F X W B T   M X K X B   G Y H K V
X F X G M
```

Uniliteral frequency distribution - plaintext:



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
9	2	2	4	16	3	2	1	9	0	2	2	5	12	11	3	1	10	6	15	4	1	2	0	3	0

Uniliteral frequency distribution - ciphertext:



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	9	0	2	2	5	12	11	3	1	10	6	15	4	1	2	0	3	0	9	2	2	4	16	3	2

Figure 7-2 (U). Encipherment by a direct standard cipher alphabet (U).

(2) Encipherment by a reversed standard cipher alphabet.

Message:

TANK COMPANY MOVING UP IN SUPPORT HOLD THE PRESENT POSITION
AFTER ONE SIX ZERO ZERO DISENGAGE AND FALL BACK ON BLOCKING
POSITION AS SITUATION PERMITS

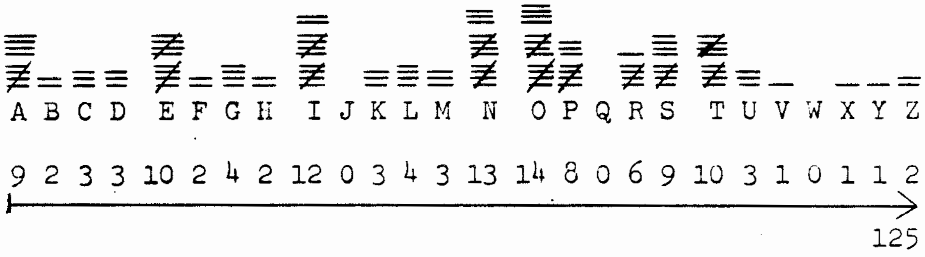
Reversed standard cipher alphabet: Ap = *Mc*

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	*M*	*L*	*K*	*J*	*I*	*H*	*G*	*F*	*E*	*D*	*C*	*B*	*A*	*Z*	*Y*	*X*	*W*	*V*	*U*	*T*	*S*	*R*	*Q*	*P*	*O*	*N*

Ciphertext:

TMZCK YAXMZ OAYRE ZGSXE ZUSXX YVTFY BJTFI
XVIUI ZTXYU ETEYZ MHTIV YZIUE PNIVY NIVYJ
EUIZG MGIMZ JHMBB LMKCY ZLBYK CEZGX YUETE
YZMUU ETSMT EYZXI VAETU

Uniliteral frequency distribution - plaintext:



Uniliteral frequency distribution - ciphertext:

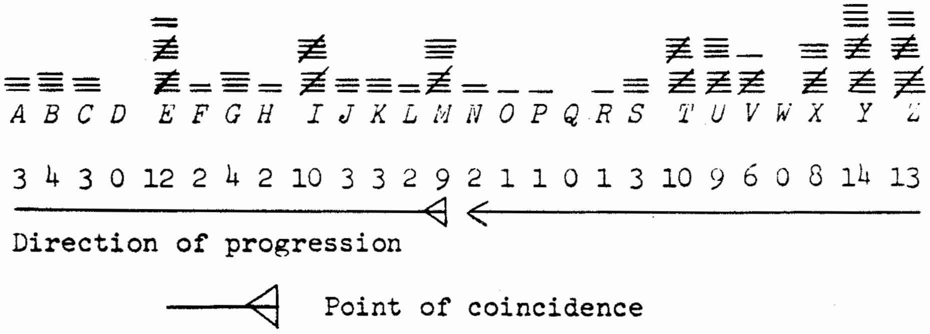


Figure 7–3 (*C*). *Encipherment by a reversed standard alphabet* (*U*).

c. In the preceding examples, several points should be noted. The spatial relationship of peaks and troughs within either cipher component remains constant, differing in the points of coincidence and the different directions in which the order of their progression may lie, relative to the plain components. These differences are purely mechanical, due only to the point at which the alphabets are juxtaposed and the direction of their inscription. Another difference, which will be shown only when the frequency distribution of the ciphertext is compared to an expected normal uniliteral frequency distribution, is that a variation in the order of the high-frequency letters occurs. This is a result of the construction of the plaintext and in no way invalidates the frequency distribution or its use.

7-10. (~~C~~) System Identification and Recovery of The Cipher Alphabet

a. In practice, the identification of a given cryptographic system as being uniliteral monoalphabetic substitution, based on a direct standard cipher alphabet and the recovery of the plaintext values of the cipher sequence of that alphabet, involves one and the same process, based upon the characteristics of standard cipher alphabets and the normal uniliteral frequency distribution. A frequency distribution made of a cryptogram produced by this type system will show the characteristic peaks and troughs of a normal uniliteral frequency distribution for the plaintext, except peaks and troughs will not correspond and the direction of progression of the sequence may be reversed. Identification of this system's use, and the recovery of the plaintext values of the cipher sequence, lie in fitting the uniliteral frequency distribution of the ciphertext to a normal uniliteral frequency distribution. This is known as "fitting the distribution to the normal."

b. Identification and recovery of the plaintext is then simply a matter of identifying the plaintext value of two or more cipher letters and the use of these values to determine the direction of progression of the cipher sequence relative to the plain sequence. The identification of a cipher letter, determining its associated plaintext value, is based upon its frequency of occurrence relative to all other letters of the cipher sequence. For example, the value of a high-frequency cipher letter immediately is suspected as one of the normal high-frequency letters (E, T, N, R, O, A, I, S). By assuming the values of several high-frequency cipher letters, a base can be established to correlate the peaks and the troughs of the ciphertext distribution to those of a normal uniliteral frequency distribution.

c. In fitting the actual distribution of the ciphertext to the expected norm, two functions must be considered. First, correspondence of values will not necessarily be exact regarding frequencies of occurrence. For example, the normal order of occurrence for the high-frequency plaintext letters is E, T, N, R, O, A, I, S. But, note that the frequency of these same letters in the cryptogram in paragraph 7-9*b*(2), in their order of occurrence, is O, N, I, E, T, A, S, R. Second, although frequency of occurrence may vary, the spatial relationship between the high-frequency letters, and all letters, will remain constant. Because of the former fact, the point of coincidence of the two sequences may be in question. However, this can always be resolved by considering the spatial relationship of peaks and troughs. Considered as a group, their correspondence of frequency between sequences should always be relatively close.

d. In the final analysis, the accuracy of identification and recovery of the cipher alphabet hinges on the consistent substitution of the plaintext values for the cipher character in the cryptogram resulting in intelligible plaintext. If this is not the case, no matter how close the approximation between actual and expected frequencies, or how well the fit is, only two possibilities exist. First, the closeness of the fit is pure coincidence and another equally good fit can be obtained from the same data. Second, the cryptogram involves something more than simple monoalphabetic substitution by means of single standard cipher alphabet.

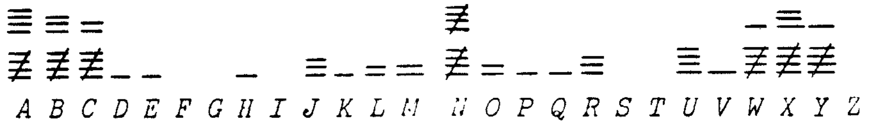
7-11. (~~C~~) Solution Using a Uniliteral Frequency Distribution

a. Essentially, the method of solution is an attempt to fit the distribution of the ciphertext to the expected normal distribution. Accordingly, the first step is to prepare a uniliteral frequency distribution of its ciphertext. Using the message in figure 7-4, the distribution can be derived.

```
YJCAX UBANY XACNJ BCNAW BUXYN BXOYA

XBYNL CQRUU VRWNM JWMLX ENANM KHBCA

XWPYX RWCBW NJALA NBCDO
```



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
9	8	7	1	1	0	0	1	0	3	1	2	2	10	2	1	1	3	0	0	4	1	6	8	6	0

Figure 7-4 (C). Uniliteral frequency distribution, substitution ciphertext (U).

(1) If there is any question as to the system involved in the production of this cryptogram, the uniliteral frequency distribution above should serve to resolve it. First, substitution, rather than transposition is indicated by the fact that normal low and medium-frequency letters in this distribution are high in occurrence. Were it transposition, where values are unchanged, there would not be this reversal of frequency characteristics. Second, uniliteral monoalphabetic substitution is suggested by the peaks and troughs, shown by the distribution, which do not correspond to their normal positions relative to the alphabet. This further suggests a displacement of the points of coincidence between the plain and cipher sequence. If nonmonoalphabetic substitutions are involved, the peaks and troughs are suppressed.

b. Solution of this type system depends upon assuming the plaintext value of one or more cipher letters, establishing the direction of progression, and attempting to produce intelligible plaintext as the final text. Comparing this distribution to a normal distribution, certain similarities and dissimilarities are observed as shown in figure 7–5.

(1) Note that the pattern of peaks and troughs in the normal distribution have a specific spatial relationship, the highest crest over the letters A, E, I, N, R, S, O, and the toughs marked by T, B, G, J, K, P, Q, U, V, W, X, Y, and Z. Note also that the letters R, S, T, and U combined, form a plateau, as does L, M, N, and O. In horizontal distances, A is separated from E by three letters, E from I by three letters, I from N by four letters, and N from T by five letters.

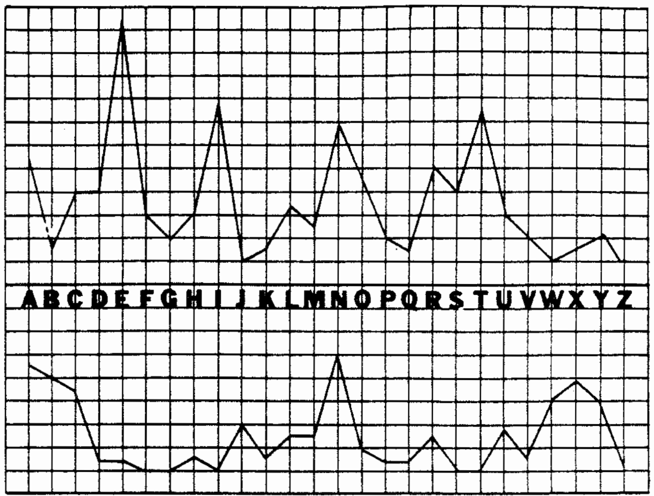


Figure 7–5 (~~C~~). Identification of ciphertext values by comparison (U).

(2) Examination of the distribution prepared from the ciphertext reveals a similar spatial pattern, but one which is located above different letters. Note that a peak located at *J* is followed by another at *N*, separated by three spaces; another is located at *R*, again a three space interval; *U* also represents a peak, at an interval of two spaces, and is followed by a plateau at *W*, *X*, and *Z*.

(3) Considering the cyclic nature of the alphabet, Z followed by A, and assuming that the progression of the pattern in the ciphertext's distribution is to the right, the two patterns can be alined by shifting the cipher sequence to the left until *J* cipher coincides with A plain.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*

(4) As this alphabet is not reciprocal, i.e. Ap=*Jc* but *Ac* does not equal Jp; the values must be inverted to form a deciphering alphabet. That is, the cipher component placed in alphabetic order with the plain component below it.

For example:

C	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q

(5) Using the above deciphering alphabet, the cryptogram can now be deciphered, success indicating that all previous assumptions are correct. If failure results, the analyst reexamines the distribution attempting to determine the correct point of coincidence between the two alphabets.

YJCAX UBANY XACNJ BCNAW BUXYN BXOYA
PATRO LSREP ORTEA STERN SLOPE SOFPR
XBYNL CQRUU VRWNM JWMLX ENANM KHBCA
OSPEC THILL MINED ANDCO VERED BYSTR
XWPYX RWCBW NJALA NBCDO
ONGPO INTSN EARCR ESTUF

PATROLS REPORT EASTERN SLOPES OF PROSPECT HILL MINED
AND COVERED BY STRONG ~~POI~~NTS NEAR CREST

c. In the example above, a direct standard cipher alphabet is used in enciphering the plaintext. Had the cipher alphabet been a reversed standard, the same methods of analysis would have been fully applicable, the only difference being that the progression of the relationships of peaks and troughs in a distribution of the ciphertext would be in reverse order as well as offset. To aline this distribution to the normal, it is then inscribed in reverse order after determination of the point of coincidence. Further, a slight variation exists in the final deciphering text. As reversed standard cipher alphabets are partly reciprocal, the construction of a deciphering alphabet is not always required.

7–12. ~~(C)~~ Solution by Completing the Plain Component

a. The foregoing method of solution involves the construction and study of a frequency distribution as a means of recovering the plaintext. There is another method, applicable to direct standard alphabets and to reversed standard alphabets with a slight variation, which is much more rapid. As this system is purely mechanical, it does not involve the construction of a frequency distribution. The principle underlying this method of analysis is based upon the inherent characteristics of uniliteral monoalphabetic cipher alphabets, where direct standard or reversed standard alphabets are used as the cipher sequence. The key element in both cases is an orderly sequence of values present in both the plain and cipher sequences.

b. The significance of this characteristic is seen in the following cipher alphabet.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*X*	*W*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*

(1) Note again that the cipher alphabet was produced by juxtaposing two normal alphabets, the lower or cipher sequence being displaced 9 letters to the left until Ap=*Jc*. This relative degree of shift is equal in all cases as long as the sequence of the letters in the alphabets are not disarranged. For example, note that there is a 9-letter difference between *Bc* and *Kc*, Cp and Lp, etc. As a direct standard cipher alphabet is being dealt with, there are only 25 possible positions in which the two alphabets may be juxtaposed to produce a cipher alphabet. The 26th position, Ap=*Ac*, clearly gives only plaintext. Where this sytem is used then, only one of the 25 possible positions can be correct.

(2) The alphabet above could be slipped through all 25 possible positions, from Ap=*Bc* to Ap=*Zc*, checking each for its ability to decipher a message. This is time consuming. Instead, the sequence of the letters themselves can be used. Note the encipherment of the following plaintext, first by the cipher alphabet above, and then by a similar alphabet where Ap=*Kc*.

CONTACT	MADE	WITH	ENEMY	Plaintext
LXWCJLC	*VJMN*	*FRCQ*	*NWNVH*	Cipher Ap=*Jc*
MYXDKMD	*WKNO*	*GSDR*	*OXOWI*	Cipher Ap=*Kc*

(3) In the example above, the sequence of letters in the columns is formed by superimposing the ciphertext progress, following each progressive displacement of point of coincidence. Therefore, given the cryptogram, a solution can be obtained simply by inscribing alphabets vertically in sequential order, using as the starting point each letter of the ciphertext as demonstrated in figure 7–6. In effect, this process duplicates the possible ciphertext derived from all 25 positions.

Example:

```
GXKGA TJKXS UXZGX LOXKD     Cipher text
HYLHB UKLYT VYAHY MPYLE
IZMIC VLMZU WZBIZ NQZMF
JANJD WMNAV XACJA ORANG
KBOKE XNOBW YBDKB PSBOH
LCPLF YOPCX ZCELC QTCPI
MDQMG ZPQDY ADFMD RUDQJ
NERNH AQREZ BEGNE SVERK
OFSOI BRSFA CFHOF TWFSL
PGTPJ CSTGB DGIPG UXGTM
QHUQK DTUHC EHJQH VYHUN
RIVRL EUVID FIKRI WZIVO
SJWSM FVWJE GJLSJ XAJWP
TKXTN GWXKF HKMTK YBKXQ
ULYUO HYYLG ILNUL ZCLYR
VMZVP IZZMH JMOVM ADMZS
WNAWQ JZANI KNPWN BENAT
XOBXR KABOJ LOQXO CFOBU
YPCYS LBCPK MPRYP DGPCV
ZQDZT MCDQL NQSZQ EHQDW
AREAU NDERM ORTAR FIREX     Plain text
BSFBV OEFSN PSUBS GJSFY
CTGCW PFGTO QTVCT HKTGZ
DUHDX QGHUP RUWDU ILUHA
EVIEY RHIVQ SVXEV JMVIB
FWJFZ SIJWR TWYFW KNWJC
```

Figure 7-6 (C). Solution by completing the plain component, direct standard cipher alphabet (U).

c. In those cases where a reversed standard cipher alphabet is used, a preliminary step is required to form the base for the projection of the vertical alphabetical sequences. This is required because, although a sequence is present in the ciphertext, the mechanics of the system are reversed. For example, with the following message, a base can be established as shown in figure 7-7. Then each column can be completed to recover the plaintext.

Message: XRSWX TSADY HPDSE IULPY

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Plain
Z	*Y*	*X*	*W*	*V*	*U*	*T*	*S*	*R*	*Q*	*P*	*O*	*N*	*M*	*L*	*K*	*J*	*I*	*H*	*G*	*F*	*E*	*D*	*C*	*B*	*A*	Cipher

CIHDC GHZWB SKWHV RFOKB

CIHDC	*GHZWB*	*SKWHV*	*RFOKB*	Cipher text
DJIED	*HIAXC*	*TLXIW*	*SGPLC*	
EKJFE	*IJBYD*	*UMYJX*	*THQMD*	
FLKGF	*JKCZE*	*VNZKY*	*UIRNE*	
GMLHG	*KLDAF*	*WOALZ*	*VJSOF*	
HNMIH	*LMEBG*	*XPBMA*	*WKTPG*	
IONJI	*MNFCH*	*YQCNB*	*XLUQH*	
JPOKJ	*NOGDI*	*ZRDOC*	*YMVRI*	
KQPLK	*OPHEJ*	*ASEPD*	*ZNWSJ*	
LRQML	*PQIFK*	*BTFQE*	*AOXTK*	
MSRNM	*QRJGL*	*CUGRF*	*BPYUL*	
NTSON	*RSKHM*	*DVHSG*	*CQZVM*	
OUTPO	STLIN	EWITH	DRAWN	Plain text
PVUQP	*TUMJO*	*FXJUI*	*FSBXO*	
QWVRQ	*UVNKP*	*GYKVJ*	*FTCYP*	
RXWSR	*VWOLQ*	*HZLWK*	*GUDZQ*	
SYXTS	*WXPMR*	*IAMXL*	*HVEAR*	
TZYUT	*XYQNS*	*JBNYM*	*IWFBS*	
UAZVU	*YZROT*	*KCOZN*	*JXGCT*	
VBAWV	*ZASPU*	*LDPAO*	*KYHDU*	
WCBXW	*ABTQV*	*MEQBP*	*LZIEV*	
XDCYX	*BCURW*	*NFRCQ*	*MAJFW*	
YEDZY	*CDVSX*	*OGSDR*	*NBKGX*	
ZFEAZ	*DEWTY*	*PHTES*	*OCLHY*	
AGFBA	*EFXUZ*	*QIUFT*	*PDMIZ*	
BHGCB	*FGYVA*	*RJVGU*	*QENJA*	

Figure 7–7 (7). Solution by completing the plain component, reversed standard cipher alphabet (U).

d. Using the foregoing method, when the letters of a cipher alphabet are known sequences, considerable time and effort can be saved. In some cases this prior knowledge is the only possible means of solving very short cryptograms that might otherwise be unsolvable. The essential point in any case is that the sequence of the letters used must be established. Even mixed sequences can be handled in exactly the same way. If, however, the sequence is unknown, methods to be covered later must be used. Generally, since this method is so easy, it should be a first step in those cases where the cryptogram is obviously a substitution cipher in monoalphabetic terms. First a direct standard alphabet should be tried, and then a reversed standard alphabet should be tried. If both fail, a logical assumption is that the cryptogram in question involves a mixed cipher alphabet.

CHAPTER 8 ~~(C)~~

UNILITERAL MONOALPHABETIC SUBSTITUTION SYSTEMS USING MIXED CIPHER ALPHABETS

Section I. ~~(C)~~ GENERATION AND USE OF MIXED CIPHER ALPHABETS

8–1. ~~(C)~~ Mixed Cipher Alphabets

a. Mixed cipher alphabets differ from standard cipher alphabets in that one or both of the sequences is a mixed sequence. A mixed sequence is a series of letters that does not correspond to normal sequential order of the alphabet used. As a general rule, a mixed cipher alphabet will consist of one of the following mixes.

(1) The plain component is a standard sequence; cipher component is a mixed sequence.

(2) The plain component is a mixed sequence; the cipher component is a standard sequence.

(3) Both components are the same mixed sequence with displaced points of coincidence.

(4) Both components are different mixed sequences.

(5) Both components are the same mixed sequence but one reversed.

b. Two main types of mixed alphabetic sequences are randomly mixed and systematically mixed sequences. The latter type because it is based upon a scheme that by its nature is systematic, is useful because it makes possible the derivation of one or more mixed sequences from easily remembered words, phrases, or similar keys. Additionally, it does not require written documentation. A disadvantage in producing a mixed sequence through a systematic disarrangement is that the possibility of its analysis is always present. As practical considerations set a limit to the complexities that can be introduced by systematically mixing an alphabet, where greater security is required, randomly mixed alphabets are used.

c. Randomly mixed alphabets give more cryptographic security than do the less complicated systematically mixed alphabets because they give no clues to the position of letters. Whenever the laws of chance operate in the construction of a mixed alphabet, a thorough disarrangement is likely to be produced. The primary disadvantage of random alphabets is that they are not susceptible to local generation. They must be reduced to writing and distributed to all interested correspondents with explicit instructions pertaining to their use.

8–2. ~~(C)~~ Keyword Mixed Cipher Alphabet

a. One of the simplest types of systematically mixed sequences that is used in a cipher alphabet is the keyword mixed alphabet. In this type, the disarrangement is achieved through the use of a keyword to establish the framework of the sequence. The sequence begins with the keyword. Any letter repeated in the keyword is used only once, at its first appearance. Thereafter it is dropped. These letters are then followed by all other unused letters of the alphabet in their normal sequence.

Example:

Keyword: CRYPTOGRAPHIC
Repeated letters dropped: CRYPTOGAHI
Letters not appearing in keyword added in their normal sequence: *CRYPTOGAHIBDEFJKLMNQSUVWXZ*

b. This type sequence, when paired with a sequence other than a reversal of itself is nonreciprocal. When positoned against a double inscription of itself it is nonreciprocal, except at one juxtaposition. Therefore, for convenience in enciphering and deciphering, two alphabets are constructed, an enciphering alphabet in which the letter of the plain component coincides with the normal sequence, and a deciphering alphabet in which the sequence of letters in the cipher component coincides with the normal.

Example:

Enciphering alphabet

P A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
C *C R Y P T O G A H I B D E F J K L M N Q S U V W X Z*

Deciphering alphabet

C *A B C D E F G H I J K L M N O P Q R S T U V W X Y Z*
P H K A *L M N* G I J *O P Q R S* F D T B U F *V W X* Y C Z

c. The keyword or phrase used need not consist of any definite number of letters, although those which most thoroughly disarrange the normal sequence are most appropriate. The reasons for this can be seen in the enciphering alphabet above. Note that the two distinct segments of the cipher sequence are obvious, the keyword and the remaining alphabetic sequence. Note also that in the deciphering alphabet, neither is completely apparent though there is evidence of sequencing shown underlined. The importance of the former characteristic is that it provides the analyst with a means whereby the solution of a cryptogram is hastened. The analyst needs only to reconstruct the cipher alphabet in terms of an enciphering alphabet, as analysis of the message progresses, using each value as it is recovered. Once a partial recovery passes a certain point, it may be possible to recover the alphabet using pattern alone.

8–3. (C) Transposition Mixed Cipher Alphabets

a. It is possible to disarrange the sequence of an alphabet even more thoroughly by applying any one of the transposition methods treated previously as cipher systems. The alphabet to which the transposition process is applied may be either a standard alphabet, a keyword mixed alphabet, or even a random alphabet. In a random alphabet, little is gained by disarranging the sequence. Some of the possibilities offered by this method are illustrated below:

(1) Simple columnar transposition using keyword mixed alphabet:

Q U A D R N G L E
B C F H I J K M O
P S T V W X Y Z
Q B P U C S A F TDHVRIWNJXGKYLMZEO

(2) Numerically keyed columnar transposition:

8 5 3 4 7 2 6 1
U N I L T E R A
B C D F G H J K
M O P Q S V W X
Y Z
A K X E H V I DPLFQNCOZRJWTGSUBMY

(3) Route transposition (alternate vertical):

V E H I C U L A R
B D F G J K M N O
P Q S T W X W Z
V B P Q D E H F S TGICJWXKULMYZNARO

b. The systems of disarrangement above produce certain patterns as a result of the mechanical process involved, and due to the alphabet selected for disarrangement, which will provide the analyst with a means of recovery. Note that the keyword appears in the first row and that the succeeding rows contain the remaining alphabetic sequence. The last row, an incomplete row, contains some portion of the sequence *UVWXYZ*. These last letters then are scattered at specific intervals through the cipher alphabet by the process of columnar extraction. If the extraction is straight columnar, the letters appear at an interval equal to the number of rows of the matrix, in sequential order left to right. If the extraction process is numerically keyed, the letters appear in key number order, again at intervals equal to the number of rows. In the case of route transposition, patterns also exist but they are usually not so pronounced. One such pattern is the pairing of the terminal letters. Note that *WX* and *YZ* are paired in the alphabet above.

8–4. (C) Decimation Mixed Cipher Alphabets

a. In this method of deriving a systematically mixed sequence, an alphabet, either a normal or a keyword mixed sequence, is counted off, letter by letter, using a predetermined interval. As each letter is decimated, or counted off, it is eliminated from the basic sequence and set aside. The count continues around the alphabet until all letters are eliminated. As the letters are eliminated, they are set down in the order of their elimination to form a new sequence. An example of this method is depicted in figure 8–1.

Basic alphabet (keyword mixed sequence):
TELGRAPHBCDFIJKMNOQSUVWXYZ

Decimated at an internal of 6:
TELGRAPHBCDFIJKMNOQSUVWXYZ

```
12345612345612345612345612
     A     F     O     X
34561 23456 12345 61234 56
   G      D       Q      Z
123 4 5612  34561  2345 6
       H       M        Y
123 4 5 61  234 5  6123
        B          S
456 1 2  3  456 1   234
  L           K
56  1 2  3  45  6   123
 E              N
4   5 6  1  23      456
      P               W
1   2    3  45      61
                    U
2   3    4  56       1
             J
2   3    4  5        6
                     V
1   2    3  4
5   6    1  2
    R
3        4  5
6        1  2
T
         3  4
         5  6
            I
```

AFOXGDQZHMYBSLKENPWUJVRTIC

As C is not eliminated in the decimation process, it accordingly appears as the last letter of the sequence.

Figure 8–1 (C). Derivation of mixed sequence by decimation (U).

b. Another method of decimating an alphabet, which is at once simpler but also limited, is to use each letter in the count whether or not it has been used before. For example, in figure 8–2 the standard alphabet is decimated at an interval of five.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
12345123451234512345123451
    E    J    O    T    Y
23451234512345 - etc.
   D    I    N

EJOTYDINSXCHMRWBGLQVAFKPUZ
```

Figure 8–2 (C). Decimation, reuse of letters in count (U).

The limitation of the method is that the interval must be an odd number, as even numbers will cause repeated letters. For example, in figure 8–3 a standard alphabet is shown decimated at an interval of four.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
12341234123412341234123412
34123412341234123412341234
12341234
DHLPTXBFJNRVZDH        Repeated letters.
```

Figure 8–3 (C). Repetitions in decimation as a result of even numbers as interval (U).

Section II. (C) RECOVERY OF MIXED CIPHER ALPHABETS

8–5. (C) General

a. The analyst should always attempt the recovery of the method used in generating the cipher alphabet simultaneously with the analysis of the cryptogram. This effort is to be distinguished from the normal reconstruction of the cipher alphabet which occurs as a matter of course with the analysis of a cryptogram. The purpose of recovering the method of generation of a cipher alphabet is to enable the analyst to recover the cipher alphabet in its entirety and thereby aid in the solution of the cryptogram. If sufficient cipher-to-plain values can be obtained by reconstruction as a by-product of analysis of the message, the possibility exists that they may be used to determine the method of generating the cipher alphabet. Where this can be achieved early in the solution of the message, a great deal of effort can be saved and, in some cases, transform the process of cryptanalysis to one of decipherment.

b. Cipher alphabets should be reconstructed in the form of enciphering alphabets, the plain component in alphabetic sequence. This is important for two reasons. First, if the sequence of the cipher component has an observed pattern, decimation, keyword, etc., it will appear in this arrangement. Thus any evidence of system in its construction, however slight, may serve to collaborate identifications already made, and may yield the clues necessary for complete identification of the method used and total recovery of the alphabet. Second, once a method of cipher alphabet generation has been determined, it affords an insight into the general method, keys, and keywords used and may be of assistance in subsequent studies of similar messages.

8–6. (C) Recovery of Keyword Mixed Sequences

a. Recovery of keyword mixed sequences, when used as the cipher component with a standard sequence as the plain component, presents little or no difficulty. The primary problem likely to be encountered is one of recognizing the keyword given only a few values. However, even here a few rules apply that will aid the analyst. For example, the partially reconstructed enciphering alphabet below was derived through the analysis of a message.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	*S*				*Z*				*V*					*T*	*H*			*D*	*F*	*G*	*I*					

b. A keyword mixed sequence can be divided arbitrarily into two segments, that composed of the keyword and that composed of the remaining a'phabetic sequence. Having previous knowledge of what constitutes the normal alphabet and its sequence, the analyst can use this with a minimum of recovered values to recover the keyword segment, the unknown. Examination of the cipher sequence above reveals the possible position of the two segments divided by the letter *Z*. It is possible that *Z* is part of the keyword but not very likely. If the keyword starts at this point, it runs to some point to the right. The cipher sequence *DFGI* is natural, a good alphabetic sequence possibly marking the resumption of the alphabetic sequence and therefore the end of the keyword, except that the *E* and *H* are missing. The *H* is noted preceding the sequence *DFGI* in the keyword segment. The *E*, a high-frequency letter, is safely assumed to be a part of the keyword also.

(1) The object now is to determine those letters of the alphabetic segment. By so doing, certain letters can be eliminated which must then be part of the keyword. The space between the *S* and *Z* provides for only three letters. In the alphabetic sequence, six letters appear. But of the six, *V* and *T* are already placed leaving four letters, *UWXY*. Also the space between the *TH* and the *D* provides two spaces for the letters *ABC*. Of these possibilities, it is far more likely that the placement is *UXY* and *BC*, though the former may also be *UWX*. Accepting the combination *UXY*, the alphabet is now shown as follows:

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	*S*	*U*	*X*	*Y*	*Z*				*V*					*T*	*H*	*B*	*C*	*D*	*F*	*H*	*I*					

(2) At this point, the assumed value is checked against the cryptogram by attempting further decipherment, success confirming the assumptions. Further analysis of the sequence depends upon the discovery of new values as a result of confirming the assumed value, i.e., the whole process is like a series of building blocks. The assumption of one letter may aid in completing a word in a cryptogram or may suggest another letter which in turn provides the basis for the assumption of yet another value. This value then is checked against both the alphabet and the frequency distribution of the ciphertext. This in turn enables the analyst to expand the cryptogram and the cipher sequence. For example, assume that in the process of confirming the letters assumed previously, the analyst finds that the letters Hp=*Ac*, Lp=*Oc*, and Wp=*Kc*. The alphabet now appears:

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	*S*	*U*	*X*	*Y*	*Z*	*L*		*A*	*V*			*O*	*R*	*T*	*H*	*B*	*C*	*D*	*F*	*G*	*I*	*J*	*K*			

(3) On this basis, *Jc* is equated to Vp by position alone and so placed in the sequence. The placement of *M*, *N*, *P*, and *Q* is now quite easy. Three of the four must be associated with X, Y, and Z of the plain sequence. Zp, a low-frequency letter, lends itself admirably to this association. The analyst need only check his distribution for one of the letters *M*, *N*, *P*, or *Q* which either does not appear, or appears rarely. For example, finding no occurrence of a *Qc* he at once equates it to Zp, because it is the only letter which immediately precedes the *S*.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	*S*	*U*	*X*	*Y*	*Z*	*L*		*A*	*V*			*O*	*R*	*T*	*H*	*B*	*C*	*D*	*F*	*G*	*I*	*J*	*K*			*Q*

(4) The letters now remaining to be placed are *E*, *M*, *N*, *P*, and *W*, open'ng two possibilities. The keyword is assumed, if evidence warrants. Each value is checked by decipherment or by using the frequency distribution. The plaintext value is assumed and then checked by decipherment. In any event, a solution is soon reached.

8–7. ~~(C)~~ Recovery of Transposition Mixed Cipher Alphabets

a. The recovery of transposition mixed cipher alphabets involves essentially the same processes as the cryptanalysis of transposition ciphers. In the latter, the analytic attacks are based upon the inherent characteristics of the system with initially little or no knowledge of the plaintext other than any characteristics which may have appeared in the ciphertext. In the case of transposition mixed cipher alphabets however, the analyst is dealing with several known factors. For example, examine the enciphering alphabet below.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	*R*	*A*	*M*	*E*	*B*	*P*	*C*	*D*	*Q*	*O*	*F*	*V*	*N*	*G*	*W*	*S*	*H*	*X*	*T*	*J*	*Y*	*U*	*K*	*Z*	*I*	*L*

(1) The cipher component is not a keyword mixed sequence. A keyword may have been used to prepare a base alphabet, but on appearance this base appears to have been systematically disarranged. This could have been done in one of two primary ways, transposition or decimation. Assuming then that the alphabet was produced by some means of transposition, the analyst scans the sequence for some pattern. The *V*, *W*, *X*, *Y*, and *Z* appear at an interval of 3, suggesting columnar transposition. Decimation is not considered, as all these letters appear in sequence past the midpoint of the cipher sequence. The significance of this will be dealt with later. Using the *VWXYZ* cluster as a base, a fragmentary matrix is constructed.

O	*N*	*S*	*T*	*U*
F	*G*	*H*	*J*	*K*
V	*W*	*X*	*Y*	*Z*

(2) The second and third rows show good sequential order, while the first suggests a keyword fragment. Accepting this keyword fragment, the next step is to continue to expand the sequential pattern of the second and third rows. Two clusters, *CDQ* and *EBP*, show a sequential relation in the second and third characters and are added.

E	*C*	*O*	*N*	*S*	*T*	*U*
B	*D*	*F*	*G*	*H*	*J*	*K*
P	*Q*	*V*	*W*	*X*	*Y*	*Z*

(3) Again the sequence in the second and third rows is good. Missing letters, except the *I* and *R*, already appear in the first row. Both the *I* and *R*, with their associated letters *RAM* and *IL*, are placed using the sequential pattern of their associated letters. *RAM* is placed at the left, as *A* and *M* precedes *B* and *P;* and *IL* is placed to the right as the *L* follows a *K*. Note that in the case of the *IL*, this cluster consists of only two letters, a characteristic of the extreme right of an incompletely-filled matrix. Thus the matrix now appears fully recovered:

R E C O N S T U I
A B D F G H J K L
M P Q V W X Y Z

b. Note that this solution differs from the first in that a complete cipher sequence is studied, and no correlation of its values to a cipher message is required. Given a complete sequence, it is always easier to recover the system of generating it than to work with only fragments of a sequence. However in so doing, some of the value of recovery is lost, i.e. it does not aid in the analysis of a message. The recovery of a cipher sequence from fragments is more difficult but far more rewarding in terms of actual use.

8–8. (~~C~~) Derivation of a Numeric Key

a. In those cases where a cipher alphabet is generated by keyed columnar transposition, the same techniques given above are applicable to the recovery of the matrix. The numeric key involved is then determined by noting the order in which the columns of the matrix appear in the alphabetic sequence. For example, observe the relationship between the columns of the matrix in figure 8–4 and the order of their appearance in the alphabetic sequence.

6	2	1	5	4	7	8	9	3
R	*E*	*C*	*O*	*N*	*S*	*T*	*U*	*I*
A	*B*	*D*	*F*	*G*	*H*	*J*	*K*	*L*
M	*P*	*Q*	*V*	*W*	*X*	*Y*	*Z*	

1	2	3	4	5	6	7	8	9
CDQ	*EBP*	*IL*	*NGW*	*OFV*	*RAM*	*SHX*	*TJY*	*UKZ*

Figure 8–4 (~~C~~). Relation of column order to sequence order (U).

b. When compared to the straight columnar sequence, a difference in the location of the *UVWXYZ* cluster is seen as shown in figure 8–5.

	1			2		3			4			5			6			7			8			9	
C	*D*	*Q*	*E*	*B*	*P*	*I*	*L*	*N*	*G*	*W*	*O*	*F*	*V*	*R*	*A*	*M*	*S*	*H*	*X*	*T*	*J*	*Y*	*U*	*K*	*Z*
R	*A*	*M*	*E*	*B*	*P*	*C*	*D*	*Q*	*O*	*F*	*V*	*N*	*G*	*W*	*S*	*H*	*X*	*T*	*J*	*Y*	*U*	*K*	*Z*	*I*	*L*
	6			2			1			5			4			7			8			9		3	

Figure 8–5 (~~C~~). Comparison of sequences (U).

Note that the sequence is now somewhat disturbed, but also that the interval between each of the letters is still 3. Therefore, by starting the column above the base cluster *VWXYZ*, the same result is obtained. The bottom two rows show alphabetic sequence, less those letters appearing in the top row as part of the keyword.

8–9. (~~C~~) Recovery of Decimated Sequences

a. The characteristic which provides the basis of analysis and recovery of decimated sequences is the cyclic permutations of the letters of the sequence imparted to them by the decimation process. The characteristic is seen in the examples below.

(1) Where a cipher sequence is derived by a count where all letters are used, none excluded, a constant interval of its multiple occurs between the letters that are adjacent in the base alphabet. For example, in the alphabet below, note that the interval is 5 between the letters *E–J*, *O–T*, and *Y–D*. Note also that the interval of 5 is constant in reverse, *B* to *A* and *C* to *D*, indicating that these letters were taken out of the alphabet in reverse order and after other letters normally preceding them. Using the characteristics, the alphabet is easily recovered by counting off the letters, thus placing them in their original sequence. Spaces between the letters are filled by letters in sequence as the count is continued.

Example:	*E*	*J*	*O*	*T*	*Y*	*D*	*I*	*N*	*S*	*X*	*C*	*H*	*M*	*R*	*W*	*B*	*G*	*L*	*Q*	*V*	*A*	*F*	*K*	*P*	*U*	*Z*
	–	–	–	–	*E*	–	–	–	–	*J*	–	–	–	–	*O*	–	–	–	–	*T*	–	–	–	–	*Y*	
	1	2	3	4		1	2	3	4		1	2	3	4		1	2	3	4		1	2	3	4		1
	–	–	–	*D*	–	–	–	–	*I*	–	–	–	–	*N*	–	–	–	–	*S*	–	–	–	–	*X*		
	2	3	4		1	2	3	4		1	2	3	4		1	2	3	4		1	2	3	4		1	2
	–	–	*C*	etc.																						
	3	4																								

After all the letters of the cipher sequence are counted off, the cycles are compressed into one to reform the basic alphabet.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

(2) In the case where the cipher sequence is derived by a count which excluded letters once they were used, the same counting system as above is used, but the count does not include letters previously placed, in effect duplicating the generation process. For example using the alphabet below, the count appears:

```
C F I L O R U X A E J N S W B H P V D M Y K Z T G Q
– – C – – F – – I – – L – – O – – R – – U – – X – –
1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2
A – – E – – J – – N – – S – – W – –
3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2
B
3
```

The count is continued until the basic alphabet is recovered.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

b. In both examples above, solution is predicated on the ability of the analyst to determine the proper intervals. In both instances, since a direct standard alphabet is used, this interval is easily determined, being found as the distance between adjacent letters of the base sequence. Where a keyword mixed alphabet is used as the base, it may be somewhat more difficult to determine the correct interval, but not an impossibility. Note the characteristics of the two segments of the keyword mixed alphabet in figure 8–6.

```
Keyword:  ABSTRACTION

A B S T R C I O N|D E F G H J K L M P Q U V W X Y Z

Keyword Segment      Alphabetic Sequence Segment
```

Figure 8–6 (C). Keyword and alphabetic segments, keyword mixed alphabet (U).

(1) In the sequence above, the normal alphabetic progression still remains, even though it may be missing some of its component letters. The *UVWXYZ* cluster is unchanged. These two elements, particularly the cluster, provide a basis for the analyst to determine the interval in the decimation process. If the alphabet above is decimated at an interval of 4, used letters not recounted, it appears as:

T O F K Q X B I G M W S D L Y C J Z E V N A U R P H

(2) This sequence contains certain patterns which are normally different from a decimation of a direct standard alphabet. Taking out the first three elements of the two decimated alphabets shown underlined, which end with a letter of the *VWXYZ* cluster, this pattern can be seen.

Direct standard sequence decimated at an interval of 3:

```
C F I L O R U X
A E J N S W
B H P V
```

Keyword mixed sequence decimated at an interval of 4:

```
T O F K Q X
B I G M W
S D L Y
```

(3) In the first set, the alphabetic progression is constant at an interval of 3 (*C – – F – – I – – L* etc.). In the second set, the alphabet progression is not constant nor is it at the same interval.

```
T   O   F – – – – K – – – – – Q
```

The absence of a constant interval between the letters and the lack of alphabetic progression within the individual elements indicates that the sequence is derived from a mixed alphabet base.

(4) Since the recovery of the base alphabet depends on determining the decimation interval, some means must be used to find this. The simplest method is through the use of the *UVWXYZ* cluster letters. Note that in the second decimation process illustrated above, the *X*, *W*, and *Y* each mark one run-through of the alphabet, i.e. letters are extracted at a given interval, in this case 4. The first letter to be extracted is *T*, then *O*, then *K*, then *Q*, then *X*. Then the process starts again around the alphabet. The sequence *T* to *X* contains six letters. Six divides into 26, 4 times with a remainder of 2. Therefore, the interval is 4.

(5) If the assumption of 4 as the interval is correct, when applied to a similar cipher sequence it produces a keyword mixed alphabet. To illustrate the procedure, note the recovery shown in figure 8-7.

```
D B H P X N C K V A E M S O Q R J T L Z Y W I G U E
              5 letters
              26 + 5 = 5 + 1
              interval of 5 assumed

- - - - D - - - - B - - - - H - - - - P - - - - X -
- - - N   - - - - - C - - -   - K - -   - - V -   -
- - A     - - - -       E M etc.
```

Figure 8-7 (C). Recovery of a decimated alphabet (U).

Note that the count above did not include letters once placed. If they are included, the sequence appears incorrectly as illustrated below:

```
- - - - D - - - - B - - - - H - - - - P - - - - X -
- - - N - - - - C - - - - K - - - - V
                alphabetic order reversed
```

The count continued, as in the first example above, results in the following alphabet:

S T A N D R I Z O B C E F G H J K L M P Q U V W X Y
Keyword: STANDARDIZATION

Section III. (~~C~~) SOLUTION OF UNILITERAL MONOALPHABETIC MIXED ALPHABET CIPHERS

8-10. (~~C~~) System Identification

a. The first step of cryptanalysis is the identification of the system to which a given cryptogram or series of cryptograms belong. Determination is based on certain characteristics imparted to the ciphertext by the method of encipherment. In the case of uniliteral monoalphabetic substitution, identification is usually easy, based on the spatial relationship of peaks and troughs of the normal and the cipher distributions. Where they cannot be matched, the logical assumption is that a mixed cipher alphabet is used. For example, the frequency distribution of the ciphertext of the following message appears as:

```
AAAAQ  QFFQU  PKRTT  SWZRG  QFNWD  AERLN  WDANW
DAFAO  ADDAK  OADGR  GZRGJ  RURGR  FMAXU  DAEED
AQVEE  WJWGE  RLEWJ  WGEFA  HMAID  DWZRO  WGFKR
TTEHW  QDGWQ  VQFFQ  UPEFA  HVRJR  ERAGU  AOOQG
VAXXA  IDFCV  RJRER  AGKRT  TSWOA  JWVXD  AOUDA
EEDAQ  VEFCD  WWNWD  AFCDW  WFADA  QVYIG  UFRAG
WRZCF  EWJWG  ERLEF  AHAGW  AGWDW  ZRONG  FREVR
JRERA  GDWEW  DJWXY  AAAAQ
```

(1) Note that in compiling the frequency distribution, the first and last groups of the text are not used, as they are system indicators.

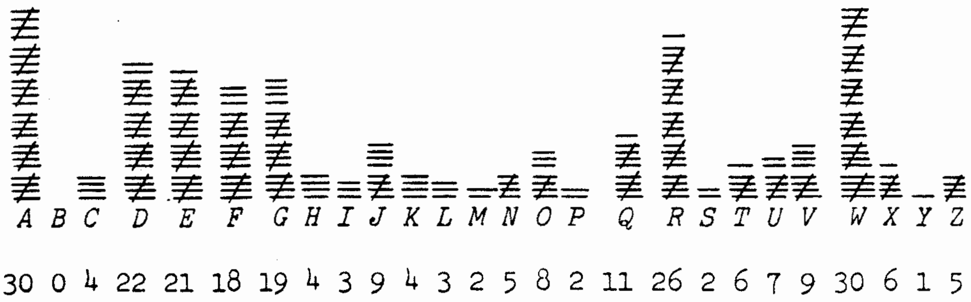


Figure 8–8 (U). Uniliteral frequency distribution, mixed monoalphabetic substitution (U).

(2) The pronounced peaks and troughs of the distribution shown in figure 8–8 are characteristic of uniliteral monoalphabetic substitution. If it is nonmonoalphabetic, it appears flattened. Further, the difference in spatial relationship of the peaks and troughs between this distribution and a normal distribution indicates that a mixed cipher sequence is used.

b. In this particular example, visual examination suffices to show that the system in use is probably monoalphabetic and uniliteral. This is caused by repeated occurrences of plaintext values which are duplicated in the ciphertext, only in different terms and easily revealed by the frequency distribution. This phenomenon is not always so evident. When such ev dence is not at hand, the analyst must use other statistical tools to aid in the identification of a system. Moreover, the analyst may use these tools to further substantiate his identification made by visual inspection.

8–11. (U) Statistical Identification

a. Several statistical tests are available for the identification of a system where the uniliteral frequency distribution does not reveal significant characteristics, either because of the shortness of the message, or because of the lack of internal characteristics in the plaintext. For short messages, in particular less than 200 letters, the expected frequency table will aid in the classification of a cryptogram as either substitution or transposition, and the Lambda (λ) or blank expectation test provides a means of identifying a substitution system as either monoalphabetic or nonmonoalphabetic. These tests given as tables are contained in paragraph 2–12 and their use explained in detail.

b. In addition to the tests above, the Phi (ϕ) test is also used to determine whether a given cipher is monoalphabetic or nonmonoalphabetic. The Phi test is a test of the observed occurrence of a given letter as contrasted to its expected random occurrence and its expected plaintext, or normal occurrence. The details of operation of the test are contained in paragraph 2–15.

c. An alternate way of testing whether a cryptogram is monoalphabetic is by determining the Phi Index of Coincidence (ϕ I.C.). The ϕ I.C. is the ratio of the number of observed occurrences (ϕo) to the number of expected random occurrences (ϕr). Shown in formula the ϕ I.C. appears as:

$$\phi\ \text{I.C.} = \frac{\phi o}{\phi r}$$

Actually this method used the same values as the Phi text, only expressing their relationships somewhat differently. That is, the ϕ I.C. gives, in terms of a ratio, the nearness of ϕo to ϕr. For example, the values given in paragraph 2–15 for ϕo, ϕr, and ϕp are:

Observed occurrence	$\phi o = 154$
Expected random	$\phi r = \ 94$
Expected plain	$\phi p = 164$

In terms of the ϕ I.C. the ratio of ϕo to ϕp is:

$$\phi\ \text{I.C.} = \frac{154}{94} = 1.64$$

The greater the value of the ϕ I.C. the stronger the indications of monoalphabeticity are. To illustrate this, consider the case where ϕo and ϕr are equal:

$$\phi o = 100 \quad \phi\ \text{I.C.} = \frac{100}{100} = 1.00$$
$$\phi p = 100$$

d. The theoretical ϕ I.C. of English plaintext is $\frac{.0667}{.0385}$ equaling 1.73, and the I.C. of random text is $\frac{.0385}{.0385}$ equaling 1.00. These values are determined by the fact that .0385 and .0667 are respectively the random constant and the plain constant of English in decimal terms. As uniliteral monoalphabetic substitution does not change the relative value of occurrence of letters of the plaintext but only their alphabetic identification, the ϕ I.C. can be used for determining the monoalphabetic or nonmonoalphabetic nature of the system. Thus, the ϕ I.C.

of the cryptogram being examined, 1.64, can be compared to the ϕ I.C. of plaintext, 1.73, and random, 1.00. As it approximates the ϕ I.C. of English plaintext, the system is assumed to be monoalphabetic. If the ϕ I.C. of a cryptogram closely approaches the ϕ I.C. of random text, we assume that the system is nonmonoalphabetic. The degree of approach is a a matter of the cryptanalyst's judgment.

8–12. (~~C~~) Preparation for Analysis

a. As a preliminary step to analysis of any cryptogram, the analyst should organize his work. Given a cryptogram to analyze, a work sheet is prepared. This need not be elaborate, but is in a format that lends itself to study and one which can be kept and used as a record of the solution, the actual work being performed on similar sheets. Also as an adjunct to the work sheet, the analyst keeps a technical summary of the solution explaining in some detail the steps followed and their success in obtaining a final solution. This is especially important in the case of solutions of new systems, and in those instances where another analyst is expected to use the result produced. Although there is no specific format for either the example given below and those in following paragraphs, they serve as models.

b. The cryptogram for analysis is copied on a work sheet of ¼-inch cross-section paper. If copied by hand, the writing is in ink and each letter is in accordance with the standard military printing system. In the case of monoalphabetic uniliteral ciphers, the message is copied as individual letters, regardless of the groupings of the message text, one letter to a cell with a space between each. To aid in the references to a particular letter, row and column coordinates may be assigned. Horizontal lines may be identified by capital letters and vertical rows by numbers. Thus, A1 equates to the first letter of the cryptogram, row A, column 1. This format is shown in figure 8–9.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
A	Q	F	F	Q	U	P	K	R	T	T	S	W	Z	R	G	Q	F	N	W	D
B	A	E	R	L	N	W	D	A	N	W	D	A	F	A	O	A	D	D	A	K
C	O	A	D	G	R	G	Z	R	G	J	R	U	R	G	R	F	M	A	X	U
D	D	A	E	E	D	A	Q	V	E	E	W	J	W	G	E	R	L	E	W	J
E	W	G	E	F	A	H	M	A	I	D	D	W	Z	R	O	W	G	F	K	R
F	T	T	E	H	W	Q	D	G	W	Q	V	Q	F	F	Q	U	P	E	F	A
G	H	V	R	J	R	E	R	A	G	U	A	O	O	Q	G	V	A	X	X	A
H	I	D	F	C	V	R	J	R	E	R	A	G	K	R	T	T	S	W	O	A
I	J	W	V	X	D	A	O	U	D	A	E	E	D	A	Q	V	E	F	C	D
J	W	W	N	W	D	A	F	C	D	W	W	F	A	D	A	Q	V	Y	I	G
K	U	F	R	A	G	W	R	Z	C	F	E	W	J	W	G	E	R	L	E	F
L	A	H	A	G	W	A	G	W	D	W	Z	R	O	N	G	F	R	E	V	R
M	J	R	E	R	A	G	D	W	E	W	D	J	W	X	Y					

Figure 8–9 (~~C~~). Ciphertext work sheet (U).

c. After the work sheet is prepared, the text is closely examined for repetitions within the text. Such repetitions, a characteristic of monoalphabetic substitution, are indications of identical words or expressions in the underlying plaintext and prove to be extremely useful in the assumption of letters and whole words. The search normally begins for digraphic and trigraphic repetitions, these being easiest to locate. They are further examined for possible extension of repetitions of greater length. In the search, note any reversible repetitions. As the repetitions are found, underscore them indicating the direction of progression of reversible digraphs by an arrowhead. Properly marked, the work sheet appears as in figure 8–10.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
A	Q	F	F	Q	U	P	K	R	T	T	S	W	Z	R	G	Q	F	N	W	D
B	A	E	R	L	N	W	D	A	H	W	D	A	F	A	O	A	D	D	A	K
C	O	A	D	G	R	G	Z	R	G	J	R	U	R	G	R	F	M	A	X	U
D	D	A	E	E	D	A	Q	V	E	E	W	J	W	G	E	R	L	E	W	J
E	W	G	E	F	A	H	M	A	I	D	D	W	Z	R	O	W	G	F	K	R
F	T	T	E	H	W	Q	D	G	W	Q	V	Q	F	F	Q	U	P	E	F	A
G	H	V	R	J	R	E	R	A	G	U	A	O	O	Q	G	V	A	X	X	A
H	I	D	F	C	V	R	J	R	E	R	A	G	K	R	T	T	S	W	O	A
I	J	W	V	X	D	A	O	U	D	A	E	E	D	A	Q	V	E	F	C	D
J	W	W	N	W	D	A	F	C	D	W	W	F	A	D	A	Q	V	Y	I	G
K	U	F	R	A	G	W	R	Z	C	F	E	W	J	W	G	E	R	L	E	F
L	A	H	A	G	W	A	G	W	D	W	Z	R	O	N	G	F	R	E	V	R
M	J	R	E	R	A	G	D	W	E	W	D	J	W	X	Y					

Figure 8–10 (~~C~~). Ciphertext prepared for analysis (U).

8–13. (~~C~~) Biliteral and Triliteral Frequency Distribution

a. In order to study and make use of the repeated patterns underscored, a frequency distribution of digraphs and trigraphs may be made. Properly compiled, this data provides a base for comparison of repeats in the ciphertext against similar digraphs and trigraphs which occur in English plaintext, and which also aids in the identification of vowels and consonants. Basically there are three methods of compiling this data.

(1) Each letter of the ciphertext may be shown with its two preceding letters, a triliteral distribution with two prefixes.

(2) Each letter may be shown with its two succeeding letters, a triliteral distribution with two suffixes.

(3) Each letter may be shown with its preceding and succeeding letters, a triliteral distribution with one prefix and one suffix.

b. For the study of monoalphabetic ciphers, the last method is most satisfactory and will be used here. In its construction, it is quite simple. Across the bottom of a sheet of cross section paper, a cipher alphabet is inscribed in its normal order. Above each letter, arranged in columns, the letters which precede and succeed it in the ciphertext are entered. The paired letters then represent the prefix and suffix, in that order, of the letter they are inscribed above. Below the horizontal alphabet in parentheses is the frequency value of that letter, the same values that appear in the uniliteral frequency distribution. An example of this method of constructing a triliteral frequency distribution using the ciphertext is shown in figure 8–11.

(30)	(0)	(4)	(22)	(21)	(18)	(13)	(4)	(3)	(9)	(4)	(3)	(2)	(5)	(8)	(2)	(11)	(26)	(2)	(6)	(7)	(9)	(30)	(6)	(1)	(5)
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
DE		FV	WA	AR	QF	RQ	AM	AD	GR	PR	RE	FA	FW	AA	UK	-F	KT	TW	RT	QP	QE	SZ	AU	VI	WR
			WA								RN					FU	ZG					ND			
DN		FD	WA	AE	FQ	DR	EW	AD	WW	AO	RE	HA	LW	KA	UE	GF	EL	TW	TS	RR	QQ	ND	AX		GR
DF					QU								AW								HR	AV			
FO		FD	AD	ED	AA	RZ	AV	YG	WW	FR			WW	RW		AV			RT	XD	GA	ND	XA		WR
																	GG					EJ			
OD		ZF	DA	VE	RM	RJ	AA		RR	GR			OG	AO		WD	ZG		TE	QP	CR	JG	VD		RC
DK																						GD			
OD			AG	EW	EA	RR			RR					OG		WV	JU		RT	GA	WX	EJ	WY		WR
																	UG					OG			
MX			UA	GR	GK	WE			AW					WA		VF	GF		TS	OD	QE	JG	X-		
DE			EA	LW	QF	WE			WW					AU		FU	EL			GF	QY	DZ			
DQ			ID	GF	FQ	WF			RR					RN		OG	ZO				ER	OG			
FH			DW	TH	EA	DW			DW							AV	KT					HQ			
MI			QG	PF	DC	AU										AV	VJ					GQ			
FH			IF	RR	EC	QV											JE					SO			
RG			XA	RR	AC	AK											EA					JV			
UO			UA	AE	WA	IU											VJ					DW			
VX			EA	ED	UR	AW											JE					WN			
XI			CW	VF	CE	WE											EA					ND			
RG			WA	FW	EA	AW											KT					DW			
OJ			CW	GR	GR	AW											FA					WF			
DO			AA	LG													WZ					AV			
DE			WW	RV		WF											EL					GR			
DQ			GW	RR		AD											ZO					EJ			
DF.			WJ	WW													FE					JG			
FD																	VJ					GA			
DQ																	JE					GD			
RG																	EA					DZ			
FH																						DE			
HG																						OG			
WG																						ED			
RG																						JX			

Figure 8–11 (~~C~~). *Triliteral frequency distribution* (*U*).

c. The method used in figure 8–11 constructing the triliteral frequency distribution provides a complete list of all trigraphs and all digraphs in the cryptogram. Using the table, repeated trigraphs and digraphs can be quickly isolated. In studying the digraphs, it is immaterial whether prefix and base letter, or base letter and suffix, is used, as long as the same pair 's used consistently. For example, the digraphs *DA*, *RA*, and *FA* are found using prefix and base letter *A*; the same digraph can be found when base letter *D*, *R*, and *F* are combined with their suffixes.

d. From the triliteral frequency distribution, figure 8–11, the analyst can extract a listing of those elements most frequently repeated in order to develop a condensed table of repetitions. This table should also include word-length repeats found in the initial examination of the text. The purpose of making a condensed table of repetitions is to limit the study to those items of the greatest probable importance. Therefore in this table, as an arbitrary rule for messages of average length, digraphs and trigraphs which occur less than four and three times respectively need not be listed. At the option of the analyst, digraphs of repeated letters, regardless of number of repetitions, may be listed. Following each item listed, the frequency of its occurrence should also be included. Figure 8–12 following, is an example of a condensed table of repetitions drawn from the triliteral frequency distribution above and the message text.

DIGRAPHS

DA-11	*WD*-6	*RE*-4	*EF*-4	*AG*-6
FA-5		*EE*-3	*FF*-2	*WG*-5
RA-4				
OO-1	*AQ*-3	*ER*-6	*TT*-3	*DW*-5
		ZR-4		*JW*-5
				EW-4
				NW-4
				GW-4

TRIGRAPHS

RAG-4	*WDA*-4	*RER*-3	*RTT*-3	*WJW*-3
FAH-3	*ERA*-3	*ERL*-3	*AGW*-3	*NWD*-4
DAQ-3	*JRE*-3	*KRT*-3	*WGE*-3	*EWJ*-3
DAE-3	*VRJ*-3	*EFA*-3	*RJR*-3	*AQV*-3

POLYGRAPHS

VRJREPAG-3	*QFFQUP*-2	*NWDA*-4
WJWGE-3	*DAQV*-3	

Figure 8-12 (~~C~~). *Condensed table of repetitions* (*U*).

8-14. (~~C~~) Analysis of Vowel-Consonant Relationship

a. By applying certain known characteristics to the elements previously isolated, it is possible to classify the high-frequency cipher letters into two groups, probable consonants and probable vowels. This classification in turn permits the assumption of plaintext values for those elements, values which then can be substituted for ciphertext in the cryptogram. The basis for this classification is quite simple. The manner in which vowels and consonants combine with each other and among themselves is different in each case, and they combine with characteristic frequency. An example of these characteristic frequencies is seen in the tables of digraphic frequencies in appendix A. Examination shows that the 18 digraphs representing 25 percent of all digraphs are composed of the letters:

E T N R O A I S D H V

With the exception of the H and the V, the normal high-frequency vowels and consonants will account for approximately two-thirds of the cryptogram above although they represent only a little more than one-third of the alphabet.

b. Further examination reveals that of the 18 digraphs, 9 contain an *E*, three of which are reversed.

ED	EN	ER	ES		
	NE	RE	SE	TE	VE

Of the remaining nine digraphs, five contain an N, four contain a T, four are a consonant combination, and none are combinations of vowels.

A N	S T
I N	T H
O N	T O
N D	O R
N T	

Of the vowels, E combines most readily, and then with the N, R, S, T, D, and V in that order. N combines most readily with the vowels, specifically with E, O, I, and A, in that order. The consonant T combines most readily with other consonants, the N, H, and S, in that order. Therefore, if several high-frequency cipher letters are observed combining with one letter, the assumed value of Ep, they may be assumed to be the equivalents of N, R, S, and T. D and V would be low-frequency combinations. Those cipher letters assumed to be consonants should be observed in combination with another group of high-frequency cipher letters representing the vowels, A, I, and O. Generally vowel combinations are limited and should not be observed in combination with any great frequency. But certain diphthongs may appear in the text, and since the digraphs are drawn from the ciphertext in sequential order, any one may represent a word bridge thereby forming a vowel combination. For example, the following phrase enciphered, results in an *EO* combination:

SHIFT FIRE ON SCHEDULE

EO Digraph

c. To apply the foregoing principles, the analyst will use the uniliteral frequency distribution, the triliteral frequency distribution, and the condensed table of repetitions. Only after all the high-frequency cipher letters and combinations contained therein are studied will any deduced values be applied to the cryptogram. The first step then is to list the high-frequency cipher letters of the cryptogram using the uniliteral frequency distribution previously prepared.

A	*W*	*R*	*D*	*E*	*G*	*F*	*Q*	*J*	*V*
3	3	2	2	2	1	1	1	9	9
0	0	6	2	1	9	8	1		

By their frequency of occurrence, the cipher letters probably represent the plaintext letters:

E T N R O A I S D H

On the basis of frequency, both *Ac* and *Wc* are equally good choices for Ep. By using the triliteral frequency distribution, the combinations of these letters can be written out for consideration, using the following format depicted in figure 8–13 which shows both combinations and frequencies.

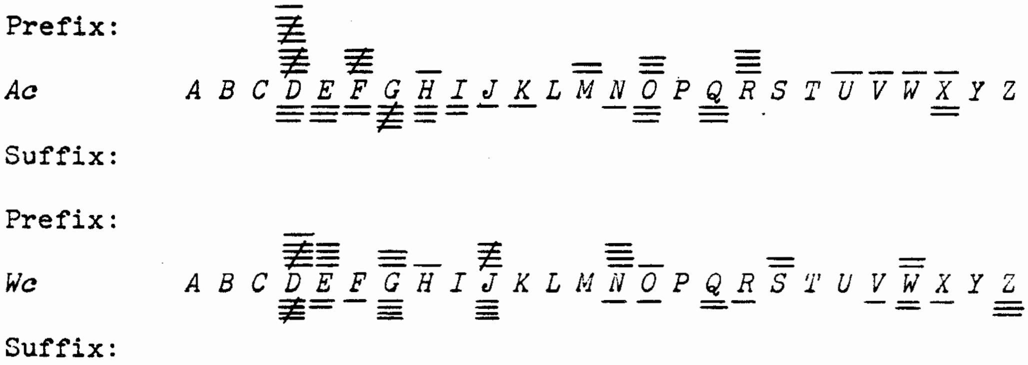

Prefix:
Ac
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Suffix:
Prefix:
Wc
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Suffix:

Figure 8–13 (C). Vowel consonant relationships (U).

Of the two sets of combinations, that of *Wc* with *Dc*, *Ec*, *Gc*, and *Jc* seems more suggestive of Ep combining with Np, Rp, Sp, and Tp to form the reversible digraphs noted in preceding paragraphs than does the possible combinations exhibited by *Ac*. For this reason, the choice of *Wc* as Ep is assumed. If in the course of further study this assumption proves incorrect, the *Ac* value will be assumed to be Ep and the data studied in that light.

d. If *Wc* is Ep, it follows that *Dc*, *Ec*, *Gc*, and *Jc* represent consonants. And, if this is correct, they should be found in combination with other high-frequency letters which represent the vowels A, I, O, and U. Using the condensed table of repetitions, these letters are seen as combining readily with *Ac* and *Rc* and less readily with the cipher letters *Nc*, *Fc*, and *Oc*. The cipher letters *A* and *R* probably represent the cipher equivalents for two of the plaintext vowels A, I, O, and U. The letters *Nc*, *Fc*, and *Qc* probably represent consonants.

	Vowels	Consonants	Possible Consonants
cipher	*WAR*	*DEGJ*	*NFQ*
assumed plain	(E)		

(1) Further identification of vowels can be made on the basis of the occurrence of dipthongs. The table of digraphs shows that the most frequently used dipthongs are:

dipthongs:	IO	OU	EA	EI	AI	IE	AU	EO	AY	UE
frequency:	41	37	35	27	17	13	13	12	12	11

Referring to figure 8–12, the digraph *RAc* appears quite frequently. *Ac* and *Rc* being assumed vowels, the *RA* combination should represent a diphthong, and by frequency of occurrence the diphthong IO is suggested. The frequencies of the individual letters, *Rc* and *Ac* are such that they correspond to the expected frequency of Ip and Op. Thus the plaintext values of I and O are assigned to *Rc* and *Ac* respectively.

(2) Returning to the suspect consonants, it is noted that the cipher letters *D, E, G,* and *J* combine well with the assumed Ep (*Wc*) suggesting that they

represent four of the plain consonants N, R, S, T, and V. The frequency of combination of those letters is as follows:

R E	(98)	E R	(87)
T E	(7)	E T	(37)
N E	(57)	E N	(111)
V E	(57)	E V	(20)
S E	(49)	E S	(54)

Study of prior tabulations reveals that *Wc* (Ep) combines with *D*, *E*, *G*, and *J* cipher as shown in figure 8–14.

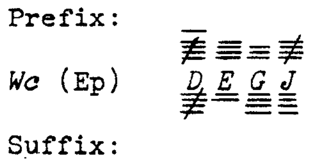


Figure 8–14 (C). Analysis of Wc as Ep (U).

Dc, as the most frequent combination with *Wc*, is accepted tentatively as Rp. The *Ec* combination is noncommittal but the *Gc* also shows a good reversal pattern, similar to the NE–EN reversal. Further, the trigraph *RAG* is noted on the condensed table of repetitions as being of relatively high frequency. By previously assumed values, this trigraph equates to ION if *Gc*=Np. Referring to figure 8–12, the *RAGc* is seen as a word ending occurring three times, each time preceded by *Ec*. The plaintext trigraph ION is one of the most common trigraphs and is usually preceded by T or S, the T being more common. Thus *Ec* likely represents either T or S plaintext. The preceding table of combinations shows that the value of combinations of E with S and T are almost equal. Both are equally good doublets, i.e. TT or SS. Therefore, since the evidence is inconclusive for the moment, the *Ec* is not considered further.

e. The cipher letter *F* is the next to be examined. In the condensed table it is observed as appearing in combination with *Ec*, either Sp or Tp as *EFc*, and in combination with itself as a doublet *FFc*. Although the *F* has a high frequency (18) the latter appearance casts doubt on its being a vowel. Vowels as doublets have the following frequencies:

AA	3
EE	42
II	–
OO	6
UU	–
YY	–

The assumed cipher values for Ap and Ep exclude two possibilities, and the expected frequency of the OO doublet is so low that it would hardly fit the number of occurrences of the doublet *FFc*. Therefore *Fc* is assumed to be a consonant. The high-frequency consonants appear as doublets with a frequency of:

TT 19	SS 19	VV 0
NN 8	DD 8	
RR 11	HH 0	

Considering the foregoing frequencies, it is obvious that *Fc* can also equal Sp or Tp, giving rise to several possible combinations with *Ec*, which also can be either Sp or Tp.

	Ec = Sp and *Fc* = Tp		*Ec*	= Tp and *Fc* = Sp
thus	*EFc* = STp =	or thus	*EFc* =	TSp
	FFc = TTp		*FFc* =	SSp
	EEc = SSp		*EEc* =	TTp

Faced with this choice where the frequency of occurrence within the cryptogram is equal, one other possibility is open for use in identifying the correct plain-to-cipher equation. This is done by checking the relative plaintext occurrences of the digraphs ST and TS. The digraphic frequency table figure 8–1, shows that TS has a frequency value of 19 while the value of ST is 63. Therefore, the first combination above, where *EFc* = STp, and where *Ec* = Sp and *Fc* = Tp may be accepted.

8–15. (C) Analysis of Word Pattern

a. To this point the following values have been assumed:

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C					*W*				*R*					*G*	*A*			*D*	*E*	*F*						

The analyst could, using the same techniques described, continue the identification of single letters by combining the recovered values of cipher letters with unrecovered cipher letters, playing the resultant frequency of the digraphs against those listed in the appropriate frequency tables. However, there is another method of establishing the identification of individual letters. This is through the use of word patterns and the probable word method.

b. In foregoing paragraphs, stereotypes in military communications are mentioned. These are certain words, phrases, and abbreviations occurring with regularity. Not only do certain words appear with a greater frequency than others, but also certain words exhibit specific characteristics of pattern and letter usage which are useful to the analyst. Consider the following words:

OCCUPY	BATTALION	DEFENSE
LOSSES	COMMANDING	

Each is composed of certain letters which occur in patterned regularity, certain letters being repeated. This phenomenon, called idiomorphism, provides a means whereby certain words are readily identified and their plain letter values assumed. As a means of deciphering idiomorphic patterns and classifying them, a literal symbol is assigned to the first letter of a distinctive pattern and to each succeeding different letter. For example, the words above are classified as:

```
    AA          ABBA               AABA
O   CC UPY   B  ATTA LION     LO   SSES
    ABACDA       AABCDEC
D   EFENSE   CO MMANDIN G
```

Note that the letters A, B, C, D, E, etc. are assigned beginning with the first repeated letter of the word. Each time the word letter is repeated, the same pattern letter is also repeated. As can be observed in the foregoing examples, patterns span repeated letters in the word.

c. The same system of classification is applied to cipher repeats that occur in monoalphabetic substitution. For example, the polygraphs contained in the condensed table of repetitions are classified into the following idiomorphic classes:

```
  ABACA        ABBA       ABCD
V RJRER AS     QFFQ UP    NWDA
  ABA          ABCD
  WJWGE        DAQU
```

There are two general ways that these word patterns are used:

(1) In those cases where no cipher-to-plain values have been recovered, the analyst assumes that a specific pattern is a given word. This process is in reality only a form of guessing, the correctness of the guess being directly related to the analyst's familiarity with the general circumstances surrounding the message and the general nature of its contents. The use of this method may or may not be helpful. Where a word is assumed, values can be assumed which can be applied to other probable words, each in turn generating new values. In some cases however, this method involves more time and effort than a straightforward analytic approach.

(2) The second case involves the use of this method in conjunction with other normal analytic approaches. Specifically, the values derived from a study of vowel-consonant relationships are applied, in most cases, to word patterns thus providing a firmer base for the assumption of probable words. For example, the cipher polygraphs preceding are reduced to partial plaintext as follows:

Idiomorphic class:	A B A C A	A B B A
Cipher:	*V RJRER AG*	*QFFQUP*
Plaintext:	— I — I S I ON	— T T — —

(3) The analyst, by referring to the listing of idiomorphic word patterns in appendix D–3, can search the appropriate class for words which contain the correct plaintext elements. In doing this, remember that the elements dealt with here are word patterns and not lengths. The pattern derived from an examination of the ciphertext may represent either a complete word, a word fragment, or even parts of two adjacent words used in the plaintext. Scanning the word list of idiomorphic pattern ABACA, only one word is found within this class that contains the correct plaintext values.

```
C   VRJRER—AG
P   -I-ISION
    DIVISION
```

In the case of the idiomorphic pattern ABBA, several possible words which conform to the requirements are found.

```
C   QFFQUP
P    TT
    ATTACH
    ATTACK
```

Although each word is different, they both contain the repeated A. Therefore *Qc* can be equated to Ap.

d. By transferring the new plaintext values with their associated cipher values, the enciphering sequence is now expanded to:

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	*Q*			*V*	*W*				*R*					*G*	*A*			*D*	*E*	*F*		*J*				

At this point, the analyst may choose one of four possible routes toward a final solution, or may use any combination of these routes.

(1) Continue a study of word patterns.

(2) Revert to a study of digraphs.

(3) Attempt to reconstruct the alphabet above using its obvious sequences to assume letter values and then checking them by (1) and (2) above.

(4) Begin substituting the plaintext values now recovered for the appropriate ciphertext values in the message and then attempting to find additional values by reading out valid plaintext.

8-16. (C) Substituting Deduced Values

a. Thus far the values accepted as being correct are almost purely hypothetical. They have been tested against one another in combinations divorced from their context in the message. No matter how valid any of the values may seem to be, the final test of their validity lies in their consistent application to the ciphertext to produce intelligible plaintext. As an aid, the analyst may rearrange the cipher-to-plaintext relationship to produce a deciphering alphabet to decipher the message. This, and the partially recovered plaintext is shown in figure 8-15.

C	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
P	O			R	S	T	N			V							A	I				D	E			

```
   1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20

A  Q  F  F  Q  U  P  K  R  T  T  S  W  Z  R  G  Q  F  N  W  D
   A  T  T  A           I           E     I  N  A  T     E  R
B  A  E  R  L  N  W  D  A  N  W  D  A  F  A  O  A  D  D  A  K
   O  S  I        E  R  O     E  R  O  T  O     O  R  R  O
C  O  A  D  G  R  G  Z  R  G  J  R  U  R  G  R  F  M  A  X  U
      O  R  N  I  N     I  N  V  I     I  N  I  T     O
D  D  A  E  E  D  A  Q  V  E  E  W  J  W  G  E  R  L  E  W  J
   R  O  S  S  R  O  A  D  S  S  E  V  E  N  S  I     S  E  V
E  W  G  E  F  A  H  M  A  I  D  D  W  Z  R  O  W  G  F  K  R
   E  N  S  T  O        O     R  R  E     I     E  N  T     I
F  T  T  E  H  W  Q  D  G  W  Q  V  Q  F  F  Q  U  P  E  F  A
         S     E  A  R     E  A  D  A  T  T  A        S  T  O
G  H  V  R  J  R  E  R  A  G  U  A  O  O  Q  G  V  A  X  X  A
      D  I  V  I  S  I  O  N     O        A  N  D  O        O
H  I  D  E  C  V  R  J  R  E  R  A  G  L  R  T  T  S  W  O  A
      R  T     D  I  V  I  S  I  O  N     I
I  J  W  V  X  D  A  O  U  D  A  E  E  D  A  Q  V  E  F  C  D
   V  E  D     R  O        R  O  S  S  R  O  A  D  S  T     R
J  W  W  N  W  D  A  F  C  D  W  W  F  A  D  A  Q  V  Y  I  G
   E  E     E  R  O  T     R  E  E  T  O  R  O  A  D        N
K  U  F  R  A  G  W  R  Z  C  F  E  W  J  W  G  E  R  L  E  F
      T  I  O  N  E  I        T  S  E  V  E  N  S  I     S  T
L  A  H  A  G  W  A  G  W  D  W  Z  R  O  W  G  F  R  E  V  R
   O     O  N  E  O  N  E  R  E     I     E  N  T  I  S  D  I
M  J  R  E  R  A  G  D  W  E  W  D  J  W  X  Y
   V  I  S  I  O  N  R  E  S  E  R  V  E
```

Figure 8-15 (C). Partially recovered plaintext (U).

b. Examination of the partially recovered plaintext now reveals several sequences which, although incomplete, contain a sufficient number of key letters to make the identification of the others relatively simple. These newly assumed letters may then be substituted for other cipher letters. For example, the sequence A1 through C17 probably reads:

"ATTACK WILL BEGIN AT ZERO SIX ZERO ZERO
TOMORROW MORNING"

From this sequence the cipher-to-plain value can be drawn:

C	*U*	*P*	*K*	*T*	*S*	*Z*	*N*	*L*	*O*
P	C	K	W	*L*	*B*	*G*	Z	X	M

The deciphering alphabet now appears as:

C	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
P	O			R	S	T	N	P			W	X		Z	M	K	A	I	B	L	C		E			G

Using the alphabet for further decipherment, again assuming letters, the message can be deciphered to read:

"ATTACK WILL BEGIN AT ZERO SIX ZERO ZERO TOMORROW
MORNING IN VICINITY OF CROSSROADS SEVEN SIX
SEVEN STOP YOUR REGIMENT WILL SPEARHEAD ATTACK
STOP DIVISION COMMAND OF FOURTH DIVISION
WILL BE MOVED FROM CROSSROADS THREE ZERO THREE
TO ROAD JUNCTION EIGHT SEVEN SIX STOP ONE ONE
REGIMENT IS DIVISION RESERVE"

The cipher alphabet used is:

C	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
P	O	Q	H	R	S	T	N	P	U	V	W	X	Y	Z	M	K	A	I	B	L	C	D	E	F	J	G

By rearranging the values of the two sequences, the enciphering alphabet can be derived and the keyword found.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	*Q*	*S*	*U*	*V*	*W*	*X*	*Z*	*C*	*R*	*Y*	*P*	*T*	*O*	*G*	*A*	*H*	*B*	*D*	*E*	*F*	*I*	*J*	*K*	*L*	*M*	*N*

Keyword: CRYPTOGRAPHY
Hp = *Cc*

c. The example presented in the preceding paragraphs, being an artificial illustration set up to demonstrate general principles, is relatively easy to solve. This is so because the frequencies of the various elements analyzed: letters, digraphs, trigraphs, and word patterns, correspond well with that expected. This is not always the case. The principles illustrated are general in nature and application, and depend upon the formulation of assumptions. Recognize that any assumption may be incorrect as well as correct, the best means of determination being to test each, casting out those that prove incorrect. The analyst will find it most profitable to vary the analytic approach thus providing a source of additional assumptions. In some cases, a single approach may suffice to solve a simple cryptogram, but in the long run, the more varied the techniques employed the surer the solution.

8–17. (~~C~~) The Consonant Line Method

a. Another method for the determination of vowel and consonant equivalents, which is extremely useful in difficult cases of monoalphabetic substitution, is the consonant line method. This method makes use of the positions of letters in the ciphertext relative to the occurrence of adjacent letters and is based upon the tendency for low-frequency consonants to be flanked on one or both sides by vowels. If a distribution is made of the contacts of the low-frequency ciphertext letters of a monoalphabetic cryptogram, vowel-equivalents can be distinguished from consonants in that they are usually represented by a combination of the following characteristics:

(1) They are usually high-frequency letters.

(2) They have a variety of contacts.

(3) They combine readily with low-frequency letters.

(4) They do not combine readily with one another and less so with themselves.

b. The identification of possible vowels using the foregoing characteristics is simplified by the construction of a consonant line diagram, an enlarged T. For example, construct a triliteral frequency distribution, see figure 8–16.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
		US	SZ	-Y	QY		ZU	QP	UQ	ZR	QD	QR	KV		QS	ZX	EU	CE	ZY	HC	NS	QE	QX	EZ	YH
		DQ	LQ	SE	VZ		PQ	JQ	SE	SN	EQ		XQ		IH	XC	YS	ED	RW	RJ	UQ	QH	XQ	ER	DQ
			ZD	ES	ER		JQ	EZ	QJ	US					SY	DP	HZ	PE	XP	SJ	QF	TX	ZR	TE	RT
			DC	SR	VS		WR	HZ	JH						XR	JW	KJ	RJ		XU	SJ	JX	WS	FR	IK
			ZD	WY	WF		QE	RH	UI						TQ	EI	YS	QU		RS	QF	JF	SU	PZ	YX
			DX	JQ	FQ		SI	QE	RE							HJ	XT	RK		SK	HQ	SD	QY	XZ	IH
			SE	YI			ZR	QS	RQ							HS	HI	VP		QS			DZ	RS	FD
			WE	JQ			IQ		SY							IW	MJ	XX		XZ			ZR	JS	YD
				YI			RZ		ZW							EF	XE	EH					GR		XX
				JQ			SV		VR							VH	XY	YJ					SP		YJ
				HS			QE		SJ							HV	EU	YD					WZ		XE
				RL			QE		QW							CM	PQ	UU					RU		HQ
				DR					JS							JX	FH	KX					ZT		UX
				IY												LQ	JX	UV					SN		
				ZF												QX		FX							
				HS												RI		IH							
				HQ												ZU		EJ							
				D-												PV		JW							
																NI									
																EJ									
																FH									
																VH									

Figure 8–16 (~~C~~). Triliteral frequency distribution (U).

Using the triliteral distribution of figure 8–16, a consonant line diagram is constructed as in figure 8–17. Above the crossbar, all low-frequency letters of the distribution (C, K, L, M, N, P, T, V, F, W) are inscribed horizontally, repeated on the right and the left. Below the crossbar, the letters used as prefixes are inscribed to the left of the vertical part, under the letters they precede. Those letters used as suffixes are inscribed to the right, under the letter they follow.

CONSONANT LINE

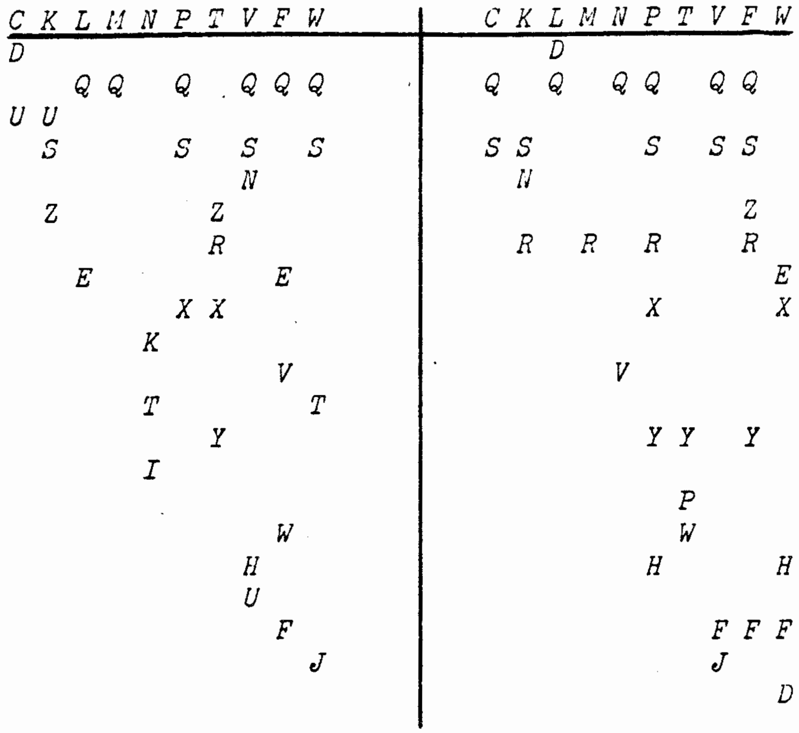


Figure 8–17 (~~C~~). Consonant line diagram (U).

c. Considering both the number of contacts and their variety shown in the diagram, it is likely that the cipher letters *Q*, *S*, and *R* are vowel equivalents. The cipher letters *X*, *Z*, and *E* also appear possible as does *Y*. However, they represent a total of seven letters where there are only six vowels. The normal frequency of Up and Yp is less than the high-frequency consonants. Therefore, the last four cipher letters probably contain one or more consonant equivalents. Having isolated three vowel equivalents with some certainty and four other letters as probably representing several vowel equivalents, the analyst has several options.

(1) With the most likely vowel equivalents, the procedures given in the study of vowel-consonant relationship may be followed to determine the identity of each vowel and associated high-frequency consonants.

(2) A study of each vowel's contacts can be made in order to classify additional consonant equivalents. For this, a vowel line is constructed (fig. 8–18), for those most likely vowel equivalents. This line may be constructed like the consonant line, or as a simplified form given below. In either case, the intent is to tabulate the contacts of the vowel equivalents, having in mind the characteristic of a vowel contacting a consonant more often than it contacts another vowel, or itself.

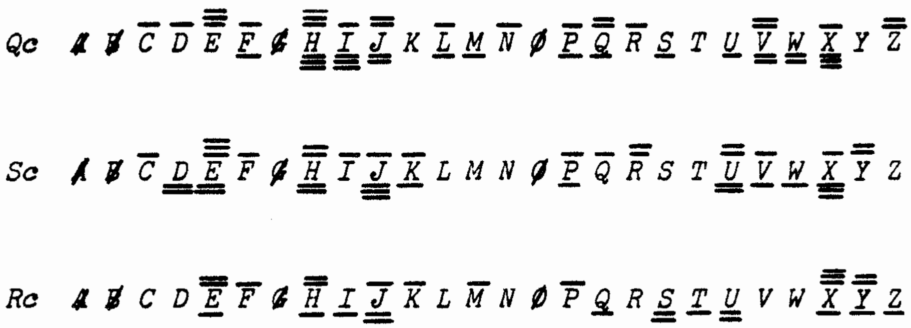


Figure 8–18 (~~C~~). Vowel equivalent line (U).

d. Examination of the *Qc* vowel-equivalent line reveals that *Hc, Ic, Jc, Vc,* and *Xc* are probably consonant equivalents. The *Sc* line tends to confirm the *Jc* and *Xc* consonant-equivalent assumption, and also indicates that the *Ec* may also be a consonant equivalent. The *Rc* line confirms *Ec, Hc, Jc,* and *Xc* as probable consonant equivalents, and also indicates that *Yc* may also be a consonant equivalent. Thus far then, the following assumptions appear logical:

Vowel Equivalents: *Qc, Sc, Rc*
Consonant Equivalents: *Ec, Hc, Ic, Jc, Vc, Xc,* and *Yc*

If the above assumptions are valid, only the *Zc* of the questionable vowel equivalent is actually a vowel equivalent. At this point, the analyst resorts to a study of the characteristics of vowels and consonants in combination and relation to one another to discover the correct plaintext equivalent for each cipher value.

CHAPTER 9 (~~C~~)

MULTILITERAL MONOALPHABETIC SUBSTITUTION SYSTEMS

Section I. (C) CHARACTERISTICS AND TYPES

9–1. (~~C~~) Introduction

a. Monoalphabetic substitution is classified into either uniliteral or multiliteral. In the former, there is a strict one-to-one character relationship between the units of the plaintext and the units of the ciphertext. A multiliteral monoalphabetic substitution cipher, on the other hand, is a cryptographic system that produces ciphertext units of two or more characters for each equivalent character of the plaintext.

b. The term multiliteral is used in cryptography in its broadest sense. It is applied to those systems which exhibit a constant relationship between one ciphertext unit and one plaintext unit, regardless of whether the system employs letters, numbers, or special symbols as the ciphertext character. For specific reference, multiliteral systems are classified by the number and type of ciphertext characters used to replace each plaintext unit.

(1) Biliteral refers to systems involving the use of two-letter ciphertext units.

(2) Triliteral refers to systems involving the use of three-letter ciphertext units.

(3) Dinomic refers to those systems involving the use of two-figure ciphertext units.

(4) Trinomic refers to those systems involving the use of three-figure ciphertext units.

c. Multiliteral systems in general represent an attempt to offer greater security than the simple uniliteral cipher systems. Once the principle of solving uniliteral substitution systems by the analysis of the plaintext characteristics reflected in the ciphertext became known, the cryptographer, sought methods that would either disguise, suppress, or eliminate these characteristic frequencies or patterns in the ciphertext. Among the multiliteral systems developed are simple biliteral systems, biliteral systems using variants, and multinomic systems.

9–2. (~~C~~) Simple Biliteral Substitution

a. In simple biliteral substitution systems, figure 9–1, the ciphertext unit to plaintext unit ratio is a constant 2 to 1. The ciphertext unit is either a letter or number, with its identity having little or no effect upon either the cryptographic process or the cryptanalysis of the ciphertext produced. Generally, these systems are based upon a matrix which contains the plain component alphabet. Row and column coordinates form the ciphertext units which are substituted for each plaintext value. Note that to fit the alphabets to the dimensions of the matrices, the I and J are combined into a single cell in the first; the I and J, U and V are combined in the second matrix.

	R	*I*	*D*	*G*	*E*
C	*A*	*B*	*C*	*D*	*E*
R	*F*	*G*	*H*	*I*	*K*
E	*L*	*M*	*N*	*O*	*P*
S	*Q*	*R*	*S*	*T*	*U*
T	*V*	*W*	*X*	*Y*	*Z*

CRc = Ap

	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
3	*A*	*D*	*G*	*K*	*N*	*Q*	*T*	*X*
2	*B*	*E*	*H*	*L*	*O*	*R*	*V*	*Y*
1	*C*	*F*	*I*	*M*	*P*	*S*	*W*	*Z*

31c = Ap

Figure 9–1 (~~C~~). Simple biliteral substitution systems (U).

b. In figure 9–1, the plaintext component is limited to 25 and 24 characters respectively by combining certain values which could be used interchangeably without causing a loss of intelligibility. Encryption in either of the systems is the same. The plaintext equivalent is located within the matrix, and the row and column coordinates indicate its position in its ciphertext value. For example, the message below could be enciphered as shown:

S E N D R E I N F O R C E M E N T S X X

SDCEEDCG SICERGEDRREGSICDCEEICEEDSGSD TDTD

SDCEE DCGSI CERGE DRREG SICDC EEICE EDSGS DTDTD

or

SEND REINFORCEMENTS XX

16223532 26221335122526112214223537 16 3838

16223 53226 22133 51225 26112 21422 35371 63838

c. The process of decipherment is the reverse of the process of encipherment. The cryptographer breaks the ciphertext into digraphs or dinomes and, using these as coordinates, locates their equivalent plaintext value. Note that in these particular systems, the order of selecting the row and column coordinates as ciphertext values must be predetermined as row and column or as column and row. Normally the former system, similar to reading map coordinates, is used.

d. The biliteral and dinomic alphabet produced by the system illustrated above is also termed bipartite, as each cipher element can be divided into two distinct parts, each having a clearly defined function as row or column coordinates. On occasion, the systems illustrated are termed bipartite systems due to the nature of the cipher alphabet produced.

e. It is obvious to the analyst that these particular systems offer little or no difficulty. Essentially, the process does not effectively disguise either letter frequency or word pattern. Further, the bipartite nature of the alphabets produced by these systems is one of their weaknesses, making them easy to recognize by the analyst. In effect, the foregoing system does nothing more than double the length of the ciphertext, offering little more security than the uniliteral monoalphabetic substitution system. To circumvent these weaknesses, multiliteral systems employing variants were developed.

9–3. (~~C~~) Biliteral Systems With Variants

a. In a basic biliteral system, a given plaintext value is always replaced by one constant ciphertext element. Each time that letter is used again, the same ciphertext element appears. The biliteral system with variants is an attempt to provide variant ciphertext values for each plaintext value, thus suppressing the appearance of letter frequency and word patterns in the ciphertext. There are two basic methods whereby these variant values are introduced. The first, using subterfuge, results in a pseudovariant which only camouflages the true biliteral nature of the alphabet.

(1) One such method is to construct the matrix, including row and column coordinates, in such a manner that the resulting cryptogram resembles other systems. For example, using the matrix in figure 9–2, messages could be enciphered, and when the ciphertext is divided into five-letter groups, it gives the appearance of code groups.

	B	*C*	*D*	*F*	*G*
A	*A*	*B*	*C*	*D*	*E*
E	*F*	*G*	*H*	*I*	*K*
I	*L*	*M*	*N*	*O*	*P*
O	*Q*	*R*	*S*	*T*	*U*
U	*V*	*W*	*X*	*Y*	*Z*

R	A	I	D	S
OC	*AB*	*EF*	*AF*	*OD*

Figure 9–2 (~~C~~). Artificial code language matrix (U).

(2) Another method is to add additional digits, thereby disguising the bipartite nature of the alphabet. For example, where the ciphertext is composed of dinomic elements, a "sum-checking" digit which is the noncarrying sum of the two digits of the element may be used. The cryptogram produced by the dinomic system previously illustrated could be changed to appear as a trinomic system by the following operation.

CIPHERTEXT
16223 53226 22133 51225 26112 21422 35371 63838
1+6=7 167, 2+2=4 224, 3+5=8 358, etc.
CIPHERTEXT AFTER SUMMING DINOMES
16722 43583 25268 22413 43581 23257 26811 22241
45224 35837 01673 81381

(3) Even a set of randomly selected characters may be used, inserted following each digraph or dinome solely for the purpose of confusing the

analyst. But here, as in the two preceding examples, little is gained. In the first case, the limitations in the values used soon reveal the system as simple multiliteral, and the bipartite nature of its alphabet makes analysis easy. This is also true with the second case, and additionally, this particular method results in one plaintext element being replaced with three ciphertext characters—an inordinate increase of message length for security gain.

b. By far the simplest practical method of introducing variants into a multiliteral substitution system is by the use of additional row and column indicators. Figure 9–3 illustrates some of the possibilities whereby this can be accomplished.

			V	W	X	Y	Z
			Q	R	S	T	U
K	F	A	A	B	C	D	E
L	G	B	F	G	H	I	K
M	H	C	L	M	N	O	P
N	I	D	Q	R	S	T	U
O	J	E	V	W	X	Y	Z

(1)

				A	E	I	O	U
T	N	H	B	A	B	C	D	E
V	P	J	C	F	G	H	I	K
W	Q	K	D	L	M	N	C	P
X	R	L	F	Q	R	S	T	U
Z	S	M	G	V	W	X	Y	Z

(2)

					O				
					M	N			
					J	K	L		
					F	G	H	I	
					A	B	C	D	E
O	M	J	F	A	E	N	A	L	U
	N	K	G	B	T	R	S	F	W
		L	H	C	O	I	H	Y	X
			I	D	D	C	M	V	K
				E	P	G	B	Q	Z

(3)

	1	2	3	4	5
09	H	Y	D	R	A
15	U	L	I	C	B
21	E	F	G	K	M
27	N	O	P	Q	S
33	T	V	W	X	Z

(4)

				1	2	3	4	5	6	7	8	9
0	8	5	1	T	E	R	M	I	N	A	L	S
	9	6	2	B	C	D	F	G	H	J	K	O
		7	3	P	Q	U	V	W	X	Y	Z	I
			4	2	3	4	5	6	7	8	9	Ø

(5)

Figure 9–3 (~~C~~). *Multiliteral systems with variants* (*U*).

c. The matrices in figure 9–3 represent some of the simpler means of accomplishing biliteral substitution with variants. Each is disguised by one or more characteristics representative of biliterals with variants.

(1) Note that example 1 provides six possible variant cipher elements for each plaintext unit. Ap could be represented by any one of the cipher digraphs *KV*, *KQ*, *FV*, *FQ*, *AV*, or *AQ*.

(2) Example 2, which is an extension of the pseudovariant system shown in paragraph 9*b*(1), now provides four variants for each plaintext element.

(3) Example 3 illustrates a method of providing a number of variants approximately equal to the normal frequency of occurrence of a given plaintext letter. Thus Ep may be replaced by 25 different cipher equivalents, while the Kp is replaced by only two.

(4) Example 4 illustrates that a biliteral alphabet need not be a bipartite. No single element exclusively indicates row or column, i.e. the digit 1 indicates two rows of one column.

(5) Example 5 illustrates a method of providing for the normal frequency of usage of the plaintext letter, this time based upon a key word composed of high-frequency letters. It also provides for the use of digits rather than requiring that they be spelled out.

(6) Note that encipherment using matrices 1 and 2 are commutative; the coordinates can be read in any direction and the same plaintext letter is

always found. For example, in matrix number 2, *BAc* and *ABc* both equate to Ap. All other matrices illustrated are noncommutative; therefore, the method of indicating and reading out the plaintext letters must be agreed upon in advance. For example, in matrix 3 the cipher element *BD* may indicate Fp or Cp depending on whether the order is row-column, or column-row.

9–4. (~~C~~) Security of Multiliteral Monoalphabetic Substitution

The obvious disadvantage of all such methods discussed in the preceding paragraph is that the cryptographic text is exactly twice as long as the original plaintext. Moreover, there is no great compensating advantage from the standpoint of security in most cases. It is possible that the number of variants is so extensive that the system's overall security could be improved, but any such scheme would entail the risk of error in the encryption process. It has been shown through experience that when given a number of choices of variant values, the cryptographer will, over a period of time, tend to use only a very few of those available. Thus the provision of variant values by the system can be largely forfeited.

Section II. (~~C~~) ANALYSIS OF MULTILITERAL SYSTEMS

9–5. (~~C~~) Introduction

a. The analysis of simple multiliteral systems and multliteral systems with variants, whether dinomic or biliteral, involve certain similar techniques and methods. Although the more complicated variant systems may require the use of techniques particular to their case, the underlying principles are similar. Accordingly, those general principles will be explained and demonstrated in this section. Those special techniques applicable to specific cases will be developed in the succeeding section.

b. The analysis of all multiliteral systems may take one of two general courses. One method which can easily be employed in the case of a simple multiliteral system, and which under certain circumstances can be used in the case of multiliterals with variants, is the solution of the literal values as though they were monographic. This is done by using the same approach as for the analysis of uniliteral monoalphabetic substitution. To demonstrate the basis for this particular approach, examine the cryptogram given below. Herein, it can be seen that the ciphertext, produced by the system illustrated in paragraph 9–2, exhibits the same pattern repeats and letter frequencies as does the plaintext. The only difference is that the ciphertext exhibits this pattern digraphically rather than monographically.

Message

ATTACK TO BEGIN AT ZERO SIX ZERO ZERO HOURS TOMORROW XX

Ciphertext

CRSGS GCRCD RESGE GCICE RIRGE DCRSG
TECES IEGSD RGTDT ECESI EGTEC ESIEG
RDEGS ESISD SGEGE IEGSI SIEGT ITDTD

c. When the message above is reduced to uniliteral terms, the word patterns of the underlying plaintext seem to leap out.

```
A   B   B   A
CR  SG  SG  CR  CD  RE  SG  EG  CI  CE  RI  RG  ED  CR  SG
A   B   C   D                   A   B   C   D   A   B   C   D
TE  CE  SI  EG  SD  RG  TD  TE  CE  SI  EG  TE  CE  SI  EG
                            A   B   A   C   C   A
RD  EG  SE  SI  SD  SG  EG  EI  EG  SI  SI  EG  TI  TD  TD
```

d. The second general approach involves the simultaneous analysis of the ciphertext for plaintext values and the recovery of the matrix. This approach may be used for either the simple biliteral or the biliterals with variants. It is more appropriate in the case of the latter system, for all variant forms of each cipher element must be identified prior to the reduction of the cipher elements to uniliteral terms.

e. Prior to the start of any analysis, however, a system must be identified as to general class and wherever possible to the specific type within that class. In the following paragraph, methods of identifying multiliteral systems are treated in detail.

9–6. (~~C~~) Identification

a. The identification of a biliteral system is much easier than the identification of some uniliteral substitution systems. This is particularly so in the case of the simpler forms of the biliteral system. Normally, the initial basis of identification lies in the recognition of the textual limitation imposed by the number of characters used as row and column indicators and their manner of use. Where the indicators are limited in number and are bipartite in nature, identification of the system is quite easy. For example, a uniliteral frequency distribution of the following cryptogram would hardly be necessary, as the limitation in the number of letters used is obvious.

```
AHARE  SSEER  ARCSC  RSHSS  CHCHS  SASPH
ARAOC  SAECH  ARAEP  OSSCO  SEASP  HAOSE
SSASP  ESSAE  CRSEA  ESSCR  SECHA  RCOCS
AEAEA  RCRCH  SSCHC  HSSSO  PSJJJ
```

The briefest examination reveals that aside from the three J's appearing at the end of the message, these probably being nulls, there are only eight different letters used, the letters *A*, *H*, *R*, *E*, *S*, *C*, *P*, and *O* respectively. If the message is divided into digraphs and another count is made, a definite positional limitation would be observed. The letters *A*, *E*, *S*, *C*, and *P* would be found in the first position and the letters *H*, *R*, *S*, *E*, and *O* would be noted in the last position. On the basis of these limitations, the analyst could safely assume that the message represents a case of multiliteral encipherment.

b. A close examination of the message reveals several other features which are characteristics of multiliteral systems in general and which may also be used for identification purposes.

(1) The number of the letters or digits in the message, excluding nulls if they are added after encipherment of the plaintext, is a multiple of the cipher element. In the example above, there are 112 letters, or 56 digraphs. Conversely, the length of the cipher element can sometimes be derived from message length, for example, a dinomic system using sum checks. In any event, the analyst immediately explores this possibility.

(2) The number of letters or digits in repeated series are the same in each case and are a multiple of total message and cipher element length. For example, in the message above, two repeats occur: *RSHSS CHCHS SASPH* and *SSCHC HSSSO*, which are equal in length, 8 letters or 4 digraphs long.

(3) The number of letters between repeated sequences, between the beginning of the message and occurrence of first repeat, and between the end of the last repeat and the end of the message, are all multiples of two. For example, there are 18 letters before the first repeat. The repeat contains 8 letters. Following it, there are 74 intervening letters, again the 8 letters are repeated, then 4 letters to the end of the message. Each interval is a multiple of 2; hence, this is the cipher element's size.

9–7. (~~C~~) Statistical Tests

a. Just as the Phi (ϕ) and the Index of Coincidence (I.C.) tests can be applied to a cryptogram to determine whether it is monoalphabetic, so also can variations of these same tests be applied to the digraphic distribution of a cryptogram to determine whether the cryptogram in question is monoalphabetic when considered as a multiliteral cipher. The basis for the application of these tests lies in the uniliteral nature of simple multiliteral substitution and the limitations inherent in a multiliteral with variants which make it susceptible to these tests.

b. In foregoing chapters, both the ϕ and the I.C. tests are explained in terms of their application to uniliteral monoalphabetic substitution. The general form of the tests when applied to digraphic distributions remains unchanged though the values are now different. The plain and random constants and the "N" in the formulas now pertain to the number of digraphs under consideration instead of the number of single letters. The formulas are shown below:

(1) Digraphic Phi test, (2ϕ).

$2\phi o = \Sigma f(f-1)$

$2\phi p = .0069N(N-1)$

$2\phi r = .0015N(N-1)$

f = Number of occurrences of each digraph

N = Number of occurrences of all digraphs (ΣF)

(2) Digraphic 2ϕI.C. test.

$$\text{I.C.} = \frac{\Sigma C-(f-1)}{N(N-1)}$$

C = The number of possible digraphs, i.e. the number of letters in the alphabet squared. For English C = 26x26 = 676.

N = Number of occurrences of all digraphs.

f = Total number of occurrences of each digraph.

(3) The digraphic I.C. can also be determined by comparing the value of observed occurrences to the value of expected random occurrences, with the I.C. being expressed in terms of a ratio between the two values. The formula for this test may be expressed as:

$$\text{I.C.}=\frac{2\phi o}{2\phi r}$$

In the case of digraphs, the I.C. for English plaintext is 4.66 and the I.C. for digraphic English random text is 1.00.

c. These foregoing tests, as all statistical tests, are subject to a degree of error, depending upon the makeup of the cryptographic test being studied. Specifically, in the case of multiliteral systems the presence of repeated groups, the limitations in the number of different digraphs present, and the size of the sample itself all tend to distort the test results. Therefore, they must always be used with caution, with the preferential method being to employ them in conjunction with other evidence for identification purposes.

d. The first step in using any of the test steps is to tabulate the frequencies of all digraphs comprising the message, and to determine the individual value of f(f−1). This may be done as follows:

```
WMTST  SWMIM  BOIST  SWMWU  WUEMT  MHMTE  EMIUE
MHUTE  TMEMW  OEMIU  ISTOW  EEMEU  TUIST  OTSTO
TUIUI  SHSEM  WSESE  MISTS  WMHSH  UTUHS  ISESE
UEUTU  HSTST  STUHM  HSEMW  MIMIO  WUTOI  UEMXX
```

	WM	WU	WO	WE	WS	TS	TM	TE	TO	TU	IU	IS	IM
f	5	3	1	1	1	7	2	2	4	5	4	6	2
f(f−1)	20	6	0	0	0	42	2	2	12	20	12	30	2

	EO	EM	EU	ES	HS	HM	HU	
	1	10	3	2	5	2	2	Σf=N=69
	0	90	6	2	20	2	2	Σf(f−1)=270

(1) Using the values determined above, the values of the 2φ test may be computed as follows:

$2\phi o=\Sigma f(f-1)=270$
$2\phi p=.0069N(N-1)=.0069\times69\times68=31.5478$
$2\phi r=.0015N(N-1)=.0015\times69\times68=7.0380$

(2) The 2φ I.C. may be computed as follows:

$$\frac{C\ f(f-1)}{N(N-1)}=\frac{676\times270}{68\times69}=\frac{182520}{4692}=38.9$$

(3) And the second method of determining a digraphic I.C. may be computed as follows:

$$2\text{ I.C.}=\frac{2\phi o}{2\phi}=\frac{270}{7}=38$$

e. Note that in the case of the computation of 2 I.C. above, the value derived is in the value range of 31 to 43. In the case of the biliteral system the expected values for a simple biliteral fall in the range of 20 to 40, and the expected values for a biliteral with variants is 6 to 20. The extremely high difference in value computed for the digraphic Phi test lies in the fact that the test involves a comparison between an expected occurrence based on the possibility of 676 different digraphs used in plaintext, against the actual occurrence of only 69.

9–8. (~~C~~) Analysis of Biliteral Systems

a. Once the system has been satisfactorily identified, the analysis of the system may commence. The analysis may include the simultaneous attempt to recover the matrix and the establishment of plaintext values for the cipher elements.

(1) In the first case, use is made of the number and positional limitations of the cipher elements. For example, a tabulation of the letter comprising the foregoing message reveals that only nine different letters (*W*, *M*, *T*, *S*, *I*, *E*, *O*, *H*, and *U* respectively) were used. Further examination quickly reveals that there is a definite positional limitation involved. The letters *W*, *T*, *I*, *E*, and *H* occur in the first position and the letters *M*, *S*, *O*, *U*, and *E* appear in the last position. The number of the letters involved and their positional limitation immediately suggests a 5 x 5 matrix of 5 cells by 5 cells with these letters as row and column indicators. Accordingly, a matrix of this configuration figure 9–4 is set up:

	M	*S*	*O*	*U*	*E*
W					
T					
I					
E					
H					

Figure 9–4 (C). Preliminary matrix with row and column indicators (U).

(2) Note that the dimension of the assumed matrix is determined by the composition of the cipher elements. This step presupposes the correct identification of the cipher unit and correct interpretation of their positional significance. At this particular point it matters little if the row and column indicators are reversed, for a simple turn of 90° will correctly realine the indicators.

b. After identifying the row and column indicators and determining the matrix dimensions, the next step is to insert values into the cells of the matrix. It is at this point that use is made of the uniliteral nature of simple multiliteral substitution by reducing the digraphs to uniliteral terms. This may be done very easily by substituting a letter for each different digraph appearing in the cryptogram. If not more than 36 different combinations are present in the cryptogram, the extra values above 26 may be represented by digits. As a general rule, where less than 26 different cipher elements are encountered, it is advisable to reduce them to uniliteral terms. This permits the construction of a triliteral frequency distribution, and use of all other studies associated with the analysis of monoalphabetic substitution.

(1) For this purpose the tabulation of digraphs previously made may be used. Using this tabulation, one letter is assigned to each different cipher element.

WE	*WM*	*WO*	*WS*	*WU*	*TS*	*TM*	*TE*	*TO*	*TU*	*IU*	*IS*	*IM*	*IO*
A	B	C	D	E	F	G	H	I	J	K	L	M	N
EO	*EM*	*EU*	*ES*	*HS*	*HM*	*HU*							
O	P	Q	R	S	T	U							

This process results in a pseudoplaintext which reflects all the underlying characteristics of the true plaintext. Inasmuch as the same characteristics are exhibited by the ciphertext elements, there may be some question as to the need of this step. The reason for this is twofold; first, it permits the differentiation of the row and column indicators and the plaintext letter they represent (useful in the reconstruction of the matrix), and second it provides a suitable element for manipulation in applying the technique of solving monoalphabetic substitution systems. While this factor is not of any great importance in relatively short cryptograms, it is very helpful where many cipher elements are under study.

c. With the digraphs reduced to uniliteral terms and having an assumed matrix, the recovery of the plaintext may begin. In this step the frequency distribution of the pseudoplain values may be studied individually and fitted to the normal to recover their true plaintext values; or the message text may be scanned for word patterns and then compared to the frequency distribution for identification of plaintext letter values. In all cases, when a plaintext value has been recovered, it may be inserted in the matrix at the point of intersection of its cipher row and column indicators. This permits the simultaneous reconstruction of the matrix, and if it shows any symmetrical pattern, allows the placement of additional plaintext values, thus hastening the final solution. The cryptogram, reproduced in terms of the arbitrary uniliteral values previously assigned, now appears in figure 9–5 with significant repeats underlined.

B F F B M O L F B E E P G T H P K P

U H G P C P K L I A P Q J L I F I J

K L S P D R P L F B S U J S L R Q Q

J S F F J T S P B M N E I K P

Figure 9–5 (C). Ciphertext prepared for analysis (U).

(1) The patterns *ABBA* – – and *ABA* – – for the sequence *BFFBM* and *PKPUH* are suggestive of the words *ATTACK* and *ENEMY* respectively. Accepting these assumptions for the moment, the plaintext values are inscribed in the matrix using the appropriate cipher diagraphs as row and column indication.

```
   P  A   T   T    A   C   K           E   N   E   M   Y
 P-P  B   F   F    B   M   0           P   K   P   U   H
   C  WM  TS  TS   WM  IM  EO          EM  IU  EM  HU  TE
                        M   S   0   U   E
                    W   A
                    T       T           Y
                    I   C           N
                    E   E       K
                    H               M
```

(2) Analysis continues in the same vein as above, i.e. by attacking the characteristics of the ciphertext itself. However, in this case, sufficient evidence is at hand to attempt recovery of the matrix. Note that the first column in the matrix contains the first and terminal letters of the first five letters of the alphabet (ABCDE), suggesting the *C* and *D* are the correct values for the blank cells. If this is the case, presuming the letters to be inscribed in alphabetic order, the sequence of the row indicators are out of order; E, as *EMc*=Ep must be last, and T and H of the row indicators must then lie in either the second and fourth, or fourth and second positions respectively. Assuming the latter, the word WHITE is noted; therefore, the matrix is rearranged accordingly (fig. 9-6) and B and C plain are inscribed.

	M	*S*	*O*	*U*	*E*
W	A				
H	B			M	
I	C			N	
T	D	T			Y
E	E		K		

Figure 9–6 (C). Insertion of plaintext values (U).

(3) Examination of the columns shows a good alphabetic pattern downward. However, they are not in order sequentially; the row containing the *T* follows the *A–E* row when it should appear as the next to last row. Thus the columns can be recorded as follows and missing values assumed (fig. 9–7).

	M	*O*	*U*	*S*	*E*
W	A	F	L	Q	V
H	B	G	M	R	W
I	C	H	N	S	X
T	D	I	O	T	Y
E	E	K	P	U	Z

Figure 9–7 (C). Solution of matrix (U).

(4) Using this matrix the message is now deciphered logically, proving all past assumptions.

ATTACK HAS BEEN STALLED BY ENEMY DEFENSIVE POSITIONS REQUEST ARMOR SUPPORT TO BREACH LINE.

d. The foregoing solution represents an example of attacking the message through the system which produced it. This is possible only because the system was simple; no variants were used. The keywords were common and could easily be assumed, and a recognizable route of inscribing the plaintext into the matrix was apparent from the first. While this method for solution is quicker than an analysis of word patterns, use of frequency distributions, etc., it is not always possible. In such cases, once a multiliteral cipher has been reduced to uniliteral terms, the most difficult multiliteral ciphers may be successfully solved by the monoalphabetic analytic techniques given previously.

Section III. (~~C~~) ANALYSIS OF MULTILITERAL WITH VARIANTS

9–9. (~~C~~) General

a. In the final analysis, the simple biliteral system offers no more security than a uniliteral substitution system. To circumvent this obvious weakness, variant multiliteral systems are used. The systems provide for additional row and column indicators or for variant internal values. These enable the substitution of several different cipher elements for each plaintext element. The ratio of cipher elements to plaintext elements may now be two or more to one, instead of the one to one ratio of a simple multiliteral system.

b. An example of a multiliteral system with external variants is shown in paragraph 9–3*c*. Cryptographically, the method of operation of these systems is similar to that of the simple multiliteral system, with the exception that the cryptographer now has a choice of several values for each plaintext value.

Using the first and second examples shown in paragraph 9–3*c*, Ap is represented by the cipher elements shown below:

Example 1. *KQ, KV, FQ, FV, AQ, AV*=Ap
Example 2. *TA, NA, HB, BA* =Ap

To a great extent, the actual number of variant cipher elements for a given plaintext letter occurring in a cryptogram is dependent upon the cryptographer; often the actual number used is limited by failure to make use of all values provided.

c. Identification of multiliteral with variants is basically the same as that for a simple multiliteral system. The cryptographic text will generally exhibit the same characteristics, though perhaps not as pronounced. These characteristics are:

(1) A uniliteral frequency distribution may show a limitation on number of letters used, depending upon the total number of row and column indicators used.

(2) Some positional limitations will usually be present with certain letters or numbers appearing only as row or column indicators.

(3) Message length, repeats, and distance between repeats will be divisible by the length of the cipher element.

(4) Repeats are likely to be short and fragmentary, and are often composed of several different values.

(5) The 2 ϕ I.C.'s produced by the statistical tests will be lower (6–20) than for a simple biliteral system. Generally, the shorter the message or the less repeats it contains, the lower the 2 ϕ I.C. will be.

d. Once the variant values of a multiliteral with variants system can be equated to specific letters, the course of analysis is in all respects similar to that employed in the case of the analysis of a simple multiliteral system. The cipher units are reduced to uniliteral terms; then frequencies, repeated sequences, and word patterns are studied for the substitution of plaintext values. It is in the former area, the matching of the variant values, that different techniques are employed. In one technique, the structures and frequencies of occurrence of the cipher units are studied to identify variant values having the same plaintext value. In another technique, the approach lies in the study of isomorphic repetitions of text for the determination of like variant values. Both techniques are amplified in succeeding paragraphs.

9–10. (~~C~~) Frequency Matching of Variants

a. In the case of a variant system, where the total number of variants is limited, matching of variant values becomes possible through a study of their frequency distribution. This method of matching is predicated on the assumption that in a message of moderate length, all variant cipher values for a given plaintext letter will be used. Further, it assumes that each variant will be used with approximately equal frequency. Thus, the variant row and column indicators for any given letter will appear equal in combination with one another. For example, the variant values for Ap given in the example in paragraph 9–9*b* can be expected to appear equally often. The total number of occurrences of a set of variant cipher values will approximate the frequency of the plaintext letter they represent. Thus, a definite pattern is imparted to the cipher elements which can be observed when a digraphic frequency count is made in the form of a matrix. Therein, the rows and columns correspond to the variant values which exhibit profiles equating to the frequency of combination of these letters. Where a number of rows or columns have a similar profile, a common plaintext value for their indicators may be assumed. A digraphic frequency count of the message in figure 9–8① will appear as shown in figure 9–8②.

```
ALNPI  CNDED  EGKDO  CATNT  FGAPF  DOQBM
IGECB  UOUNQ  FLBQB  TIDAT  NLRPE  HILAQ
AGETB  HBPSQ  BGICF  GFCBT  EGIHO  PRGAP
EPOQK  UFPAH  ALAMN  PKDAU  IHAGS  MAQFM
NQSUB  UEDOP  ATICO  DBHKC  AUBUF  CSHID
BGBPK  GOQBD  KHBTF  DFUAT  KQAGO  MOUED
NPEUA  HKCNC  BQECF  HBHBL  IGBMA  UFGIP
BGKDO  CIHNQ  SGAPF  QSMSL
```

Divided into digraphic elements:

```
AL  NP  IC  ND  ED  EG  KD  OC  AT  NT  FG  AP  FD
OQ  BM  IG  EC  BU  OU  NQ  FL  BQ  BT  ID  AT  NL
RP  EH  IL  AQ  AG  ET  BH  BP  SQ  BG  IC  FG  FC
BT  EG  IH  OP  RG  AP  EP  OQ  KU  FP  AH  AL  AM
NP  KD  AU  IH  AG  SM  AQ  FM  NQ  SU  BU  ED  OP
AT  IC  OD  BH  KC  AU  BU  FC  SH  ID  BG  BP  KG
OQ  BD  KH  BT  FD  FU  AT  KQ  AG  OM  OU  ED  NP
EU  AH  KC  NC  BQ  EC  FH  BH  BL  IG  BM  AU  FG
IP  BG  KD  OC  IH  NQ  SG  AP  FQ  SM  SL
```

Figure 9–8① (~~C~~). *Preparation of ciphertext for digraphic frequency distribution* (*U*).

	L	P	C	D	G	T	H	M	U	Q
A	— —	— — —			— — —	— — — —	— —	—	— — —	— —
N	—	— — —	—	—		—				— — —
I	—	—	— — —	— —	— —		— — —			
E		—	— —	— — —	— —	—	—		—	
K			— —	— — —	—		—		—	—
O		— —	— —	—				—	— —	— — —
F	—	—	— —	— —	— — — —		—	—	—	—
B	—	— —		—	— — —	— — —	— — —	— —	— — —	— —
R		—		—						
S					—		—	— —	—	—

Figure 9–8② (~~C~~). *Digraphic frequency distribution* (*U*).

b. A study of the frequency profile may begin with either the rows or columns. In either case, it is usually better to start with the one which has the most pronounced profile, seek a match for it, and then move on to the least pronounced. By this process of elimination, even the least characteristic profile can usually be matched. Note, however, that the digraphic frequency distribution represents the original enciphering matrix in an expanded form because its row and column indicators are disassociated and disarranged and do not have internal plaintext values. Thus, the process of matching the profiles will result in the construction of the matrix to its original dimension and the reassociation of the variant values. In this process, the analyst should be alert to the possibility that some system may have been used in assigning the row and column indicators. If this is the case, a short cut can hasten the final solution.

(1) Examination of the digraphic frequency distribution shows four rows which have pronounced profiles; they are rows *A*, *B*, *E*, and *F*. At first glance rows *B* and *F* appear similar, but a closer examination shows a discrepancy between the frequencies for *FT*, *FH*, *FM*, *FU*, *FQ*, and *BT*, *BH*, *BM*, *BU*, and *BQ*. Therefore, this match is rejected. Considering a match between rows *A* and *B*, a much closer correspondence in frequencies is noted, thus they may be accepted as a match (fig. 9–9).

		L	P	C	D	T	T	H	M	U	Q
A	B										

Figure 9–9 (~~C~~). *Match of rows A and B* (*U*).

(2) Because the affinity of rows *E* to *F* is not particularly negatively or positively pronounced, they may be momentarily dropped from consideration Scanning the rows again, it is quoted that *O*

exhibits an affinity for columns, *P*, *C*, *D*, and again for *M*, *U*, *Q*. Excluding rows *A*, *B* as previously matched, the only other row indicators shown in combination are the column indicators *Q*, *N*, *K*, *F*, and *S*. *S* can be rejected due to its low profile; *K* has a similar but weaker affinity for *U* and *Q*, so it, too, may be rejected. This leaves *F* and *N* for possible matches to *O*. Of the two, *N* seems the most logical as both *N* and *O* are combined frequently with *P* and *Q*, while *F* has no high-frequency combination in common with *O*. The matrix now appears as shown in figure 9-10.

	L	P	C	D	G	T	H	M	U	Q
A B										
N O										

Figure 9-10 (~~C~~). *Matching rows N and O inserted* (*U*).

c. The rows above are relatively easy to match. Rows *A* and *B* are matched because of their pronounced profile, and *N* and *O* because of similar affinities to specific column indicators. Another method of determining a match involves computing a separate value for each trial match of a row or column against the remaining rows and columns. The value of each match is derived by multiplying the two values contained in adjacent cells of each arbitrary match, and summing their products. The match having the highest value may be presumed to be correct. For example, *E* row can be compared to the following three possible matches, as shown in figure 9-11.

	L	P	C	D	G	T	H	M	U	Q	
E	0	1	2	3	2	1	1	0	1	0	
F	0	1	2	2	4	0	1	1	1	1	
	0	1	4	6	8	0	1	0	1	0	= 21
E	0	1	2	3	2	1	1	0	1	0	
K	0	0	2	3	1	0	1	0	1	0	
	0	0	4	9	2	0	1	0	1	0	= 17
E	0	1	2	3	2	1	1	0	1	0	
I	1	1	3	2	2	0	3	0	0	0	
	0	1	6	6	4	0	3	0	0	0	= 20

Figure 9-11 (*C*). *Possible matches of row E* (*U*).

(1) While all matches are fairly close, the match of rows *E* and *F* may be tried first. This test, however, as all tests, is susceptible to error. Notice how in the above a small difference in combinations could result in *E* being almost equally well matched to *K* or *I*.

(2) By a process of elimination, with only four unmatched rows left, further matching is quite simple. *R* and *S*, both with extremely low profiles, are obvious matches, leaving *I* and *K* to be matched. At this point the matrix appears as in figure 9-12.

	L	P	C	D	G	T	H	M	U	Q
A B										
E F										
I K										
N O										
R S										

Figure 9-12 (~~C~~). *Completion of row matches* (*U*).

d. The column indicators could be matched by the same process used for matching the row indicators. This, however, should not be necessary. Notice the pattern of the row variants: i.e. *AB* follows sequentially as does *E* and *F*, with a space for two letters between. This space is possibly for *C* and *D*, which appear as column variants. Thus, *C* and *D* may represent a match. This possibility is quickly confirmed when the column profiles of the two are inspected. Assuming a consistent pattern, the matrix can be recovered as seen in figure 9-13.

	C D	G H	L M	P Q	T U
A B					
E F					
I K					
N O					
R S					

Figure 9-13 (~~C~~). *Matrix with both rows and columns matched* (*U*).

e. Analysis of the cryptogram beyond this point follows the same techniques as those used in the case of simple multiliteral systems. The digraphic variants are reduced to uniliteral terms by inserting an arbitrary plain sequence in the matrix. A distribution is made, and a study of the frequencies of letters and repetitions of patterns in the pseudo-plaintext begins.

9–11. (~~C~~) Isomorphic Characteristics in Determination of Equivalents

a. A characteristic of encipherment by multiliteral systems with variants is the disruption of isomorphic patterns in the plaintext. This disruption may be seen in the encipherment of the word RECOMMENDED by the two systems illustrated in paragraph 9–2 (fig. 9–1) and example 3 in paragraph 9–3*c* (fig. 1–3).

Simple multiliteral encipherment:

R	E	C	O	M	M	E	N	D	E	D
SI	*CE*	*CD*	*EG*	*EI*	*EJ*	*CE*	*ED*	*CG*	*CE*	*CG*
	A	B	C	D	D	A	E	F	A	F

Multiliteral with variant encipherment:

R	E	C	O	M	M	E	N	D	E	D
KK	*JA*	*DB*	*CA*	*IC*	*DL*	*MJ*	*AG*	*IF*	*JA*	*DJ*

b. For all practical purposes, the isomorphic pattern of the plaintext word clearly reproduced in the first encipherment is completely extinguished by the second method of encipherment. If the text of a given variant system is scarce, and if all possible variant values are fully used and wholly independent of one another, the solution can become exceedingly difficult. However, in practice this situation is rarely encountered, as practical military communications are such that a sufficient volume of text is usually available to provide a basis for establishing equivalent values. To illustrate the possibilities of determining equivalent values by a study of isomorphic repeats, consider the example below, each set being a series of different numeric ciphertext values of one underlying plaintext word or sequence of letters. Note that although these repeats are useful for analysis they first must be isolated from the text as representing a probable word or phrase. Usually this occurs in the cases where stereotyped beginnings or endings are used. In this case, the examples are arbitrarily selected for the purpose of illustration.

Set A

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
12	*37*	*02*	*79*	*68*	*13*	*03*	*37*	*77*
82	*69*	*02*	*79*	*13*	*68*	*23*	*37*	*35*
82	*69*	*51*	*16*	*13*	*13*	*78*	*05*	*35*
91	*05*	*02*	*01*	*68*	*42*	*78*	*37*	*77*

Set B

(1)	(2)	(3)	(4)	(5)	(6)	(7)
71	*12*	*02*	*51*	*23*	*05*	*77*
11	*82*	*51*	*02*	*03*	*05*	*35*
11	*91*	*02*	*02*	*23*	*37*	*35*
97	*12*	*51*	*02*	*78*	*69*	*77*

c. Examination of individual cipher sequences in each set shows no isomorphic pattern other than a few scattered repeats. However, inspection of the columns formed by the superpositioning of the cipher sequence reveals that in columns (3) and (4) of set B, the dinomes *51* and *02* are used exclusively and interchangeably. In column (3) of set A, the dinomes *51* and *02* are also used interchangeably, but in column (4) different dinomes appear. A close study of each column leads to the acceptance of the following groupings as possible equal cipher equivalents:

12	*37*	*02*	*79*	*68*	*03*	*77*	*71*
82	*69*	*51*	*16*	*13*	*23*	*35*	*11*
91	*05*		*01*	*42*	*78*		*97*

d. The equivalent values derived above may be assigned arbitrary values to reduce them to uniliteral terms. Thereafter, these equivalencies may be used to find additional sets of equivalent values in the ciphertext. The analyst may recover plaintext letters, by applying the method of the analysis of probable words and word patterns, and then proceed to analyze the uniliteral terms in that light. For example, the sets of cipher equivalents could be reduced to the following word pattern:

Set A

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
12	*37*	*02*	*79*	*68*	*13*	*03*	*37*	*77*
82	*69*	*02*	*79*	*13*	*68*	*23*	*37*	*35*
82	*69*	*51*	*16*	*13*	*13*	*78*	*05*	*35*
91	*05*	*02*	*01*	*68*	*42*	*78*	*37*	*77*
	A	B	C	D	D	E	A	

Set B

(1)	(2)	(3)	(4)	(5)	(6)	(7)
71	*12*	*02*	*51*	*23*	*05*	*77*
11	*82*	*51*	*02*	*03*	*05*	*35*
11	*91*	*02*	*02*	*23*	*37*	*35*
97	*12*	*51*	*02*	*78*	*69*	*77*
		A	A			

e. Besides the isomorphic pattern of the words themselves, the indication that certain letters are the same is of value in determining the exact words these patterns represent. The fact that the dinomes of column (3) in set A and those of columns (3) and

(4) in set B are similar was previously mentioned. An examination of the grouping of possible cipher equivalents also shows that the last three letters of both words have the same plaintext value. Using the word patterns and the expected similarity of letters, a word pattern list can be scanned for words which conform to these conditions, resulting in the discovery of the words:

```
- A B C D D E A -     - - A A - - -
A R T I L L E R Y     B A T T E R Y
```

f. The determination of equivalencies may appear to be an easy matter, as is their extension to probable words. However, it may be very difficult, as the cryptanalyst can never be certain that a set of cipher sequences showing what appears to be the use of variant values to encipher the same plaintext word or phrase is correct. There is always the possibility that they are parts of different plaintext sequences. For example, the cipher sequence on the surface represents the same word with two variants appearing in the first position.

```
17  82  31  82  14  63
27  82  40  82  13  63
```

However, it could as easily represent the different words MANAGE and DAMAGE or other similarly constructed words.

9–12. ~~(C)~~ Analysis of Isologs

a. Occasionally in military communications, a situation occurs where one plaintext message is enciphered in either two different systems or variations of the same system. The cryptogram thus produced, differing in ciphertext but having the same underlying plaintext, is termed an isolog. Isologs, no matter how produced, are among the most important means available to the cryptanalyst in solving a cryptogram. In some instances, isologs are the only practical means of entering systems which offer no other clues. Such an entry proves useful in multiliteral systems employing variants where conditions preclude the application of techniques previously discussed.

b. Normally an isolog is recognized by equality, or near equality, of length of two or more messages. An isolog may be suspected where this similarity of message length is noted. However, before accepting this condition as fact, a confirmation in similarities is sought in those elements pertaining to handling and transmission of the message, such as, serial numbers, originators, etc. Also, if the isolog is generated by the use of variations of the same system, a few scattered repeats may be noted throughout the message. It is an isolog of this nature that provides a means of solving multiliterals with variants.

c. Regarding the analysis of isologs and isologous segments of multiliterals with variants, the technique employed is only an extension of the methods used in the determination of equivalent values by a study of isomorphic characteristics. The only difference is that in this case the whole message as an isolog, or large portions of it as isologous segments, are studied. Moreover, the study of word patterns and the derivation of probable words may involve whole phrases rather than individual words.

d. Given two messages suspected of being isologs, a digraphic distribution is made for each in figure 9–14① and 9–14② and examined for any characteristics which might aid in the analysis of the cryptogram. The messages and their respective distributions follow.

```
Message A

A    82265   63103   74839   69842
     32529   70115   80277   89106
B    94000   13828   54082   40065
     63629   33918   43158   81048
C    26458   45039   81713   52538
     73309   20749   61752   16476
D    38728   91147   99926   41468
     13365   33881   89697   93816
E    51750   57074   11804   43255
     28120   27730   31199   79962
F    27865   60653   90870   40867
     46594   19855   10822   22987
G    46723   36245
```

	1	2	3	4	5	6	7	8	9	Ø
1	2	1	1	1	2	1	-	1	1	2
2	1	1	-	1	1	2	2	2	1	-
3	2	2	-	-	1	1	-	5	2	2
4	1	1	1	1	2	2	1	1	1	-
5	1	1	2	1	2	2	-	-	1	1
6	1	3	1	2	1	-	1	1	1	-
7	1	2	1	2	2	1	1	1	1	1
8	2	2	1	1	-	1	2	1	2	2
9	1	2	2	1	-	1	2	2	2	1
Ø	2	1	1	1	1	2	1	2	-	2

Figure 9–14① (~~C~~). Digraphic frequency distribution, message A (U).

Message B

	5	10	15	20
A'	30150	87497	14511	97360
	49676	50106	45647	99181
B'	69672	53889	41563·	25203
	90628	77536	20351	10570
C'	89277	75011	35199	90138
	99974	50232	04115	89216
D'	38463	17547	14648	00646
	85864	53898	26121	83878
E'	94889	33728	11272	20504
	06484	32103	98715	42662
F'	80760	89880	44105	52900
	59728	22855	87300	70893
G'	57682	46253		

	1	2	3	4	5	6	7	8	9	Ø
1	4	1	-	2	1	1	-	1	2	1
2	1	1	-	1	1	2	2	2	1	1
3	1	2	-	-	2	1	1	5	-	2
4	1	-	1	1	3	2	1	1	1	-
5	1	1	1	1	2	1	-	1	2	1
6	-	3	-	2	1	-	2	1	1	1
7	1	1	1	1	2	1	1	1	1	1
8	1	1	-	-	1	1	2	1	2	3
9	1	1	2	1	-	-	2	3	2	1
Ø	2	1	2	2	2	3	1	3	-	1

*Figure 9–14*② (~~*C*~~). *Digraphic frequency distribution, message B* (*U*).

e. As both dinomic distributions reveal a random scattering of frequencies with no single pronounced pattern in either row or column, multiliteral systems with variants may be assumed for each. Further, although the distributions are flat, they are very similar in respect to the location of both blanks and points of high frequency. It may, therefore, be tentatively assumed that the two messages are variations of one system. An examination of each message reveals no single outstanding characteristic which indicates the underlying plaintext or system of encryption. Therefore, the messages may be compared to each other to determine if any such pattern exists, and to further their identification as isologs. This is done by inscribing one above the other, assigning row and column coordinates for reference purposes. Because the system involved is multiliteral, the text is arranged in dinomic elements, as shown in figure 9–15.

					5					10					15					20
A	82	26	56	31	03	74	83	06	08	42	32	52	97	01	15	80	27	78	91	06
A'	30	15	08	74	97	14	51	19	73	60	49	67	65	01	16	45	64	79	91	81
B	94	00	01	38	28	54	08	24	00	00	08	62	93	39	18	43	15	88	10	48
B'	69	67	25	38	89	41	56	32	52	03	90	62	87	75	36	20	35	11	05	70
C	26	45	84	50	39	81	71	35	25	33	73	30	92	07	49	61	75	21	64	76
C'	89	27	77	50	11	35	19	99	01	33	99	97	45	02	32	04	11	58	92	16
D	38	72	89	11	47	99	92	64	14	68	13	36	53	38	81	89	69	79	38	16
D'	38	46	31	75	47	14	64	80	06	46	85	86	45	38	98	26	12	18	38	78
E	51	75	05	70	74	11	80	44	32	55	28	12	02	77	30	31	19	97	99	62
E'	94	88	93	37	28	11	27	22	05	04	06	48	43	21	03	98	71	54	26	62
F	27	86	56	06	53	90	87	04	08	67	46	59	41	98	55	10	82	22	29	87
F'	80	76	08	98	80	44	10	55	29	00	59	72	82	28	55	87	30	07	08	93
G	46	72	93	62	45															
G'	57	68	24	62	53															

Figure 9–15 (~~*C*~~). *Superimposition of messages A and B* (*U*).

f. When the paired digraphs formed by the superimposed messages are scanned closely, several digraphs are repeated at the same position in each message. Some of the repeats are:

	(14)	(19)
A	*01*	*91*
A′	*01*	*91*

	(4)	(12)
B	*38*	*62*
B′	*38*	*62*

	(4)	(10)
C	*50*	*38*
C′	*50*	*38*

	(1)	(5)	(14)	(19)
D	*38*	*47*	*38*	*38*
D′	*38*	*47*	*38*	*38*

	(6)	(20)
E	*11*	*62*
E′	*11*	*62*

	(15)
F	*55*
F′	*55*

	(4)
G	*62*
G′	*62*

The repeated occurrence of the same dinomes in both messages at the same relative position, always paired and also coupled with the similarities in the frequency distribution, is strongly indicative that the messages are produced from the same enciphering system. The fact that certain values are paired while the intervening dinomes between appear random may be explained by the assumption that the system provides a number of variants for high-frequency letters and few or none for low-frequency letters. Thus, the plaintext value for the dinomes paired in both messages could be low-frequency letters. Further, if this is the case, the dinomes appearing in both messages between a set of pairs must then represent the use of variant values to encipher the same plaintext sequence.

g. Using the foregoing assumption as a base, it is possible to form a chain of possible equivalent values by equating dinomes to each other. For example, the first six sets of dinomes of each message may be written vertically as follows:

Message A	A′
82	*30*
26	*15*
56	*08*
31	*74*
03	*97*
74	*14*

As it has been assumed that these dinomes are equal values for the same plaintext letters, it then follows that if any one of these are found paired with another dinome then it too must represent the same value. For example, in position A A′ (4) and (6) the paired dinomes *31 74* and *74 14* are found. If *74* is related as equal in plaintext value to *31*, *14* must also be equal in value to *31* and *74*. Thus a sequence of *31 74 14* may be desired. By continuing the same chaining process on a reciprocal basis (possible because both messages are enciphered by the same matrix), the following chain of equal values, figure 9–16, is derived, arranged in order of length.

```
06 14 15 26 28 31 35 73 74 81 89 98 99
02 07 20 22 43 44 63 90
12 37 48 51 69 70 83 94
03 30 41 54 65 82 97
05 10 24 32 49 87 93
16 18 36 76 78 79 86
27 45 53 64 80 92
11 39 75 88
21 58 77 84
46 59 68 72
00 52 67
04 55 61
08 29 56
19 71 96
01 25
13 85
42 60
38
47
50
62
91
```

Figure 9–16 (C). Chain of equal values (C).

h. The equivalent values produced by the chaining process can now be assigned arbitrary letters to reduce them to uniliteral terms, and each message can now be studied on these terms. Not only will word patterns come to light when the uniliteral terms are substituted for the dinomes, but also since the system apparently made provision for high-frequency letters, they in turn can be identified by the number of their variant values. For example, the first chain above probably equates to E of the plaintext. Using the assumed E value and the list of equivalent values, a sequence of word patterns and their partial plaintext values is easily derived. For example:

A	*82*	*26*	*56*	*31*	*03*	*74*	*83*	*96*	*98*	*42*	*32*	*52*	*97*	*01*
A′	*30*	*15*	*08*	*74*	*97*	*14*	*51*	*19*	*73*	*60*	*49*	*67*	*65*	*01*
P	–	E	–	E	–	E	–	–	E	–	–	–	–	–
	A	B	C	B	A	B	D	E	B	F	G	H	A	

Then, comparing this to a list of word patterns, all the other plaintext values could be determined. For example, the first eight letters of the pattern probably mark a whole word. A similar pattern which contains an E in the appropriate positions is the word REFERENCE which can easily be expanded to REFERENCE YOUR for the whole isologous sequence. With a few known values for the arbitrary uniliteral term, the solution of the remainder of the message poses no particular difficulty, and the enciphering matrix could be recovered as shown in figure 9–17. A word of caution though, this method is not always 100 percent certain. In some cases mistakes made in transmitting or copying the message and also the lack of values may prevent the chaining process from being carried through.

	1	2	3	4	5	6	7	8	9	Ø
1	D	N	H	E	E	A	–	A	C	O
2	I	T	–	O	M	E	S	E	F	T
3	E	O	–	–	E	A	N	B	D	R
4	R	Y	T	T	S	L	V	N	O	–
5	N	U	S	R	P	F	–	I	L	X
6	P	W	T	S	R	–	U	L	N	Y
7	C	L	E	E	D	A	I	A	A	N
8	E	R	N	I	H	A	O	D	E	S
9	G	S	O	N	–	C	R	E	E	T
Ø	M	T	R	P	O	E	T	F	–	U

Figure 9–17 (C). Reconstructed matrix (U).

By manipulating the rows and columns, a diagonal arrangement of the plaintext values can be obtained as shown in figure 9–18.

	6	8	9	1	5	4	3	7	2	Ø
7	A	A	A	C	D	E	E	I	L	N
1	A	A	C	D	E	E	H	K	N	O
3	A	B	D	E	E	H	J	N	O	R
8	A	D	E	E	H	I	N	O	R	S
9	C	E	E	G	I	N	O	R	S	T
2	E	E	F	I	M	O	Q	S	T	T
Ø	E	F	I	M	O	P	R	T	T	U
5	F	I	L	N	P	R	S	T	U	X
6	I	L	N	P	R	S	T	U	W	Y
4	L	N	O	R	S	T	T	V	Y	Z

Figure 9–18 (C). Recovered matrix (U).

Section IV. (~~C~~) MULTINOMIC SYSTEMS

9–13. (~~C~~) General

a. Analytically, any distinction between multiliteral and multinomic systems, because of the use of alphabetic or numeric values as row and column indicators, is generally inappropriate. Multiliteral systems of the type previously covered employ the same principles of cryptography, independent of the nature of their row and column indicators. Thus, being cryptographically similar, they are susceptible to the same analytical techniques of their identification, analysis, and final solution.

b. There are several systems, though multiliteral with variants, which are sufficiently different to warrant additional study. These systems use numeric values exclusively for the cipher elements, and the manner of deriving the cipher element is somewhat different from that normally associated with multiliteral systems. The systems can be classified as multinomics, and the techniques of analysis employed are slightly different.

c. Cryptographic systems which may be grouped within this class are the columnar numerical, the monome-dinome, and the monome-dinome-trinome systems.

9–14. (~~C~~) Columnar Numeric System

a. One of the most simple of the dinomic systems from both a cryptographic and a cryptanalytic point of view is a columnar numeric system. This is a multiliteral system because the cipher element to plain element ratio is commonly 2 to 1, but it is unlike the previous systems because the cipher element is not derived from row and column coordinates. Each plaintext value is assigned several cipher values arranged in a columnar matrix as depicted in figure 9–19.

A	B	C	D	E	F	G	H	IJ	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	01	02	03	04	05	06	07
35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	26	27	28	29	30	31	32	33	34
69	70	71	72	73	74	75	51	52	35	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68
87	88	89	90	91	92	93	94	95	96	97	98	99	00	76	77	78	79	80	81	82	83	84	85	86

Key: *TRHP*

Figure 9–19 (~~C~~). Columnar numeric system (U).

b. The number of rows of dinomic cipher values may vary as may the system of inscription. Note that in the above example, each row of 26 sequential letters begins at a letter corresponding to a letter of the keyword and is inscribed in its normal progressive order. The overall security of the system is easily improved by randomly assigning the dinomes in each row. However, this entails the loss of its primary advantages which are a limited number of dinomic strips, each sequential and juxtaposed on a keyword that is easy to remember and duplicate.

c. A message is enciphered by substituting for each plaintext value one of its dinomic cipher equivalents. For example, a message can be enciphered with this system as shown in figure 9–20. Decipherment is just the reversal of encipherment.

```
 A  I  R    R  E  C  O  N  N  A  I  S  S  A  N  C  E    I  N  D  I  C  A  T
08 16 26   24 12 10 48 47 56 35 43 27 61 87 47 37 12   52 56 38 52 71 69 28

 E  S    E  N  E  M  Y    A  R  T  I  L  L  E  R  Y    U  N  I  T  S
73 27   91 99 39 46 85   69 60 62 52 45 54 39 60 67   29 56 16 01 25

 A  R  E    B  E  I  N  G    D  I  S  P  L  A  C  E  D    T  O    F  A  R
35 26 39   70 73 95 56 75   72 43 61 58 45 87 71 39 72   28 57   92 35 26

 B  A  N  K    O  F    S  O  U  T  H    R  I  V  E  R    S  T  O  P
36 08 99 44   48 74   61 21 29 80 15   60 16 64 12 60   27 62 48 22

 N  O    O  T  H  E  R    I  N  D  I  C  A  T  O  R  S    O  F
47 57   21 28 42 73 60   95 47 38 52 10 35 62 21 24 79   57 40

 E  N  E  M  Y    W  I  T  H  D  R  A  W  A  L    O  B  S  E  R  V  E  D  X
39 56 12 98 33   04 43 62 51 11 60 87 31 08 45   21 36 27 39 60 03 73 90 66

08162  62412  10484  75635  43276  18747  37125  25638

52716  92873  27919  93946  85696  06252  45543  96067

29561  60125  35263  97073  95567  57243  61584  58771

39722  85792  35263  60899  44487  46121  29801  56016

64126  02762  48224  75721  28427  36095  47385  21035

62212  47957  40395  61298  33044  36251  11608  73108

45213  62739  60037  39066
```

Figure 9–20 (C). Encipherment using the columnar numeric system (U).

d. Analysis generally involves the same techniques as the analysis of uniliteral monoalphabetic ciphers, with provision made for the fact that a number of dinomic sequences are involved. Assuming that the dinomes of the system have been inscribed sequentially, a four-part dinomic frequency distribution can be made with each part corresponding to 25 or 26 progression numbers. For example, such a frequency distribution of the message above would appear as in figure 9–21.

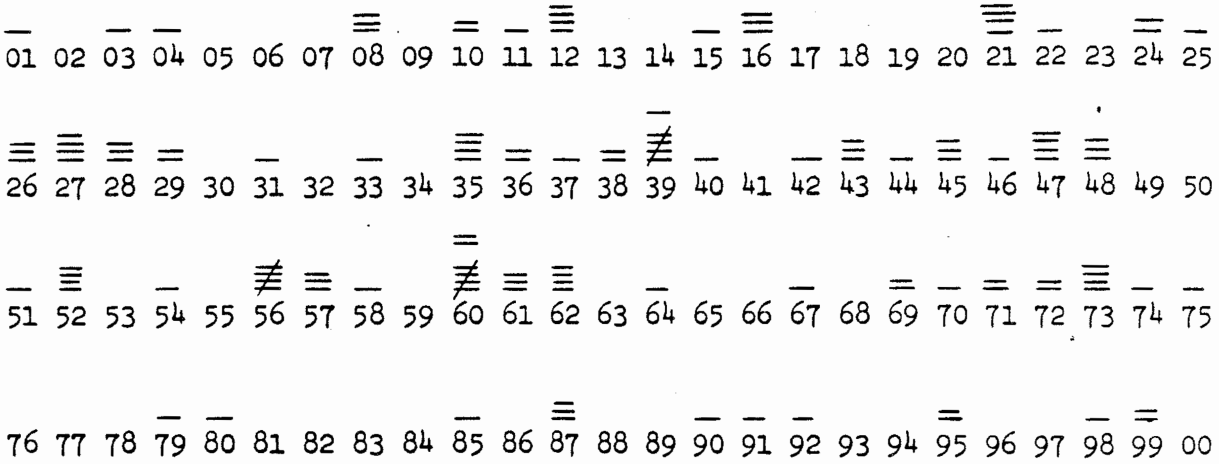


Figure 9–21 (*U*). *Four-part dinomic frequency distribution* (*U*).

e. Each sequence above represents a simple monoalphabetic frequency distribution. This fact, once realized, should immediately lead to the next step of fitting the distribution to the normal. Note that the second and third sequences have the most pronounced peaks and troughs, and therefore would be the sequences to begin with. Once they have been fitted to the norm, the remaining sequences fall into place as each sequence represents a part of a whole. Without referring back to the original cryptographic system, the analyst should be able to equate three of these sequences to the norm by visual inspection alone. For example, starting with the third sequence and mentally matching an alphabetic sequence to the peaks and troughs, it is clear that *51c*=Hp. The same type examination of the second sequence shows that *35c*=Ap. These two may be inscribed thusly:

A	B	C	D	E	F	G	H	IJ	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
35	*36*	*37*	*38*	*39*	*40*	*41*	*42*	*43*	*44*	*45*	*46*	*47*	*48*	*49*	*50*	*26*	*27*	*28*	*29*	*30*	*31*	*32*	*33*	*34*
69	*70*	*71*	*72*	*73*	*74*	*75*	*51*	*52*	*53*	*54*	*55*	*56*	*57*	*58*	*59*	*60*	*61*	*62*	*63*	*64*	*65*	*66*	*67*	*68*

f. The placement of the first and fourth sequences would be a little more difficult under ordinary circumstances. However, this is not necessary. The sequence recovered represents 50 percent of the total system; therefore, one-half the text could be recovered, thus permitting the assumption of plaintext values for the cipher dinomes of the two remaining strips. Moreover, since each sequence is progressive, the valid assumption of only one cipher value inevitably leads to the placement of all others.

9–15. (~~C~~) Monome-Dinome Systems

a. This type system, one of the more important multiliteral systems, differs from others in that it replaces constant-length plaintext units with cipher elements of variable lengths. The ratios of cipher element to plain element may be 1 to 1 or 2 to 1. The variation in the ratio is brought about by omitting one row coordinate. Thus, some plaintext letters are represented by a two-digit cipher element, composed of both row and column indicators, while others are indicated by a column indicator only. Figure 9–22 illustrates the structure of the system, and its application in enciphering a message.

	1	2	3	4	5	6	7	8	9	Ø
4	A	1	B	2	C	3	D	4	E	5
6	F	6	G	7	H	8	I	9	J	Ø
-	K	.	L	-	M	-	N	-	O	P
8	Q	R	S	T	U	V	W	X	Y	Z

M	O	V	E	R	E	S	E	R	V	E	B	A	T	T	A	L	I	O	N
5	9	86	49	82	49	83	49	82	86	49	43	41	84	84	41	3	67	9	7

T	O	B	L	O	C	K	I	N	G	P	O	S	I	T	I	O	N
84	9	43	3	9	45	1	67	7	63	Ø	9	83	67	84	67	9	7

Figure 9–22 (~~C~~). *Monome-dinome system* (*U*).

Note that in the matrix, blanks appear where the blank row intersects columns having as coordinates a value used as row indicators. Thus a blank appears in columns 4, 6, and 8 above (as 4, 6, and 8 were used as row indicators) to preclude confusion in decipherment. For example, if a value (A) did appear at the intersection of a blank row and column 4, its value would be 4. Since *44c* also represents 2p, the deciphering clerk would have to decide which was the correct value, two A's or the digit 2.

b. Examination of the ciphertext produced above reveals two important facts. First, there is a constant relationship between cipher and plaintext values with no variants. Thus, Ep is always equal to *49c*. Second, the use of monomics does nothing more than confuse identification of this constant relationship. For example, the text above divided into 5-figure groups would appear thusly:

59864 98249 83498 28649 43418 48441 36797
84943 39451 67763 Ø9836 78467 97

On the surface, the text shows no evidence of which dinome or monome represents what plaintext value, as the individual identities of the dinomes and monomes are lost in the formation of the ciphertext. Moreover, because there is a constant relationship between a given dinome or monome and a plaintext value, it follows that solution of this system lies first in isolating the monomes from the dinomes and then in identifying each. Thereafter, a solution is primarily a matter of reducing the text to uniliteral terms and solving it accordingly.

c. Identification of a monome-dinome system is based on the following characteristics:

(1) The length of the cryptogram may be either odd or even.

(2) Repeats are consistent in length and structure within a message and may or may not be divisible by a constant factor.

(3) Interval between repeats may or may not be divisible by a constant factor.

(4) A monomic frequency distribution may reveal two or three digits with a high frequency.

d. Considering the message and its monomic frequency distribution in figure 9–23, the above characteristics may be noted.

	5	10	15	20	25
A	74231	59202	35723	27201	58955
B	76762	35820	73555	82373	17676
C	55572	47757	73775	87915	87272
D	23732	35778	55592	38777	85595
E	57757	78789	77878	29788	23229
F	55997	75123	85823	81581	97758
G	20735	55823	73775	81991	22567
H	85557	51199	17655	77577	89582
I	35724	97450			

Monome Frequency Distribution

1	(12)
2	(27)
3	(19)
4	(4)
5	(45)
6	(6)
7	(51)
8	(24)
9	(17)
Ø	(5)

Figure 9–23 (C). Ciphertext and monomic frequency distribution (U).

(1) The disparity between the frequencies of each digit in the monomic distribution is obvious and indicates that 2, 5, and 7 probably represent row coordinates. If this is correct, a matrix similar to the following can be drawn up containing a blank row with blank cells beneath the column indicators *2*, *5*, and *7*

	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*Ø*
–		–			–		–			
2										
5										
7										

(2) Using the cipher elements that can be derived from this matrix, the cryptogram can now be rendered to its correct elemental construction as depicted below:

74-23-1-59-20-23-57-23-27-20-1-58-9-55-76-76
23-58-20-73-55-58-23-73-1-76-76-55-57-24-77-57-73-77
58-79-1-58-72-72-23-73-23-57-78-55-59-23-8-77-78-55
9-55-77-57-78-78-9-77-8-78-29-78-8-23-22-9-55-9-9-77
51-23-8-58-23-8-1-58-1-9-77-58-20-73-55-58-23-73-77
58-1-9-9-1-22-56-78-55-57-51-1-9-9-1-76-55-77-57
78-9-58-23-57-24-9-74-50

(3) From this point on, if monomes and dinomes have been identified correctly, the solution is essentially the same as that used for uniliteral monoalphabetic ciphers, as a direct relationship exists between one plaintext element and one ciphertext element, regardless of the latter's configuration. As a matrix is involved, the analyst has an additional advantage. As the plain values are recovered, they may be inserted into the matrix. Assuming that a systematic method of inscription is followed with a normal alphabetic sequence, the route often can be assumed, permitting the placement of all values. These must later be proved by actual decipherment of the cryptogram.

e. A facet of both above matrices is the marked difference in the number of rows and columns; in both, the ratio is 4 to 10. This made possible the distinction between row and column indicators through the use of a monomic frequency distribution. Were the matrix to have an equal number of rows and columns, for example 6 each, it would produce a generally flatter frequency distribution. The occurrence of digits with any great frequency would be due to the encipherment of high-frequency letters rather than the repeated use of a few row coordinates. Thus, the identification of a monome-dinome system is more difficult. In such cases, identification sometimes can be based upon the internal characteristic of the text. For example, consider figure 9–24 containing a message produced by this type cipher and its monomic frequency distribution.

	5	10	15	20	25
A	*57357*	*29418*	*28464*	*71715*	*82946*
B	*16482*	*58257*	*57482*	*84549*	*16436*
C	*47364*	*84946*	*36471*	*71616*	*49159*
D	*55827*	*45646*	*26384*		

Monome Frequency Distribution

1	(9)
2	(8)
3	(5)
4	(18)
5	(11)
6	(13)
7	(10)
8	(10)
9	(6)
0	

Figure 9–24 (~~C~~). *Cipher message and monomic frequency distribution* (*U*).

(1) Upon initial examination, the cryptogram appears to be digraphic. The primary clues that it is not are the absence of the zero in the distribution, and the fact that the repeated groups, although even digits in length, lie at uneven distances from the beginning and end of the message and from each other. With nine digits as row and column coordinates, there could only be a matrix of 20 cells with 4 rows x 5 columns or reverse, unless one blank row indicator is used. A blank row indicator would provide for a 5 x 5 matrix of 25 cells which is suitable for an alphabet when assuming the I and J, or U and V are combined. It is possible to repeat a digit as both row and column indicators, but this would be reflected in the frequency distribution by that digit occurring more often. Also the Ø probably would have been used first before one of the other digits were repeated.

(2) Having tentatively identified the system, the analyst may now attempt the recovery of the matrix coordinates. The approach in this case, assuming no like-digits were used as row and column indicators, is to locate all doublets. Repeated digits, assuming the limitation above, are probably the repeated occurrence of a dinome derived from the intersection of a blank row and a numbered column. Searching the text, the doublet *55* is noted. Thus, on the basis of the reasoning above, 5 is accepted as a possible column indicator (fig. 9–25).

		5		

Figure 9–25 (U). Initial placement on column indicator (U).

(3) A *9* is noted as immediately preceding the doublet *55*, which is also preceded by a *5*. If *5* is indeed a column indicator the correct spacing of the cipher sequence must be *5 95 5*. Thus 9 can be tentatively accepted as a row indicator. If so, then *9* will appear only in conjunction with other digits which are column indicators. Searching the text, the dinomes *91* and *94* are found; thus *1* and *4* can also be accepted as column indicators. The process results in the expansion of the matrix as shown in figure 9–26.

	1			4	5	
9						

Figure 9–26 (U). Expansion of matrix (U).

(4) Searching the text again for further patterns, the first group *57357* is noted. As *5* is accepted as a column coordinate, the *7* which follows the *5* above must be a row indicator. Thus *73* is a dinome row and a dinome column indicator respectively. Again, a search is made for combinations of *7*, and *73*, *72*, *71*, *75*, and *74* are found. The assumed can now be inscribed (fig. 9–27).

	1	2	3	4	5
-					
7					
9					

Figure 9–27 (U). Second expansion of row and column indicators (U).

(5) By a continued inspection of the text, working backwards, i.e. finding a digit which precedes an assumed column indicator, all row indicators can be isolated quickly producing a matrix similar to that shown in figure 9–28.

	1	2	3	4	5
-					
6					
7					
8					
9					

Figure 9–28 (U). Final reconstructed form (U).

With this matrix, the cryptogram can be fractured to its individual cipher elements, reduced to uniliteral terms, and solved by a method similar to that of the preceding example.

9–16. (~~C~~) Monome-Dinome-Trinome System

a. A monome-dinome-trinome system is essentially the same as a monome-dinome system with, as the name implies, a trinomic element. This element is included as shown in the matrix and cryptogram in figure 9–29.

	1	2	3	4	5	6	7	8	9	0
-	A	F	G	L	-	Q	R	W	-	-
5	B	E	H	K	M	P	S	V	X	.
90	C	D	I	J	N	O	T	U	Y	Z

```
E   N   E  M   Y     A   T   T A   C  K   I   N G   Z
52 905 52 55 909     1 907 907 1 901 54 903 905 3 900

52905   52559   09190   79071   90154   90390   53900
```

Figure 9–29 (~~C~~). Example of monome-dinome-trinome system (U).

b. The solution of this system is basically the same as that for the first preceding example of a monome-dinome system. Identification, again, is usually made through the use of a monomic frequency distribution which will reflect a high frequency of use for those digits used as row indicators. Normally, an examination of the text will reveal two of these high-frequency digits combined in most cases in the cryptographic text. Once the row and column indicators have been isolated, solution again is merely a matter of fractioning the text into its component cipher elements, reduction to uniliteral terms, and establishing the plain-to-cipher values. As an aid, the matrix can be reconstructed simultaneously.

9–17. (~~C~~) Trinomic System

a. A variant form of the basic multiliteral system is the trinomic system in which a constant length cipher element of three digits replaces a constant length plaintext element, usually of one letter. Structurally, the systems are similar in that both employ a matrix with row and column coordinates and an alphabet inscribed therein. The primary difference is that in the trinomic system one set of indicators is dinomic and the other is monomic. The dinomic element may appear either as row or column indicators usually limited to one position, but it is possible to mix them between the two. Further, it is possible to use alphabetic values in this system rather than numeric values. An example of the normal configuration of the system using numeric values is shown in figure 9–30.

	1	2	3	4	5
16	A	B	C	D	E
72	K	I	H	G	F
38	L	M	N	O	P
94	U	T	S	R	Q
50	V	W	X	Y	Z

```
 A   D   V   A   N   C   E    T   O    P   H   A   S   E    L   I   N   E
161 164 501 161 383 163 165  942 384  385 723 161 943 165  381 722 383 165

16116   45011   61383   16316   59423   84385   723161   94316   53817   22383    165
```

Figure 9–30 (~~C~~). Trinomic system (U).

b. Cryptographically, the system offers little. As can be seen in the encipherment above, there is still the one-to-one relationship between the plain and the cipher element. In effect, the system only increases a message length by threefold with little increase in security.

c. Recognition of a trinomic system is possible through its basic characteristics. They are:

(1) Message length, discounting nulls, is divisible by three.

(2) Repeats are divisible by three.

(3) Intervals between repeats are divisible by three.

(4) Positional limitation of the dinome and monome indicators make up the trinome.

(5) Little frequency deviation is shown on a monomic frequency distribution.

d. An analysis of the characteristic above usually suffices to identify a trinomic system and to separate it into its component cipher elements. For example, observe the message below.

```
56712  79059  05125  78990  57853
43565  34756  11257  85567  90178
15673  47785  90578  13431  29901
78734  75671  27905  90512  53439
01567  56734  77859  00000
```

(1) Each repeat, each interval between repeats, each interval between repeats and end of message, and the overall message length except for three zeros used as nulls, is evenly divisible by three. Further, a close study of the group reveals the trinomic grouping. For example, the first two lines of text can be divided as follows:

```
567  127  905  905  125  789  905  785  343
565  347  561  125  785  567  901  781  567
347  785  905  781  343  129  901  787  347
567  127  905  905  125  343  901  567  567
347  785  900  000
```

(2) Having reduced the ciphertext to its elemental parts, the matrix now can be recovered. This is a simple task due to the positional limitation inherent to the system. Note each of the trinomes listed above. A close study reveals that each is composed of two units: a dinome and a monome. Further study also shows that the dinome is limited to *12*, *34*, *56*, *78*, and *90*, and the monome to *1*, *3*, *5*, *7*, and *9* respectively. Using these values a matrix can be reconstructed as in figure 9–31.

	1	*3*	*5*	*7*	*9*
12					
34					
56					
78					
90					

Figure 9–31 (*U*). *Reconstructed matrix* (*U*).

(3) With the ciphertext in its elemental parts, where the one-to-one ratio exists and with the matrix defined, solution of the message is rapid. It would be studied and analyzed exactly as a uniliteral monoalphabetic substitution cipher using all techniques associated with the solution of that type system.

PART FOUR (~~C~~)

POLYGRAPHIC SUBSTITUTION SYSTEMS

CHAPTER 10 (~~C~~)

CHARACTERISTICS OF POLYGRAPHIC SUBSTITUTION SYSTEMS

Section I. (~~C~~) CHARACTERISTICS OF POLYGRAPHIC ENCIPHERMENT

10–1. (~~C~~) General

a. The substitution systems dealt with thus far, with the exception of the syllabary square and code charts, have involved plaintext units of single elements. This part deals with substitution systems involving plaintext units composed of more than one letter, such systems being termed polygraphic. Perhaps the reader has noticed the distinction between the use of the suffix "literal" and "graphic." Terms involving literal refer to the composition of the ciphertext, as in multiliteral systems; terms involving graphic refer to the composition of the plaintext elements treated. Within this broad classification there are distinct systems classified by the number of plaintext elements involved in the encipherment process, the most common of these being the digraphic system, which involves a double element cipher unit.

b. A major characteristic of the digraphic system is that both the cipher and the plaintext elements are composed of two units, and the two units of the latter jointly determine the composition of the cipher element. In these systems, since the plaintext units jointly determine the composition of cipher elements, it cannot be said that any single plaintext letter has any one particular cipher equivalent. For example, in certain digraphic systems ABp can be enciphered as *XPc* while ACp becomes *NRc*. Thus the change in identity of but one of the plaintext letters acts to change the identity of both letters of the cipher digraph. The method by which this change is brought about will be explained in detail in subsequent paragraphs. This joint characteristic of determination is indicated by overscoring the digraphs involved, thus $\overline{XPc}$=$\overline{\text{ACp}}$.

c. The primary purpose of polygraphic systems is to provide a means of eliminating, or at least suppressing, the frequency characteristic of plaintext letters. In the preceding cipher system, the importance of this phenomenon as an "in" to the analyst is amply demonstrated. In the case of uniliteral monoalphabetic substitution where a direct one-to-one ratio is obtained, it was shown that it could be solved quickly by a simple tabulation, applying the principles of frequency and laws of probability. So it was too in the case of multiliteral substitution systems, where several, though constant, cipher values could be reduced to uniliteral terms. The important point here is that security is not necessarily a factor of the ratio of cipher element to a plain element, nor to the complexity of the system, but to the total number of variations for each possible value of the system as a whole.

d. In polygraphic substitution, variations are introduced into the system through both the cipher and the plain components. The fact that encipherment can be accomplished by combining letters serves to decrease drastically the opportunity for application of the laws of probability and principles of frequency. For example, in a message of 100 characters enciphered by a uniliteral monoalphabetic substitution system, there are only 26 different possible letters that require identification. In a digraphic system based upon an alphabet of 26 letters, there are 676 possible combinations, and a message of the same length in a digraphic system would only represent 50, at the very most, of these possible combinations. Thus the laws of probability and frequency characteristics have a restricted range in which to operate.

10–2. (~~C~~) Polygraphic Substitution Using Tables

a. The simplest method of polygraphic substitution involves the use of a table similar to that shown in figure 10–1. The operation of the system is based upon row and column coordinates as the plaintext values, which are replaced by the cipher value found at their intersection. Thus $\overline{\text{AGp}}$ becomes

$\overline{FBc}$. In those cases where a single letter occurs, as for example at the end of a message, encipherment as a digraph is obtained by adding a null, preferably a high-frequency letter. Words are enciphered by dividing the word into digraphic elements, then using the plain digraphs as row and column coordinates to locate the equivalent cipher digraph. For example:

DEFACED
X DE FA CE D
YA NZ CY

P₂

		A	B	C	D	E	F	G	H	I	J	K		X	Y	Z
	A	*FX*	*CH*	*XE*	*YY*	*ZA*	*YG*	*FB*	*CD*	*EF*	*XJ*	*ZX*	. . .	*EA*	*DJ*	*FH*
	B	*NY*	*DC*	*NB*	*ZI*	*XX*	*DX*						. . .			
	C				*AH*				*AB*				. . .		*ND*	
	D			*BB*		*YA*					*AY*		. . .	*BF*		
	E	*AX*					*AI*						. . .			
P₁	F		*AG*			*NZ*			*AZ*				. . .	*AA*		
		:	:	:	:	:	:	:	:	:	:	:	. . .	:	:	:
	N		*BC*		*CY*								. . .		*BA*	*FE*
		:	:	:	:	:	:	:	:	:	:	:	. . .	:	:	:
	X					*AC*					*AJ*		. . .	*BE*		
	Y	*DE*						*AF*					. . .		*AD*	
	Z	*AE*								*BD*			. . .	*AK*		

Figure 10–1 (C). Reciprocal cipher table (U).

b. The analyst may have noted that the cipher in figure 10–1 is reciprocal, i.e. $\overline{\mathrm{AGp}}=\overline{FBc}$ and $\overline{FBc}=\overline{\mathrm{AGp}}$. This particular cipher is deliberately constructed in this manner for ease of use, being capable of use in both the enciphering and the deciphering process. Reciprocity is not an essential factor, and for purposes of security is usually avoided. The overall security of the system above, where only one cipher equivalent is available for each plaintext digraph, is directly dependent upon its use. The security of a cryptogram produced through its use is relatively good until such time as its overuse permits the isolation and identification of the more frequently used digraphs.

c. A similar system is illustrated in figure 10–2. Encipherment of plaintext values is again by the use of row and column coordinates. Thus $\overline{\mathrm{ABp}}$ becomes $\overline{EEc}$. Note, however, in this case the values are nonreciprocal, i.e. EEp=$\overline{OAc}$ rather than $\overline{ABc}$. To decipher a message, the cryptographer looks outward from the cipher digraph to row and column coordinates, thus locating its equivalent plaintext digraph.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	*WG*	*EE*	*SN*	*TR*	*IA*	*NL*	*GC*	*HT*	*OI*	*UO*	*AM*	*RP*	*BY*	*KB*	*CD*	*DF*	*FH*	*JJ*	*LK*	*MQ*	*PS*	*QU*	*VV*	*XW*	*YX*	*ZZ*
B	*EG*	*SE*	*TN*	*IR*	*NA*	*GL*	*HC*	*OT*	*UI*	*AO*	*RM*	*BP*	*KY*	*CB*	*DD*	*FF*	*JH*	*LJ*	*MK*	*PQ*	*QS*	*VU*	*XV*	*YW*	*ZX*	*WZ*
C	*SG*	*TE*	*IN*	*NR*	*GA*	*HL*	*OC*	*UT*	*AI*	*RO*	*BM*	*KP*	*CY*	*DB*	*FD*	*JF*	*LH*	*MJ*	*PK*	*QQ*	*VS*	*XU*	*YV*	*ZW*	*WX*	*EZ*
D	*TG*	*IE*	*NN*	*GR*	*HA*	*OL*	*UC*	*AT*	*RI*	*BO*	*KM*	*CP*	*DY*	*FB*	*JD*	*LF*	*MH*	*PJ*	*QK*	*VQ*	*XS*	*YU*	*ZV*	*WW*	*EX*	*SZ*
E	*IG*	*NE*	*GN*	*HR*	*OA*	*UL*	*AC*	*RT*	*BI*	*KO*	*CM*	*DP*	*FY*	*JB*	*LD*	*MF*	*PH*	*QJ*	*VK*	*XQ*	*YS*	*ZU*	*WV*	*EW*	*SX*	*TZ*
F	*NG*	*GE*	*HN*	*OR*	*UA*	*AL*	*RC*	*BT*	*KI*	*CO*	*DM*	*FP*	*JY*	*LB*	*MD*	*PF*	*QH*	*VJ*	*XK*	*YQ*	*ZS*	*WU*	*EV*	*SW*	*TX*	*IZ*
G	*GG*	*HE*	*ON*	*UR*	*AA*	*RL*	*BC*	*KT*	*CI*	*DO*	*FM*	*JP*	*LY*	*MB*	*PD*	*QF*	*VH*	*XJ*	*YK*	*ZQ*	*WS*	*EU*	*SV*	*TW*	*IX*	*NZ*
H	*HG*	*OE*	*UN*	*AR*	*RA*	*BL*	*KC*	*CT*	*DI*	*FO*	*JM*	*LP*	*MY*	*PB*	*QD*	*VF*	*XH*	*YJ*	*ZK*	*WQ*	*ES*	*SU*	*TV*	*IW*	*NX*	*GZ*
I	*OG*	*UE*	*AN*	*RR*	*BA*	*KL*	*CC*	*DT*	*FI*	*JO*	*LM*	*MP*	*PY*	*QB*	*VD*	*XF*	*YH*	*ZJ*	*WK*	*EQ*	*SS*	*TU*	*IV*	*NW*	*GX*	*HZ*
J	*UG*	*AE*	*RN*	*BR*	*KA*	*CL*	*DC*	*FT*	*JI*	*LO*	*MM*	*PP*	*QY*	*VB*	*XD*	*YF*	*ZH*	*WJ*	*EK*	*SQ*	*TS*	*IU*	*NV*	*GW*	*HZ*	*OZ*
K	*AG*	*RE*	*BN*	*KR*	*CA*	*DL*	*FC*	*JT*	*LI*	*MO*	*PM*	*QP*	*VY*	*XB*	*YD*	*ZF*	*WH*	*EJ*	*SK*	*TQ*	*IS*	*NU*	*GV*	*HW*	*OX*	*UZ*
L	*RG*	*BE*	*KN*	*CR*	*DA*	*FL*	*JC*	*LT*	*MI*	*PO*	*QM*	*VP*	*XY*	*YB*	*ZD*	*WF*	*EH*	*SJ*	*TK*	*IQ*	*NS*	*GU*	*HV*	*OW*	*UX*	*AZ*
M	*BG*	*KE*	*CN*	*DR*	*FA*	*JL*	*LC*	*MT*	*PI*	*QO*	*VM*	*XP*	*YY*	*ZB*	*WD*	*EF*	*SH*	*TJ*	*IK*	*NQ*	*GS*	*HU*	*OV*	*UW*	*AX*	*RZ*
N	*KG*	*CE*	*DN*	*FR*	*JA*	*LL*	*MC*	*PT*	*QI*	*VO*	*XM*	*YP*	*ZY*	*WB*	*ED*	*SF*	*TH*	*IJ*	*NK*	*GQ*	*HS*	*OU*	*UV*	*AW*	*RX*	*BZ*
O	*CG*	*DE*	*FN*	*JR*	*LA*	*ML*	*PC*	*QT*	*VI*	*XO*	*YM*	*ZP*	*WY*	*EB*	*SD*	*TF*	*IH*	*NJ*	*GK*	*HQ*	*OS*	*UU*	*AV*	*RW*	*BX*	*KZ*
P	*DG*	*FE*	*JN*	*LR*	*MA*	*PL*	*QC*	*VT*	*XI*	*YO*	*ZM*	*WP*	*EY*	*SB*	*TD*	*IF*	*NH*	*GJ*	*HK*	*OQ*	*US*	*AU*	*RV*	*BW*	*KX*	*CZ*
Q	*FG*	*JE*	*LN*	*MR*	*PA*	*QL*	*VC*	*XT*	*YI*	*ZO*	*WM*	*EP*	*SY*	*TB*	*ID*	*NF*	*GH*	*HJ*	*OK*	*UQ*	*AS*	*RU*	*BV*	*KW*	*CX*	*DZ*
R	*JG*	*LE*	*MN*	*PR*	*QA*	*VL*	*XC*	*YT*	*ZI*	*WO*	*EM*	*SP*	*TY*	*IB*	*ND*	*GF*	*HH*	*OJ*	*UK*	*AQ*	*RS*	*BU*	*KV*	*CW*	*DX*	*FZ*
S	*LG*	*ME*	*PN*	*QR*	*VA*	*XL*	*YC*	*ZT*	*WI*	*EO*	*SM*	*TP*	*IY*	*NB*	*GD*	*HF*	*OH*	*UJ*	*AK*	*RQ*	*BS*	*KU*	*CV*	*DW*	*FX*	*JZ*
T	*MG*	*PE*	*QN*	*VR*	*XA*	*YL*	*ZC*	*WT*	*EI*	*SO*	*TM*	*IP*	*NY*	*GB*	*HD*	*OF*	*UH*	*AJ*	*RK*	*BQ*	*KS*	*CU*	*DV*	*FW*	*JX*	*LZ*
U	*PG*	*QE*	*VN*	*XR*	*YA*	*ZL*	*WC*	*ET*	*SI*	*TO*	*IM*	*NP*	*GY*	*HB*	*OD*	*UF*	*AH*	*RJ*	*BK*	*KQ*	*CS*	*DU*	*FV*	*JW*	*LX*	*MZ*
V	*QG*	*VE*	*XN*	*YR*	*ZA*	*WL*	*EC*	*ST*	*TI*	*IO*	*NM*	*GP*	*HY*	*OB*	*UD*	*AF*	*RH*	*BJ*	*KK*	*CQ*	*DS*	*FU*	*JV*	*LW*	*MX*	*PZ*
W	*VG*	*XE*	*YN*	*ZR*	*WA*	*EL*	*SC*	*TT*	*II*	*NO*	*GM*	*HP*	*OY*	*UB*	*AD*	*RF*	*BH*	*KJ*	*CK*	*DQ*	*FS*	*JU*	*LV*	*MW*	*PX*	*QZ*
X	*XG*	*YE*	*ZN*	*WR*	*EA*	*SL*	*TC*	*IT*	*NI*	*GO*	*HM*	*OP*	*UY*	*AB*	*RD*	*BF*	*KH*	*CJ*	*DK*	*FQ*	*JS*	*LU*	*MV*	*PQ*	*QX*	*VZ*
Y	*YG*	*ZE*	*WN*	*ER*	*SA*	*TL*	*IC*	*NT*	*GI*	*HO*	*OM*	*UP*	*AY*	*RB*	*BD*	*KF*	*GH*	*DJ*	*FK*	*JQ*	*LS*	*MU*	*PV*	*QW*	*VX*	*XZ*
Z	*ZG*	*WE*	*EN*	*SR*	*TA*	*IL*	*NC*	*GT*	*HI*	*OO*	*UM*	*AP*	*RY*	*BB*	*KD*	*CF*	*DH*	*FJ*	*JK*	*LQ*	*MS*	*PU*	*QV*	*VW*	*XX*	*YZ*

Figure 10–2 (~~C~~). Nonreciprocal cipher table (U).

d. Although the table above is nonreciprocal, a close examination reveals a certain symmetry of values in the inscription of the cipher elements. The result is that, unlike the former table, the encipherment is not truly digraphic in character. Note that in the case where the second digit of the plain digraph remains constant, the second digit of the cipher digraph also remains constant. Thus AAp=*WGc*, BAp=*EGc*, CAp=*SGc*, etc.; AAp=*WGc*, ABp=*EEc* and ACp=*SNc*. The total result is that the encipherment cf the first character of the digraph is always polyalphabetic, while the encipherment of the last character of the digraphs is monoalphabetic in vertical encipherment.

e. Generally, digraphic substitution using tables such as those previously illustrated are impractical for military use. This is not due primarily to their security faults, as this can be corrected, but because of their physical limitations. The relatively large size of the tables, the inconvenience of their production, change, distribution, and handling make their use impractical. Moreover, the same, or better cryptographic results can be obtained by the use of matrices.

10–3. (~~C~~) Polygraphic Substitution Using Matrices

a. A simple method for obtaining digraphic substitution is through the use of a four-square matrix. This is a matrix which contains four components, two cipher and two plain, each inscribed in a 5 x 5 square. The components are 25-letter alphabets in which two letters are combined, normally the I and the J (only the I being shown), and inscribed in the square by some predetermined order. Figure 10–3 depicts a normal four-square matrix.

	A	B	C	D	E	F	O	U	R	T	
	F	G	H	I/J	K	L	M	P	Q	E	
P1	L	M	N	O	P	K	Y	Z	S	N	C1
	Q	R	S	T	U	I/J	X	W	V	A	
	V	W	X	Y	Z	H	G	D	C	B	
	T	H	I/J	R	E	A	B	C	D	E	
	O	P	Q	S	N	F	G	H	I/J	K	
C2	M	Y	Z	U	A	L	M	N	O	P	P2
	L	X	W	V	B	Q	R	S	T	U	
	K	G	F	D	C	V	W	X	Y	Z	

Figure 10–3 (~~C~~). *Four-square matrix* (*U*).

(1) Digraphic encipherment is accomplished by locating the first character of the plain digraph in section P1 and the second in section P2. The substitution cipher values are found in section C1 and C2 respectively at the opposite corners of an imaginary square or rectangle. Thus ZAp becomes *HEc*. This is demonstrated in figure 10–4①.

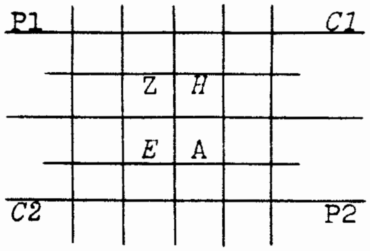


Figure 10–4① (~~C~~). *Enciphering operation, four-square matrix* (*U*).

(2) Decipherment is exactly the reverse of the enciphering process as shown in figure 10–4②. The units of the cipher digraphs are located in section C1 and C2 respectively, and their equivalent plaintext values are found at the intersection of an imaginary square or rectangle in section P1 and P2. For example *XEc*=UBp.

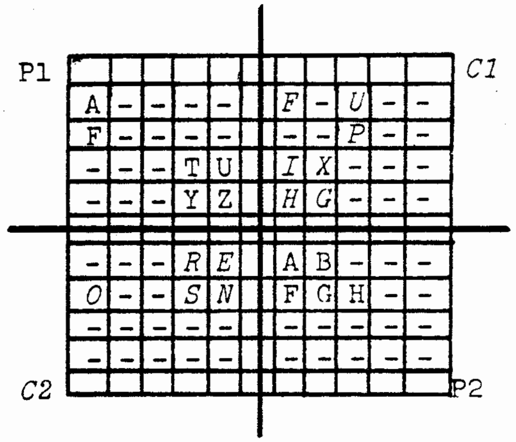


Figure 10–4② (~~C~~). *Deciphering operation four-square matrix* (*U*).

(3) Note that with each successive plain-cipher digraphic relationship, a new enciphering rectangle is created and outlined. Thus, what was previously mentioned as the ideal of polygraphic substitution now occurs. No individual letter by itself has any attached specific value. Rather its value only occurs as a result of its combination with another letter, and for each combination, different values result. Thus in figure 10–4② AFp=*FOc*, AHp=*UOc*, and FHp=*POc*.

b. It is possible to effect the same type of encipherment by using a two-square matrix and a modification in the method of finding equivalents. One such two-square arrangement, a horizontal two-square, is illustrated in figure 10–5.

	M	*A*	*N*	*U*	*F*	*A*	*U*	*T*	*O*	*M*	
P1	*C*	*T*	*R*	*I*	*G*	*B*	*I*	*L*	*E*	*S*	P2
C2	*B*	*D*	*E*	*H*	*K*	*C*	*D*	*F*	*G*	*H*	*C1*
	L	*O*	*P*	*Q*	*S*	*K*	*N*	*P*	*Q*	*R*	
	V	*W*	*X*	*Y*	*Z*	*V*	*W*	*X*	*Y*	*Z*	

Figure 10–5 (~~C~~). Horizontal two-square matrix (U).

Basically the method of encipherment is identical with that of the four-square method, the equivalent cipher values for P1 and P2 being found at the opposite corners of an imaginary rectangle in section C1 and C2 respectively. Thus $\overline{\mathrm{MPp}}=\overline{TLc}$. The exception to this rule is when the two plaintext letters appear on the same horizontal row. In these cases, the cipher digraph produced is a reversal of the plaintext digraphs. For example, the cipher equivalent for $\overline{\mathrm{TEp}}$ is $\overline{ETc}$. Observe that in both cases the first cipher letter is in the same column as the second plaintext letter.

c. Digraphic substitution of the same sort may also be effected by the use of a vertical two-square matrix as illustrated in figure 10–6.

	M	*A*	*N*	*U*	*F*	
P1	*C*	*T*	*R*	*I*	*G*	*C1*
	B	*D*	*E*	*H*	*K*	
	L	*O*	*P*	*Q*	*S*	
	V	*W*	*X*	*Y*	*Z*	
	A	U	T	O	M	
	B	I	L	E	S	
P2	C	D	F	G	H	*C2*
	K	N	P	Q	R	
	V	W	X	Y	Z	

Figure 10–6 (~~C~~). Vertical two-square matrix (U).

(1) The principle of encipherment and decipherment is once again the same as in the preceding example. The ciphertext values are found at the opposite corners of an imaginary rectangle, delineated by the position of the first and second digits of the plaintext digraphs. For example $\overline{\mathrm{MOp}}$ becomes $\overline{UAc}$. In this matrix where the two plaintext letters are found in the same column, the cipher digraphs are identical. Thus $\overline{\mathrm{MAp}}$ becomes $\overline{MAc}$. Note that unlike the horizontal two-square, the cipher equivalent is not a reversal of the same letter but the same letters in the same sequence as the plaintext.

(2) In both the vertical and the horizontal two-square systems shown above, the encipherment of a single letter can be accomplished only by adding a null to form a plaintext digraph. Usually, for reasons of security, the null chosen is a high-frequency letter.

d. A third method of digraphic encipherment using matrices is the Playfair cipher which involves only the use of one 5 x 5 square. The use of a single matrix is possible by yet another modification of the system of finding cipher equivalents, which results in a greater degree of security. A typical Playfair cipher is illustrated below:

A	*Q*	*P*	*O*	*N*
B	*R*	*Y*	*X*	*M*
C	*S*	*Z*	*W*	*L*
D	*T*	*U*	*V*	*K*
E	*F*	*G*	*H*	*I*

Encipherment and decipherment are considered in light of four categories of plaintext placement.

(1) When the members of the plaintext pair are at the opposite ends of a diagonal of an imaginary rectangle, the replacement cipher members are at the opposite ends of the other diagonal. Thus $\overline{\mathrm{AHp}}=\overline{OEc}$. Note that cipher 1 always is selected from the same row in which plain 1 appears; thus $\overline{\mathrm{ZEp}}=\overline{CGc}$, and $\overline{\mathrm{BZp}}=\overline{YCc}$.

(2) When the members of the plaintext pair lie in the same row, the letters immediately to their right form the cipher pair. Thus $\overline{\mathrm{APp}}=\overline{QOc}$, $\overline{\mathrm{POp}}=\overline{ONc}$, and $\overline{\mathrm{ONp}}=\overline{NAc}$.

(3) When the members of the plaintext pair lie in the same column, the letters immediately below them form the cipher pairs. Thus $\overline{\mathrm{ADp}}=\overline{BEc}$, $\overline{\mathrm{CEp}}=\overline{DAc}$, and $\overline{\mathrm{EBp}}=\overline{ACc}$. In both this case and that above, the rows and columns form continuous circles.

(4) When the members of the plaintext pairs are repeated letters, they must be separated by inserting a null, in this case usually a low-frequency letter such as Q or X, and then be enciphered by one of the three methods above. For example, the word BATTLES is enciphered as:

BA TQ TL ES
CB FR KS FC

A Playfair square is automatically reciprocal so far as encipherment by method (1) above is concerned. Thus $\overline{\mathrm{AYp}}=\overline{PBc}$, and $\overline{\mathrm{PBp}}=\overline{AYc}$. This reciprocity does not occur in method (2) and (3) above. Decipherment takes the exact reverse pattern of those methods outlined for encipherment.

10–4. (~~C~~) Variant Forms of Polygraphic Encipherment

a. In the foregoing paragraphs, polygraphic encipherment is totally limited to its digraphic forms for which table and matrices are used. It is important that the same basic system is so constructed as to provide trigraphic and tetragraphic encipherment and even combinations of these. In effect, the systems operate on the same general cryptographic principles with some variation to fit the specific case.

b. One possible variation of a Playfair square is shown below. This illustrates that matrices need not always be square, though this is the most common form.

W	*A*	*S*	*H*	*I*	*N*
G	*T*	*O*	*B*	*C*	*D*
E	*F*	*J*	*KA*	*KE*	*KI*
KO	*KU*	*L*	*M*	*P*	*Q*
R	*U*	*V*	*X*	*Y*	*Z*

c. Encipherment of a message by the system results in the introduction of an occasional trigraph or tetragraph in addition to the normally expected digraphs. Thus $\overline{\text{AMp}}=\overline{HKUc}$ and $\overline{\text{EPp}}=\overline{KEKOc}$. Also a number of variant values may be introduced, as CKp could equally be represented by $\overline{BKEc}$, $\overline{KEPc}$, $\overline{DKEc}$, $\overline{GPc}$, and $\overline{TPc}$. Insofar as deciphering the possible variants shown above, the deciphering clerk would merely ignore any letters following the K when obtained in the process of decipherment. Thus $\overline{\text{CKOp}}$ would be read as CK.

d. A numeric variation of the four-square system shown earlier which permits a trinomic substitution of digraphic plaintext elements is illustrated in figure 10–7.

	A	B	C	D	E	000	025	050	075	100	
	F	G	H	I	K	125	150	175	200	225	
P1	L	M	N	O	P	250	275	300	325	350	C1
	Q	R	S	T	U	375	400	425	450	475	
	V	W	X	Y	Z	500	525	550	575	600	
	Ø	1	2	3	4	V	Q	L	F	A	
	5	6	7	8	9	W	R	M	G	B	
C2	1Ø	11	12	13	14	X	S	N	H	C	P2
	15	16	17	18	19	Y	T	O	I	D	
	20	21	22	23	24	Z	U	P	K	E	

Figure 10–7 (C). Numeric variation, four-square matrix (U).

(1) Encipherment of a message proceeds as normal for a four-square system, but the numeric values are added rather than used as tetranomes or pentanomes.

PR	OC	EE	DI	NG
275	350	100	075	325
9	13	24	18	7
284	363	124	093	332

(2) Decipherment is accomplished by determining the greatest multiple of 25 contained in a given trigraph and then subtracting that multiple from the trigraph to derive C1 and C2.

284=275 284=275+9 $\overline{275c-9c}=\overline{\text{PRp}}$

e. The clumsiness of the two preceding systems explains why they are not often encountered in actual operations. As stated previously, one of the important requirements of a cryptographic system is that it be practical for common usage. While the systems do provide a degree of extra security, the amount gained is hardly worth the effort.

Section II. (C) RECOGNITION AND IDENTIFICATION OF POLYGRAPHIC SUBSTITUTION

10–5. (C) Recognition of Polygraphic Substitution

a. The methods of determining whether a given message represents a case of polygraphic substitution are rather simple. Usually a close inspection of certain of its physical characteristics suffices. When the techniques do not give clear-cut answers or when the lack of volume of text to study makes its use inappropriate, the analyst still has recourse to statistical tests and identification tables.

b. Digraphic substitution systems generally exhibit one or more of the following characteristics.

(1) Excluding nulls and indicators, message length, textual repeats, and internal distances will be multiples of two.

(2) When the ciphertext is composed entirely of letters, all are present, except one, usually the J, the U, or the V.

(3) If the ciphertext is composed of numbers when divided into trinomes, a limitation of range occurs, usually 001–676.

(4) Repeats usually begin on the odd letters and end on the even letters.

(5) The cryptogram does not yield to a multiliteral solution. Thus because of its digraphic characteristics, it most likely is digraphic.

c. In those cases where the ciphertext under study is trigraphic, similar general rules apply.

(1) Message length, repetitions, and intervening distance are usually multiples of three.

(2) Repetition usually begins with the first letter and ends with the third letter of the trigraphic ciphertext.

(3) If the cryptogram does not yield to solution of triliteral ciphers, it can be assumed to be trigraphic because of its characteristics discussed above.

d. Should the above listed characteristics prove inconclusive, initial identification may be made through the use of the statistical test and table which is covered in the following paragraph.

10–6. (~~C~~) The Digraphic Lambda (λ) Test

a. The digraphic blank expectation test, in all respects, except the form of the element treated, is the same as that for the monographic blank expectation test. Both rest on the theory that, given a certain length of plaintext and a predictable number of blanks, the nonusage of a letter will occur. The occurrences refer both to that expected for plaintext and random text, and in this test are based on digraphic elements rather than individual letters, as was the case of the former test. Again 200 elements, in this case digraphs, set the limit of messages which may be tested. Tests of messages greater than 200 elements in length are inconclusive. The digraphic test is given in chart form below in figure 10–8.

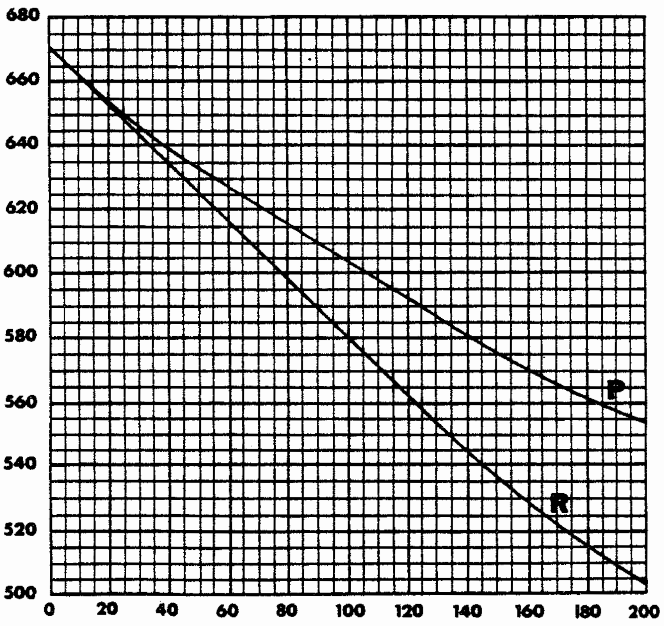


Figure 10–8 (U). Digraphic Lambda (λ) test (U).

b. Using this chart, identification is based upon the number of blanks, where a blank is a nonoccurrence of a digraph, occurring in a cipher message not exceeding 200 digraphs in length, in respect to the number of blanks, expected in plaintext and random messages of the same length. As can be seen, the chart contains two curves; curve P refers to expected blanks for plaintext and curve R refers to expected blanks for random text. In using the chart, plot the point of intersection of the vertical line (corresponding to the total number of digraphs in a given message) with the horizontal line which corresponds to the total number of blanks occurring in that message. If this point of intersection falls closer to curve P than it does to curve R, it indicates that the cryptogram is digraphic. If it falls closer to curve R than curve P, a nondigraphic substitution cipher is indicated.

c. A cipher which is polyalphabetic and which involves only two cipher components gives essentially the same results as a cipher which is truly digraphic. For this reason this test should not be used exclusively for the identification of a digraphic system, but rather to substantiate other evidence.

d. Where it becomes necessary to distinguish between a digraphic cipher and a polyalphabetic cipher using two cipher components, a digraphic frequency distribution could be made "off the cut," i.e. made of those ciphertext digraphs which are found by omitting the first letter of text, then dividing the remaining text into groups of two letters. If the system is digraphic, a distribution exhibits a poor 2ϕo; if, on the other hand, it is polyalphabetic, the 2ϕo is as satisfactory as that of a distribution made "on the cut."

10–7. (~~C~~) The Digraphic Phi Test (2ϕo)

a. The computation of the value of 2ϕo, 2ϕp, and 2ϕr for this test is the same as that given in paragraph 9–7 preceding. The difference lies in its use for the identification of digraphic systems and the interpretation of its resultant values. In digraphic systems involving substitution where all the letters of the alphabet are used, except the limitation imposed by a 25-cell matrix, the value computed for 2ϕo approaches that of 2ϕp for English plaintext which is 4.66.

b. Note again that the results of digraphic tests are subject to much wider variation than similar tests for monographic systems. Factors which contribute to this are the limited number of digraphs, of a possible 625, which may be required to encipher the text, and the presence of repeated digraphs in the text which further reduce the total number of digraphs. The end result is that statistical results must be used with caution.

10–8. (~~C~~) Identification of the Specific System

a. Once the initial recognition of a cipher message as a polygraphic cipher has been accomplished, the next step preparatory to analysis is the identification of the specific system to which it belongs. This identification can frequently be made on the basis of certain characteristics of the ciphertext which result from the method of encipherment. These individual characteristics are listed below.

(1) *Four-square ciphers.* The identification of a cipher message as the product of this system rests generally on a process of eliminating other digraphic systems as possibilities. This is not to mean that the text itself does not exhibit characteristics of its own. It does, but the identification of these characteristics are not as readily apparent and involve detailed study, while the characteristics of the other systems can often be noted by a visual inspection alone.

(2) *Two-square system.* Two-square systems are identified by the presence of plaintext digraphs in the ciphertext. Under normal circumstances approximately 20 percent of all digraphs produced by this system will be plaintext. In the specific case of a horizontal two-square system, the digraphs will be reversed. In the case of vertical two-square encipherment, the plaintext digraphs will occur in their original sequence.

(3) *Playfair ciphers.* A cipher produced by this system is generally identified by the complete absence of digraphs containing repeated letters. The reason for the absence of repeated letters as digraphs is a consequence of the fourth rule of the encipherment given in paragraph 10–3*d*(4).

(4) *Large tables.* Because of the systematic arrangement of the internal cipher values in tables such as that illustrated in figure 10–2 preceding, identification is made by a simple uniliteral frequency distribution of the letters of the cipher digraphs. For example, note that any plaintext digraph ending in A contains *Gc* as the last letter of the cipher digraph; thus $\overline{\mathrm{AA}p}=\overline{WGc}$, $\overline{\mathrm{BA}p}=\overline{EGc}$, etc. Other arrangements which are symmetrical would give similar results.

b. The above examples often allow identification by visual inspection alone. Where this is not possible, the analyst must study a given cipher in detail using procedures which are covered in succeeding paragraphs.

CHAPTER 11 (~~C~~)

SOLUTION OF POLYGRAPHIC SUBSTITUTION SYSTEMS

Section I. (~~C~~) ANALYSIS OF DIGRAPHIC CIPHERS

11-1. (~~C~~) Introduction

a. The fundamental purpose of polygraphic substitution is the suppression or total elimination of the frequency characteristics of ordinary plaintext, for it is these frequency characteristics which lead, sooner or later, to the solution of practically all substitution ciphers. The analysis of cryptograms which are the result of polygraphic substitution rests upon the basis of the frequency of the units concerned. If the substitution is digraphic, the units studied are pairs of letters and the normal frequencies of plaintext pairs become of primary concern. If the system is trigraphic, the units are sets of three letters, etc.

b. Although analysis is chiefly a case of studying frequencies, additional aid is provided by certain digraphic idiomorphs, which are the result of the particular method of digraphic encipherment used. Additionally, any knowledge available to the analyst in respect to the subject, possible contents, and the circumstances surrounding a given message are always invaluable in reaching a final solution. In any case, when a digraph is used regularly, sufficient messages soon accumulate to the point of solution by principles of frequency. In this respect note that the "sufficient quantity" varies. In some cases, where digraphic idiomorphism is pronounced, and when a number of repetitions are available, solution may be practical with only a few messages.

c. In digraphic systems in particular, the identification of only a few cipher digraphs is usually sufficient to read out longer portions of the messages. This is due to the limitation placed on the value that can be inserted between those high-frequency values normally first recovered. For example, consider the following, a portion of digraphic ciphertext with its recovered plaintext values.

```
XQ VO ZI LK AP OL ZX PV CK IK OL UK AT
      ND IN    NT    RE       NT NO
HN LK VL BN OZ BZ DY TY LE GI
   IN    SI    ON TO
```

d. With a little imagination, the partially recovered plaintext could be expanded to "SECOND INFANTRY REGIMENT." Moreover, if $\overline{CKc}=\overline{\mathrm{GIp}}$ then possibly $\overline{GIc}=\overline{\mathrm{CKp}}$, the last portion of the message subject "ATTACK." On this basis the sequence might be:

"SECOND INFANTRY REGIMENT NOT YET IN POSITION TO ATTACK."

Although these values rest on an assumption only, their validity could soon be verified; first, by attempting additional decipherment, and second, by fitting the values into the matrix which originally produced them.

e. In a manner similar to uniliteral systems, the placement of repeated digraphs at once aids and limits the choice of probable words. For example, the following repetition extracted from a message appears possible as a whole word.

VI FW HM AZ FF FW RO

In terms of digraphic idiomorphs it would be assigned the pattern

– AB – – – AB –

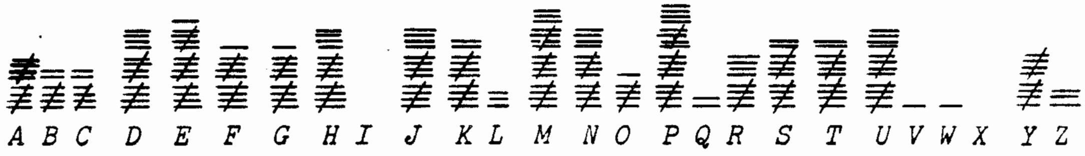
This pattern compared to those listed in appendix D (table D-4) reveals several possible words which could be used to form a base for further development of the text, by trying the set of values derived from each, in turn.

11-2. (~~C~~) Identification of Four-Square Ciphers

a. The general steps and techniques involved in the analysis and solution of a four-square cipher system are demonstrated below. Admittedly, the situation given represents a special case in that the solution is based on one message. However, the methodology remains the same for most cases, only slight variation being required to fit it to any given set of circumstances. The first step in any analytic attack is system identification. The following messages illustrate identification techniques employed in the case of four-square ciphers and subsequent analysis.

```
UNONY  TPKKM  JKZDK  JJSGR  TGLWR  AEMYP
RCJCP  YDEBC  DFHMR  MKGZA  PKPSK  MUNON
YTUFE  UUFUE  FAYVD  AMTDM  UDPEY  PPYEM
YPRCJ  CPYDE  BCDFP  SYKNE  TJSZO  UDRJG
HMUNE  MRUAS  SAPSK  MRLHS  BROUN  EETUO
JNNSA  RKDEM  REFGP  EHMDE  AMKAJ  GEMQJ
PTUDB  BDGLM  FAPSF  JPTFF  BMDCG  TSGPS
KMTGJ  GTJUN  BFNJO  NUNNT
```

b. As a preliminary step, the cipher is tested for monoalphabetic qualities by using standard alphabets and by completing the plain component as shown in paragraph 7–12. As negative results are obtained, a uniliteral frequency distribution is made as shown in figure 11–1 to determine if a mixed alphabet is involved.



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
10	7	7	14	16	11	11	14	0	14	12	3	18	14	6	19	2	9	12	12	14	1	1	0	10	3

Figure 11–1 (U). Uniliteral frequency distribution, four-square cipher (U).

Although the uniliteral frequency distribution appears rough enough to warrant an initial monoalphabetic assumption, closer inspection reveals that except for three letters there is really little frequency variation, less than might be expected for a message of this length. A ϕ test could be made if further identification is required, but considering the size of the sample and its apparent flatness, it is hardly warranted.

c. Having rejected monoalphabetic substitution, there is no need to consider transposition, as the message is not rearranged plaintext. Digraphic substitution is the next logical consideration. For this, the ciphertext is divided into digraphic units. Repeats are underlined and inspected for idiomorphic characteristics as shown in figure 11–2①.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
A	UN	ON	YT	PK	KM	JK	ZD	KJ	JS	GR	TG	LW	RA	EM	YP
B	RC	JC	PY	DE	BC	DF	HM	RM	KG	ZA	PK	PS	KM	UN	ON
C	YT	UF	EU	UF	UE	FA	YV	DA	MT	DM	UD	PE	YP	PY	EM
D	YP	RC	JC	PY	DE	BC	DF	PS	YK	NE	TJ	SZ	OU	DR	JG
E	HM	UN	EM	RU	AS	SA	PS	KM	RL	HS	BR	OU	NE	ET	UO
F	JN	NS	AR	KD	EM	RE	FG	PE	HM	DE	AM	KA	JG	EM	QJ
G	PT	UD	BB	DG	LM	FA	PS	FJ	PT	FF	BM	DC	GT	SG	PS
H	KM	TG	JG	TJ	UN	BF	NJ	ON	UN	NT					

Figure 11–2① (~~C~~). Cipher text prepared for analysis (U).

d. On the strength of the digraphic patterns exhibited by the text, divisible by two, and repetitions consisting of digraphs, it can be assumed to be a digraphic cipher. Confirmation of this assumption can be obtained by constructing a digraphic frequency distribution as shown in figure 11–2②.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
A													—					—	—								3
B		—	=			—							—					—									6
C																											
D	—		—		≡	=	—						—					—									10
E													≢							—	—						7
F	=					—	—			—																	5
G																		—		—							2
H													≡								—						4
I																											
J			=				≡				—			—							—						8
K	—			—			—			—			≣														8
L													—										—				2
M																				—							1
N					=					—									—	—							5
O															≡						=						5
P					=						=								≢	—					≡		14
Q										—																	1
R	—		=		—							—	—								—						7
S	—						—																		—		3
T							=			=																	4
U				—	=	=								≢	—												11
V																											
W																											
X																											
Y											—					≡				=		—					7
Z	—			—																							2
	7	1	7	2	10	6	9	0	0	6	4	1	17	9	1	3	0	4	9	8	4	1	1	0	4	0	
	6	1	4	2	5	4	6			5	3	1	8	3	1	1	0	4	5	6	3	1	1		4		74
F(F−1)	2		6		12	4	8			2	2		38	20	6	6			20	2	2				6		136

Figure 11-2② (~~C~~). *Digraphic frequency distribution* (*U*).

e. The appearance of this distribution shows some characteristics of digraphic substitution. Given an alphabet of 26 letters, there are 676 possible digraphic combinations. For an alphabet of 25 letters, there are 625 possible combinations. Of these, only about 300 are used in normal plaintext. In the message above, only 74 different digraphs are used, 602 total blanks assumed. For a message of 74 digraphs, the normally expected number of blanks given by the digraphic Lambda table falls within the range 617 for plaintext and 606 for random text. With such a small sample as this, the expected pattern is liable to be distorted. However, considering the number of repeated sequences in such a short message and the obvious absence of several letters, the nearness of observed blanks to expected blanks for random text may be explained in part. Furthermore, a digraphic ϕ test reflects the same condition with the observed digraphic Phi value ($2\phi o$) of 136 surpassing that expected for plain

$(2\phi p)$ 106.95, the expected random value (2ϕ) being 23.25. Note that when a digraph frequency table is used, as in figure 11–2② the value of F is found in each cell. For example, in the first column 2 is found for the digraph FA, thus $F(C-1)=2\times1=2$ for this column. To find the total, the total values of each column are then added.

11–3. (~~C~~) Analysis of Four-Square Ciphers

a. Accepting the system as digraphic, reexamination of the text reveals a doublet, the digraph FF; therefore, a Playfair cipher can be discounted. In two-square ciphers 20 percent of the total text would be plaintext, normal in the case of a vertical arrangement and reversed if the arrangement of the matrices were horizontal. Failing to note any great number of obvious plaintext digraphs, normal or reversed, the analyst can assume that a four-square system is represented. Accordingly, a matrix can be constructed as shown in figure 11–3. Direct standard alphabets are used for 12p, as this is the normal arrangement, the I and J are combined because of the absence of the former in the digraphic frequency distribution.

	A	B	C	D	E						
	F	G	H	J	K						
P1	L	M	N	O	P						C1
	Q	R	S	T	U						
	V	W	X	Y	Z						
						A	B	C	D	E	
						F	G	H	J	K	
C2						L	M	N	O	P	P2
						Q	R	S	T	U	
						V	W	X	Y	Z	

Figure 11–3 (~~C~~). Assumed plain component, four-square matrix (U).

(1) Referring back to the ciphertext, the repeat $\overline{PS}$ $\overline{KM}$ appears three times at rather regular intervals in the text. By position it seems to be a sentence separator and being of four letters the word STOP is immediately assumed. Thus $\overline{PSc}$ is assumed to be STp and $\overline{KMc}$ is $\overline{OPp}$. These values are accordingly inserted in the matrix, figure 11–4.

	A	B	C	D	E						
P1	F	G	H	J	K						
	L	M	N	O	P					*K*	C1
	Q	R	S	T	U				*P*		
	V	W	X	Y	Z						
						A	B	C	D	E	
						F	G	H	J	K	
C2				*M*		L	M	N	O	P	P2
			S			Q	R	S	T	U	
						V	W	X	Y	Z	

Figure 11–4 (C). Insertion of cipher values (U).

(2) The placement of these cipher equivalents allows the assumption of fourth placement by position alone. Generally the cipher component can be a standard sequence, a mixed sequence, or a random sequence. Further it may be inscribed into the matrix by a number of different routes. If the alphabet is standard, or keyword mixed, it is very likely that the last letters, the V–W–X–Y–Z cluster is undisturbed in respect to sequence, and if so will fall at the end of the inscription route. If the route of inscription can be determined, these letters can be placed with a certain degree of certainty. The direction of a route may sometimes be determined by the placement of the cluster letters. For example, the relative position of *Kc* and *Pc* in sequence C1 can be considered in a former light. Normally, four letters separate K and P (K L M N O P); if normal horizontal inscription is assumed for this square, three blank cells are found where four are required. Therefore it can be one of the following conditions.

(*a*) The route of inscription is something other than normal horizontal.

(*b*) That portion of the cipher component containing *K* and *P* is either mixed or has a letter missing, the letter being used in the keyword.

(*c*) Both (1) and (2) are in effect.

The first option is disproved by a simple count. The third cannot yet be disproved. In counting, however, it is observed that *K* appears in the 15th position when normally it occurs at the 11th. This means that four letters normally following it must now precede it. If this is so, a missing letter between *K* and *P* would account for only the three cells present. Furthermore, *P* which normally occurs at the 16th position is so located to provide space for only six following letters, indicating that four letters normally following it now come before. Thus, four of the letters shown below must precede the *K*:

$\underline{K}$ L M N O $\underline{P}$ Q R S T U V W X Y $\underline{Z}$
1 missing 4 missing

(3) Considering which letters can be missing in the light of their normal frequency of use may prove useful. Between *K* and *P*, *O* is probably that missing letter since it may be part of a keyword. From *P* to *Z: RSTU* or perhaps, *QU* and two of the cluster *RST* may be missing. The choice here with more letters, is more difficult. One aspect, however, is that the missing letters are probably not *VWXYZ*. On this basis, placements may be assumed as follows:

C1
K
L M N P
V W X Y Z

(4) By applying the same line of reasoning to the placement of cipher elements in the C2 square, the additional placements may also be assumed, giving a partially completed matrix as seen in figure 11–5.

	A	B	C	D	E						
	F	G	H	J	K						
P1	L	M	N	O	P					*K*	*C1*
	Q	R	S	T	U	*L*	*M*	*N*	*P*		
	V	W	X	Y	Z	*V*	*W*	*X*	*Y*	*Z*	
						A	B	C	D	E	
						F	G	H	J	K	
C2				*M*		L	M	N	O	P	P2
			S	*T*	*U*	Q	R	S	T	U	
	V	*W*	*X*	*Y*	*Z*	V	W	X	Y	Z	

Figure 11–5 (~~C~~). Placement of cipher values by assumption of sequence (U).

(5) To this point, assumption has been added to assumption, a sometimes dangerous practice but one which can be rectified quickly by checking the assumptions against the ciphertext, figure 11–6.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
A	*UN*	*ON*	*YT*	*PK*	*KM*	*JK*	*ZD*	*KJ*	*JS*	*GR*	*TG*	*LW*	*RA*	*EM*	*YP*
			YT		OP							RV			
B	*RC*	*JC*	*PY*	*DE*	*BC*	*DF*	*HM*	*RM*	*KG*	*ZA*	*PK*	*PS*	*KM*	*UN*	*ON*
			TY								RO	ST	OP		
C	*YT*	*UF*	*EU*	*UF*	*UE*	*FA*	*YV*	*DA*	*MT*	*DM*	*UD*	*PE*	*YP*	*PY*	*EM*
	YT						VY		TR					TY	
D	*YP*	*RC*	*JC*	*PY*	*DE*	*BC*	*DF*	*PS*	*YK*	*NE*	*TJ*	*SZ*	*OU*	*DR*	*JG*
				TY				ST							
E	*HM*	*UN*	*EM*	*RU*	*AS*	*SA*	*PS*	*KM*	*RL*	*HS*	*BR*	*OU*	*NE*	*ET*	*UO*
							ST	OP							
F	*JN*	*NS*	*AR*	*KD*	*EM*	*RE*	*FG*	*PE*	*HM*	*DE*	*AM*	*KA*	*JG*	*EM*	*QJ*
	SS														
G	*PT*	*UD*	*BB*	*DG*	*LM*	*FA*	*PS*	*FJ*	*PT*	*FF*	*BM*	*DC*	*GT*	*SG*	*PS*
	TT						ST		TT						ST
H	*KM*	*TG*	*JG*	*TJ*	*UN*	*BF*	*NJ*	*ON*	*UN*	*NT*					
	OP									TS					

Figure 11–6 (C). First partial reconstruction of plaintext (U).

b. No impossible combinations have occurred to disprove the assumptions relative to the placement of letters in the matrix. However, little insight has been gained into the message text. The next step then is to build on the digraphs recovered, attempting to assume additional values. This can be done easily if the positional limitation placed on one member of a cipher pair by the other member is considered. For example, consider the cipher digraphs *PK KM* located at positions A4 and 5. The positional limitations in this case are such that $\overline{PKc}$ must equal some combination of the row QRSTU of the P1 matrix and columns D J O T Y of the P2 matrix. The location of $\overline{PKc}$ in the ciphertext and the recovered values for $\overline{YTc}$ and $\overline{KMc}$ which flank it, plus self-limitation imposed by impressible combinations, QD, QT, etc., limits the choice. If a plain value of ROp was accepted for $\overline{PKc}$, the word TROOP would be completed as a possibility. Thus *K* can be placed in matrix C2.

c. Another method of determining values is possible, through a study of absolute frequencies considered in the light of possible limitations of location. For example, the ten most frequently used English plaintext digraphs are: EN, RE, ER, NT, TH, ON, IN, TE, AN, and OR. Referring back to the digraphic frequency distribution, the digraphs $\overline{EMc}$, $\overline{PSc}$, $\overline{UNc}$, and $\overline{KMc}$ are the most frequently observed. Again considering the limitation imposed by the location of *Mc* in matrix C2, note that $\overline{EMc}$ can only equal $\overline{\text{INp}}$ or $\overline{\text{ONp}}$. $\overline{\text{IMp}}$ and $\overline{\text{OMp}}$ are also possibilities but are discounted by frequency. This limitation can be seen clearly in the partially reconstructed matrix shown to the right.

	A	B	C	D	E						
P1				J				*(E)*			
				O				*(E)*			*C1*
				T							
				Y							
C2				*M*		L	M	N	O	P	P2

(1) For the moment, that digraph with the highest frequency can be accepted, $\overline{EMc}=\overline{\text{INp}}$. Another method of determining values is through the arbitrary assumption of words conditioned by logic, and then testing the values so determined. For example, consider the opening line of the message with plaintext values previously assumed.

```
                        5                         10                   15
A    UN  ON  YT  PK  KM  JK  ZD  KJ  JS  CR  TG  LW  RA  EM  UP
             YT  RO  OP                              RV      IN
```

(2) Four elements are present in the plaintext sequence above which may lead to the further recovery of values. YT is obviously a word bridge; therefore, the digraphs $\overline{UNc}$ and $\overline{ONc}$ must represent the rest of the word which refers to TROOP. A possible word is ENEMY, and if this is valid there, TROOP probably ends in S. If ENEMY is correct, then $\overline{UNc}=\overline{\text{ENp}}$, and $\overline{ONc}=\overline{\text{EMp}}$. This can be tested against the matrix as shown in figure 11–7.

	A	B	C	D	E		*O*	*U*			
	F	G	H	J	K			*E*			
P1	L	M	N	O	P					*K*	*C1*
	Q	R	S	T	U	*L*	*M*	*N*	*P*		
	V	W	X	Y	Z	*V*	*W*	*X*	*Y*	*Z*	
						A	B	C	D	E	
						F	G	H	J	K	
C2		*K*	*L*	*M*	*N*	L	M	N	O	P	P2
			S	*T*	*U*	Q	R	S	T	U	
	V	*W*	*X*	*Y*	*Z*	V	W	X	Y	Z	

Figure 11–7 (~~C~~). Test of cipher value placement (U).

(3) Note that again the positional limitations of the matrix are such that the assumed values can easily be placed. Further, the one empty space between the *K* and *M* of the *C2* square allows the placement of the *L*. With the additional values, more ciphertext can now be deciphered, figure 11–8.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
A	*UN*	*ON*	*YT*	*PK*	*KM*	*JK*	*ZD*	*KJ*	*JS*	*CR*	*TG*	*LW*	*RA*	*EM*	*YT*
	EN	EM	YT	RO	OP							RV		IN	
B	*RC*	*JC*	*PY*	*DE*	*BC*	*DF*	*HM*	*RM*	*KG*	*ZA*	*PK*	*PS*	*KM*	*UN*	*ON*
			TY											EN	EM
C	*YT*	*UF*	*EU*	*UF*	*UE*	*FA*	*YV*	*DA*	*NT*	*DM*	*UD*	*PE*	*YP*	*PY*	*EM*
	YT		KS				VY		TR						IN
D	*YP*	*RC*	*JC*	*PY*	*DE*	*BC*	*DF*	*PS*	*YK*	*NE*	*TJ*	*SZ*	*OU*	*DR*	*JG*
E	*HM*	*UN*	*EM*	*RU*	*AS*	*SA*	*PS*	*KM*	*RL*	*HS*	*BR*	*OL*	*NE*	*ET*	*UC*
												EP		IS	
F	*JN*	*NS*	*AR*	*KD*	*EM*	*RE*	*FG*	*PE*	*HM*	*DE*	*AM*	*KA*	*JG*	*EM*	*QJ*
		SS			IN									IN	
G	*PT*	*UD*	*BB*	*DG*	*LM*	*FA*	*PS*	*FJ*	*PT*	*FF*	*BM*	*DC*	*GT*	*SG*	*FS*
	TT				TL		ST		TT						ST
H	*KM*	*TG*	*JG*	*TJ*	*UN*	*BF*	*NJ*	*ON*	*UN*	*NT*					
	OP				EN			EM	EN	TS					

Figure 11–8 (C). Second partial reconstruction of plaintext (U).

d. Again, little is revealed by the recovery of the additional value. However, note the idiomorphic pattern of the last seven digraphs.

```
    A B  -   -   -  A B
TJ  UN   BF  NG  ON  UN  NT
    EN           EM  EN  TS
```

(1) By checking this pattern against those listed in appendix D (table D–4) digraphic idiomorphs, it is found that the pattern can represent the word REENFORCEMENTS. Note also the pattern

```
FJ, PT, FF, Row G Column 8, 9, 10 and QJ, PT, UD on Row F–15, G1 and 2.
    TT                                    TT
```

Assuming the placement of the $\overline{-Jc}$ to be correct as shown below, on the basis of the word $\overline{TJc}$=$\overline{\text{REp}}$ above, and assuming that TT in each case represents a doublet rather than a word bridge, additional values can be derived. For example, inspection of the matrix with the *J* inscribed in its assumed position of the C2 square reveals that $\overline{QJc}$ and $\overline{FJc}$ must equal plaintext digraphs that contain, A, B, C, D, or E in the second positions. If *Fc* is placed in the first cell of square C1 $\overline{FJc}$ would equal $\overline{\text{BAp}}$. This in combination with TT, (BATT) would in turn suggest a possible word, BATTALION.

(2) To complete the word, the plaintext digraphs of AL and IO and N– must be supplied. Note that the prior placement of $\overline{FFc}$=$\overline{\text{Alp}}$, and $\overline{BMc}$=$\overline{\text{IOp}}$ which tend to confirm the former assumption, leaving $\overline{DCc}$ to equal $\overline{\text{N–p}}$. By placing the $\overline{D–c}$ on line three of square C1, it is alined properly for the $\overline{\text{N–p}}$ value. However, as there are four possible cells in which it may fit, it cannot be exactly placed. But since it falls on that line, the last cell of the second line must contain a C, the letter immediately preceding the D alphabetically, figure 11–9.

	A	B	C	D	E	(F)	O	U			
	F	G	H	J	K			E	B	(C)	
P1	L	M	N	O	P					K	C1
	Q	R	S	T	U	L	M	N	P	T	
	V	W	X	Y	Z	V	W	X	Y	Z	
		(J)				A	B	C	D	E	
						F	G	H	J	K	
	(F)	K	L	M	N	L	M	N	O	P	P2
C2			S	T	U	Q	R	S	T	U	
	V	W	X	Y	Z	V	W	X	Y	Z	

Figure 11–9 (~~C~~). Insertion of cipher values through analysis (U).

(3) Referring back to the partial sequence shown below and comparing the plaintext values shown with the partially recovered matrix, another possibility is apparent, the word ATTACK. Note the plain equivalent for $\overline{QJc}$ must end with A, B, C, D, or E plain, and that the plain equivalent for $\overline{UDc}$ must begin with A, B, C, D, or E plain, thus placing an A on either side of the double T.

EM QJ PT UD BB
IN TT

(4) Referring back to the sequence $\underset{\text{IN}}{EM}\ QJ\ \underset{\text{TT}}{PT}\ UD$ and considering possible equivalent values, another word is suggested. Note that the plain equivalent for $\overline{QJc}$ must end with A, B, C, D, or E. Similarly, the equivalent for $\overline{UDc}$ must begin with the same letter. Thus an A may be placed to either side of the doublet (ATTA) suggesting ATTACK. Inspection of the matrix shows that the required values of $\overline{\text{ACp}}$ for $\overline{UDc}$ can be made by placing D in cell one, row one of square C2. The *Qc* can then be placed in cell one of either the second or third row, square C1. In order to derive a K plain, the cipher digraph $\overline{BBc}$ must equal $\overline{\text{K–p}}$. Note that the positions of the $\overline{B–c}$ and $\overline{\text{K–p}}$ are such that *Bc* must appear in the last cell of rows one and two of square C2.

e. At this point the analysis can take one or a combination of three courses, all involving techniques previously discussed. The analyst can attempt a recovery of the keyword alphabet used in the C1 and C2 squares. He may continue the process above, patiently reconstructing plaintext by examining patterns, assuming possible words, then checking their possibility against the matrix. The last method is simply one of attempting to decipher additional bits of the message as recovery of the matrix progresses. For example, using the matrix shown in figure 11–10① which incorporates values previously found, the message can now be deciphered in part, figure 11–10②, to read as shown.

	A	B	C	D	E	F	O	U			
	F	G	H	J	K	(Q)		E	B	C	
P1	L	M	N	O	P	(Q)				K	C1
	Q	R	S	T	U	L	M	N	P	T	
	V	W	X	Y	Z	V	W	X	Y	Z	
	D	J			(B)	A	B	C	D	E	
					(B)	F	G	H	J	K	
C2	F	K	(L)	M	N	L	M	N	O	P	P2
			S	T	U	Q	R	S	T	U	
	V	W	X	Y	Z	V	W	X	Y	Z	

Figure 11–10① (~~C~~). Partially recovered four-square matrix (U).

```
         1  2  3  4  5  6  7  8  9 10 11 12-13 14 15

A        UN ON YT PK KM JK ZD KJ JS GR TG LW RA EM YP
         EN EM YT RO OP(MO)VE ME(NT)      RV    IN
B        RC JC PY DE BC DF HM RM KG ZA PK PS KM UN ON
               TY                (ZE)RO ST OP EN EM
C        YT UF EU UF UE FA YV DA MT DM UD PE YP PY EM
         YT AN KS AN          VY    TR    AC       TY IN
D        YP RC JC PY DE BC DF PS YK NE TJ SZ OU DR JG
                  TY             ST WO(TH)RE(EZ)ER(O)
E        HM UN EM RU AS SA PS KM RL HS BR OU NE ET UO
            EN IN             ST OP          ER    IS
F        JN NS AR KD EM RE FG PE HM DE AM KA JG EM QJ
                                                    G
            SS    LE IN                          IN MA
G        PT UD BB DG LM FA PS FJ PT FF BM DC GT SG PS
         TT AC KI(NA)TL(EA)ST BA TT AL IO             ST
H        KM TG JG TJ UN BF NJ ON UN NT
         OP(SE ND)RE EN FO RC EM EN TS
```

Figure 11-10② (*C*). *Partially recovered plaintext* (*U*).

As several more words are now obvious (shown in parentheses) additional values could be recovered quickly using the techniques previously shown, the solution becoming a mechanical process.

Section II. (~~C~~) ANALYSIS OF TWO-SQUARE CIPHERS

11–4. (~~C~~) General

a. The initial identification and subsequent analysis of two-square systems is contingent upon the recognition of their one primary characteristic, that 20 percent of all cipher digraphs are in fact transparencies, i.e. the same as the underlying plaintext. In the case of vertical two-square systems, these transparencies will be identical with the plaintext they represent; while in the case of a horizontal two-square, the transparencies will be reversed. Thus, if the examination of one or more cryptograms results in the consistent observation of digraphs which form good plaintext digraphs they may be assumed to be the result of encipherment by a two-square cipher system.

b. The preliminary steps covered in the preceding section, that is, the assumption and rejection of the system being monographic and uniliteral encipherment, are followed as a matter of course. After these rejections, the ciphertext is examined closely for those characteristics given for digraphic cipher systems. The normal digraphic tests are conducted as required in order to aid in ascertaining whether the system is digraphic. Once this has been accomplished, the analyst is again faced with determining which specific system was used.

c. It is usually possible to make a final determination as to whether a cipher represents a two-square horizontal, or a two-square vertical, by a visual examination of the text. Sometimes the structure of the system is such that skeletons of words or whole phrases are readily apparent. However, this is the exception to the rule. Without some kind of a formal test, it is difficult to specify what constitutes a "good amount" of plaintext digraphs for identification. Such a test is illustrated in the succeeding paragraph.

11–5. (~~C~~) Two-Square Test

a. The test to be described is based upon an evaluation of the observed frequency of a given ciphertext digraph in terms of its expected frequency as a plaintext digraph. Any such correlation as might exist between a given plaintext digraph and its occurrence as a cipher digraph produced by a four-square, a Playfair, or a large-table system, is accidental. But in the case of a two-square system, the correlation is the result of the mechanics of the enciphering system. Thus, if a ciphertext digraph exhibits only the random expected occurrence, considered as direct and reversed transparencies, then that ciphertext may be assumed to be the product of a digraphic system other than a two-square. If however, the number of occurrences exceeds that random expected value, the ciphertext may be the product of a two-square system. Of course the mode, as direct or reversed transparencies, in which this greater value occurs, indicates the particular system used.

b. To illustrate the procedures involved in this text, and the techniques of subsequent analysis, the following ciphertext, figure 11–11, prepared for study, will be used.

```
         1  2  3  4  5  6  7  8  9 10 11 12 13 14 15

A        BO DL EM QB EP EL QH NO RQ DO AQ GL IL MU OI
B        PH TA NB TB AM MA OI DC SE ML PC GB NI AM TA
C        NN BF GE HL CK TC SE PH RI OD HL UC OI IH HC
D        DE FC PP EM ME YA IP EV RA HM QC TI SE SN QB
E        GR SP RB SS AB LF HL OR AH OP AM QN HL PO KM
F        OS AH PH SI NB TB AM MA OI QH NE NO NN ES MI
G        SP BB EM LN TA SE SN YD RK EB NG AM NN AM DE
h        NO HL OR AH OP AM QN AM IP EV RA HM QC TI SE
I        SN HL PO QB LH RI ME SY EB SS HC DF OZ TA NN
J        BF AM KQ SH QN NO ER UQ OI UT
```

Figure 11–11 (*C*). *Ciphertext for analysis* (*U*).

(1) Preliminary to a study of the digraphs as "direct" or reversed transparencies, the frequency of the digraphs is tabulated using the normal digraphic frequency matrix shown in figure 11–12.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
A		—						≡					≣≣				—										15
B		—			—	—									—												4
C											—																1
D			—		≡							—			—												6
E		=										—	≡			—		—	—			=					11
F			—																								1
G		—			—							—						—									4
H			=									≢	=														10
I								—				—				=											4
J																											0
K													—				—										2
L						—		—						—													3
M	=				=					—		—									—						7
N		=			—					=				≣	≣												13
O				—						≢						=		=	—							—	1
P			—				=								=	—											6
Q	≡	=					=							≡													10
R	—	—						—	=		—						—										7
S					≣			—	—					≡		=			=						—		15
T	≣	=	—						=																		9
U			—														—			—							3
V																											-
W																											-
X																											-
Y	—			—																							2
Z																											-
	8	13	9	2	13	2	0	11	5	8	2	11	16	11	8	8	4	4	4	1	1	2	0	0	1	1	

Figure 11–12 (*U*). *Digraphic frequency matrix* (*U*).

(2) Once the digraphs have been tabulated, the individual digraphs may be listed in alphabetic order and tested for their probability as direct or reversed transparencies. The format of the test is shown in figure 11–13. Column identity is:

Column 1 Ciphertext digraph
Column 2 Frequency of digraph in text from digraphic frequency distribution
Column 3 Logarithm of expected frequency of digraph as direct plaintext
Column 4 Product of Column 2 x 3
Column 5 Logarithm of expected frequency of digraph as reversed plaintext
Column 6 Product of Column 2 x 5

(1)	(2)	(3)	(4)	(5)	(6)
AB	1	.45	.45	.38	.38
AH	3	.25	.75	.67	2.01
AM	1	.61	.61	.78	.78
AQ	1	0	0	0	0
BB	1	0	0	0	0
BE	1	.66	.66	.38	.38
BF	1	. 0	. 0	. 0	. 0
BO	1	.38	.38	.38	.38
CK	1	.38	.38	.13	.13
DC	1	.38	.38	.13	.13
DE	3	.77	2.31	.88	2.64
DL	1	.33	.33	.53	.53
DO	1	.63	.63	.58	.58
EB	2	.38	.76	.66	1.32
EL	1	.74	.74	.79	.79
EM	3	.61	1.83	.72	2.16
EP	1	.67	.67	.70	.70
ER	1	.94	.94	.96	.96
ES	1	.86	.86	.84	.84
EV	2	.67	1.34	.87	1.74
FC	1	.25	.25	.13	.13
GB	1	. 0	. 0	. 0	. 0
GE	1	.61	.61	.38	.38
GL	1	.25	.25	.13	.13
GR	1	.42	.42	.48	.48
HC	2	.33	.66	.61	1.22
HL	6	.13	.78	.13	.78
HM	2	.25	.50	.13	.26
IH	1	. 0	. 0	.77	.77
IL	1	.70	.70	.67	.67
IP	2	.48	.96	.45	.90
KM	1	. 0	. 0	. 0	. 0
KQ	1	. 0	. 0	. 0	. 0
LF	1	.33	.33	.25	.25
LH	1	.13	.13	.13	.13
LN	1	.13	.13	.42	.42
MA	2	.78	1.56	.61	1.22
ME	2	.72	1.44	.61	1.22
MI	1	. 0	. 0	. 0	. 0
ML	1	. 0	. 0	.25	.25
MU	1	.25	.25	.42	.42
NB	2	.25	.50	.0	.0
NE	1	.87	.87	.99	.99
NJ	2	.13	.26	. 0	. 0
NN	4	.51	2.04	.51	2.04
NO	4	.66	2.64	.92	3.68
OE	1	.33	.33	.58	.58
OI	5	.13	.65	.25	1.25
OP	2	.72	1.44	.64	1.28
OR	2	.89	1.78	.74	1.48
OS	1	.61	.61	.62	.62
OZ	1	. 0	. 0	. 0	. 0
PC	1	.13	.13	. 0	. 0
PH	2	.33	.66	.13	.26
PO	2	.64	1.28	.72	1.44
PP	1	.56	.56	.56	.56
QB	3	. 0	. 0	. 0	. 0
QC	2	. 0	. 0	. 0	. 0
QH	2	. 0	. 0	.13	.26
QM	3	.13	.39	. 0	. 0
RA	1	.80	.80	.82	.82
RB	1	.25	.25	.25	.25
RH	1	.33	.33	.64	.64
RI	2	.75	1.50	.73	1.46
RK	1	.13	.13	. 0	. 0
RQ	1	. 0	. 0	.13	.13
SE	5	.84	4.20	.86	4.30
SH	1	.72	.72	.38	.38
SI	1	.77	.77	.78	.78
SN	3	.38	1.14	.71	2.13
SP	2	.55	1.10	.45	.90
SS	2	.67	1.34	.67	1.34
SX	1	. 0	. 0	.13	.13
TA	4	.74	2.96	.83	3.32
TB	2	.33	.66	.13	.26
TC	1	.45	.45	.61	.61
TI	2	.82	1.64	.73	1.46
UC	1	.33	.33	.38	.38
YA	1	.45	.45	.58	.58
YD	1	.53	.53	.13	.13
			56.42		60.52

Figure 11-13 (*U*). *Test for probability of transparencies* (*U*).

(3) As the total value of all digraphs as reversed transparencies (the sum of column six) is greater than that for the digraphs as direct transparencies (column five) it can be assumed then that the system involved is a horizontal two-square. If the value of direct transparencies had been greater, the assumption would be for a vertical two-square system. Under normal circumstances, a horizontal two-square produces N x 0.3388 reversed transparencies, while a vertical two-square produces N x .3610 direct transparencies. (N in both cases refers to the number of digraphs.) In this case, the theoretical value of expected reversed transparencies is 4.9126 (145 x .3388) which compares favorably with 4.15, the value observed as difference between columns five and six.

11-6. ~~(C)~~ Analysis of Two-Square Systems

a. The solution of both the vertical and horizontal two-square systems involves the same general principles and techniques. Only a slight modification in the reconstruction matrix is required to orient it vertically or horizontally as the case may require. The first step in either case, is to set up the reconstruction matrix, and to examine the text closely for significant characteristics. Where two-square systems are dealt with, an obvious quick entry into the cipher is by way of the transparencies. If entry can be made by this route, other more laborious and time-consuming methods, similar to those illustrated in the case of a four-square system, may be avoided. With this in mind, the text is inspected for possible transparencies.

(1) The following possible transparencies (fig. 11-14①) are noted. Although at first glance they appear unlikely, consider what occurs when one or more digraphs of each are reversed, as in figure 11-14②.

PH TA

PH SI

HL PO

EM ME YA

NO ER UQ OI UT

Figure 11-14① (C). Possible transparencies from cipher-text (U).

PH AT	THAT
PH IS	THIS
HL OP	STOP
EM EM YA	ENEMY
ON REQU OI UT	ON REQUEST

Figure 11-14② ~~(C)~~. Possible transparencies reversed (U).

The rearrangement of each digraph makes obvious a possible word, shown to the right above. Using these assumed values, a reconstruction matrix can be set up.

(2) The matrix used should be of sufficient size in height and width to allow the free movement of the letters and to avoid the establishment of false relationships. A dividing line, horizontal or vertical as required, will provide for the separation of the letters. The placement of the letters within the matrix can be determined by their use, i.e. in a horizontal two-square transparency they will lie on the same row; in a vertical two-square transparency they will lie in the same column. Thus the letters *T* and *A* must lie in one row, and *I* and *S* must lie in another row; and as they appear as reversed transparencies, *A* and *I* would appear in square P1 C2, and *T* and *S* in P2 C1. All values are checked and inscribed in a working matrix and appear as shown in figure 11-15.

P1 *C2* | P2 *C1*

					A	T						
				I			S					
			E					M				
		O							N	P		
	Q										U	
R												E

Figure 11-15 ~~(C)~~. Preliminary reconstruction matrix (U).

(3) With some values assumed in the rows of the matrix, the next step is to attempt rearrangement to obtain columnar order. To illustrate, $\overline{HL}\ \overline{PO}$ is assumed to be the cipher value of $\overline{ST}\ \overline{OP}$; thus, encipherment of the first plaintext digraph must have occurred in one of the following positions; figure 11-16.

P1 *S*	*C1* *H*
C2 *L*	P2 *T*

or

C2 *L*	P2 *T*
P1 *S*	*C1* *H*

Figure 11-16 ~~(C)~~. Analysis of cipher-plain value location (U).

Either method of encipherment demonstrates that *T* and *H* lie in the same column of square P2 C1, and *S* and *L* in P1 C2. As both *T* and *S* have been placed, *H* and *L* can be placed in their respective rows, figure 11-17. Note that care must be exercised not to place a letter in the same row or column with another unless some evidence exists to support this placement.

P1-*C2* P2-*C1*

L						A	T						
					I			S					
				E					M				
			O							N	P		
		Q										U	
	R												E
S							H						

Figure 11–17 (~~C~~). First expansion of reconstruction matrix (U).

(4) With *T* and *H* in the same row, the digraph pairs $\overline{PHc}$, $\overline{TAc}$, and $\overline{PHc}$ $\overline{SIc}$ can be checked. Assuming $\overline{PHc}$ to be $\overline{\mathrm{TH}}$p, encipherment is possible by:

P1–C2	P2–C1		P1–C2	P2–C1
T	*P*		*H*	*H*
H	*H*	or	*T*	*P*

In either case it is found that *T* and *P* and *H* and *H* appear in the same rows; that *T* and *H* and *H* and *P* lie in the same column. By incorporating this relationship with that previously established, the matrix will now appear as shown in figure 11–18.

P1-*C2* P2-*C1*

L							A	T					
						I			S				
					E					M			
	T			O				P			N		
			Q									U	
		R											E
S	H							H					

Figure 11–18 (~~C~~). Second exnansion of reconstruction matrix (U).

(5) The assumed ENEMY for the cipher digraphs $\overline{EM}$ $\overline{ME}$ $\overline{YA}$ provides a further clue. Note that $\overline{EMc}$, *Ec*, and *Mc* lie at opposite corners of a rectangle. Thus Ep and Mp must lie at the diagonally opposite corners. Mp in P1–C2 represents a new placement falling below *E*. *Ec* of P2–C1, however, has been previously placed, thus when it is moved up to its proper position to the opposite diagonal corner, *R* or P1–C2 of the same row must also be brought up. The matrix, ıearranged to show this relationship is shown in figure 11–19

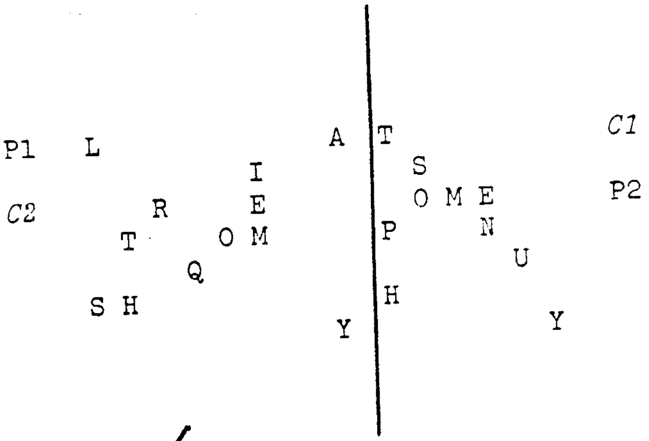


Figure 11–19 (~~C~~). Rearrangement and expansion of reconstruction matrix (U).

b. Further analysis of the ciphertext follows essentially the same route, with additional values being provided by the letters already inscribed in the matrix. For example, using the matrix above it is possible to find the following sequence of partial plaintext in the message:

Position E7–13	*HL*	*OR*	*AH*	*OP*	*AM*	*QN*	*HL*	*PO*
	ST	RO	(NG)	PO	(IN)	(TS)	ST	OP
D7–13	*IP*	*EV*	*RA*	*HM*	*QC*	*TI*	*SE*	*SN*
				-P	(OS)	(IT)	IO	(NS)
G1–7		*SP*	*BB*	*EM*	*LN*	*TA*	*SE*	*SN*
				EN		AT	IO	(NS)

(1) In the first sequence above, a possible word in STRONG POINT is easily visible. In the second and third cases, no word is apparent, except possibly POSITION in the second. However, note the similarity in the endings. If $\overline{TIc}$ and $\overline{SNc}$ are reversed transparencies, the endings produced will be similar "*TIONS*." The possibility of this being correct can be checked by referring to the preceding

tabulation of expected occurrences of the cipher digraph and appendix D (table D-4). Here we find the expected occurrences to be:

$\overline{TIc}$	82	$\overline{SNc}$	38
$\overline{ITc}$	73	$\overline{NSc}$	71

(2) Obviously the results are inconclusive in the case of the reversal of $\overline{TIc}$; however, when considered with $\overline{\text{IOp}}$ and $\overline{\text{NSp}}$, the $\overline{ITc}$ combination seems to outweigh its negative value. Moreover, an additional test, which is always to be preferred, is to try it in the system. Using all values assumed in the first case and those above, the matrix now can be expanded as illustrated in figure 11-20.

P1	1	L				I	A	T						A	P2
	2		N						S						
C2	3			R		E			O	M	E				C1
	4		T		O	M	Q	P			N	U			
	5	S	H					H						G	
	6						Y						Y		

Figure 11-20 (C). Third expansion of reconstruction matrix (U).

c. As analysis continues, the process becomes more and more mechanical. The only problem likely to be encountered is in reducing the matrix to its original dimensions, the danger being that false relationships may be established by an arbitrary telescoping. In respect to reducing the size of the matrix, it is possible to shift rows and columns to put the matrix in its correct order, but in so doing the individual letters must not be disturbed. For this purpose a partially recovered matrix as above usually exhibits sufficient characteristics to permit this. For example, assuming that a mixed alphabet of some type is used in each square, an inspection of the letters of the matrix allows the following observation.

(1) Row three R - E - / - O M E contains letters so far out of sequence as to suggest a keyword, these letters possibly being part of the keyword. Thus it may be the first row.

(2) Row one L - - - I A / T - - - - - A exhibits some alphabeticity if the P1-C2 values are A I L. Further, since the A appears in this row, as well as I and L, it may be possible to represent that part of the alphabet immediately following the keyword, or perhaps part of the keyword. In either case it may be the second row.

(3) Row six, containing the Y in both squares, can be the last row. Row four, if the T and U are not part of the keyword, must precede row six to maintain alphabeticity. Row 5, since it contains S and H in the first square, must represent a portion of the keyword. On the basis of the foregoing assumptions the matrix can now be drawn up as in figure 11-21.

P1			R		E			O	M	E			C1
	L				I	A	T					A	
C2	S	H					H					G	P2
		T		O	M	Q	P			N	U		
		N						S					
						Y					Y		

Figure 11-21 (C). Initial construction of two-square matrix (U).

d. The same shifting in respect to columns is possible. Again, however, individual letters cannot be disturbed. In rows three and four of square P2-C1 the letters H - - - - - G and P - - N seem to be reversed in respect to their normal alphabetic order. If these letters are juxtaposed according to their normal sequence (considering the O to be used in the keyword, and maintaining columnar order), this square would appear as in figure 11-22.

P1-C2								E		M		O			P2-C1
									A		T				
									G		H				
								N			P		U		
												S			
														Y	

Figure 11-22 (C). Rearrangement of square P2-C1 (U).

(1) A similar inspection of the square P1-C2 shows less in the way of alphabetic patterns that can be directly interpreted. However, consideration of other factors can provide assistance. Having assumed a keyword is being used, it can further be assumed that the letters VWXYZ probably are not used; thus they are the last line. Y then would appear in the second column and consequently so would A and Q. They begin the same column. Note that in row three, O and M are reversed. Thus the square can be put in the order shown in figure 11-23.

P1-*C2* P2-*C1*

R			E										
	L		I		A								
	S	H											
			M	O	Q	O							
		N											
		T											
					Y	(Z)							

Figure 11–23 (~~C~~). *Rearrangement of square P1–C2* (*U*).

(2) The two squares in matrix form appear in figure 11–24.

P1																P2
	R			E				E			M		O			
C2		L		I		A			A			T				*C1*
		S	H							G		H				
			T	M	O	Q		N				P		U		
			N										S			
						Y	(Z)								Y	

Figure 11–24 (~~C~~). *Partially recovered horizontal two-square matrix* (*U*).

e. Matrix reorganization and recovery can be continued or the analysis of the ciphertext can be resumed. Sometimes recovery aids in the final solution as it provides a true framework for the insertion of additional values as they are found, thus avoiding the possibility of establishing false relationship. On the other hand, the paucity of values recovered in an intitial entry and the use of a random alphabet may prevent matrix recovery until the message itself is deciphered. In any case, both matrix recovery and analysis of the text follows the same techniques just explained.

Section III. (~~C~~) ANALYSIS OF PLAYFAIR CIPHERS

11–7. (~~C~~) Rules of Encipherment

a. In the analysis of Playfair cipher messages, the reconstruction of the enciphering matrix and the recovery of the plaintext are simultaneous and inseparable operations. This is due to the cryptographic nature of the system where both the cipher and plain values occur in the same matrix, being differentiated only by the rules of encipherment, and this differently in each specific case of digraphic encipherment. The rules of encipherment dictate the possible manner and combinations of placement of plaintext equivalencies in a given situation. Further, their specific placement determines their equivalencies in other combinations. Thus the two processes should be conducted as one.

b. The relationship of the rules of encipherment upon the plain to cipher equivalencies, and their effect upon establishing the same values in the process of recovery of the ciphertext is illustrated using the matrix shown in figure 11–25.

A	B	C	D	E
F	G	H	I	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Figure 11–25 (*U*). *Example Playfair square* (*U*).

(1) Where substitution involves letters at opposite ends of a rectangle, the following relationships exist as shown in figure 11–26.

$\overline{\text{AZp}} = \overline{EVc}$

RECIPROCAL $\overline{\text{EVp}} = \overline{AZc}$

$\overline{\text{ZAp}} = \overline{VEc}$

$\overline{\text{VEp}} = \overline{ZAc}$

REVERSIBLE $\overline{\text{AZp}} = \overline{EVc}$

$\overline{\text{ZAp}} = \overline{VEc}$

$\overline{\text{EVp}} = \overline{AZc}$

$\overline{\text{VEp}} = \overline{ZAc}$

$\overline{\text{GOp}} = \overline{IMc}$

$\overline{\text{OGp}} = \overline{MIc}$

$\overline{\text{IMp}} = \overline{GOc}$

$\overline{\text{MIp}} = \overline{OGc}$

Figure 11–26 (C). Reciprocal reversible relationships (U).

If the letters are assigned numbers as the possible combination shown here:

12=34
$\overline{\text{AZp}}=\overline{EVC}$

They may be expressed as an equation. Thus:

Reciprocal	12=34	Reversible
	21=43	
Reciprocal	34=12	Reversible
	43=21	

(2) Where substitution involves letters of the same row or column these relationships may occur:

12 34
$\overline{\text{BCp}}=\overline{CDc}$
$\overline{\text{CBp}}=\overline{DCc}$
21 43

Note that in this case, only reversibility occurs and not reciprocity. That is:

$\overline{CDc}$ does not equal $\overline{\text{BCp}}$ nor does
$\overline{DCc}$ equal $\overline{\text{CBp}}$

(3) From the above it can be seen that in all cases, column, row, or rectangle (where 12=34), 21=43. But only when 1 and 2 form appropriate diagonal corners of a rectangle does 34=12 and 43=21.

c. The position that a letter occupies in the Playfair matrix coupled with the method of encipherment determines its limitation in combination with other letters, and consequently its equivalent value. Any given letter can be represented by eight other letters, the four occupying the same row and the four occupying the same column.

(1) Thus, where encipherment occurs along a row or column, a given letter can be combined with only eight other letters, which can be further limited to four if the direction of encipherment is known.

(2) In the case of encipherment involving a rectangle, the same letter can be combined with 16 other letters, 8 of its own row and column plus the 8 of the other letter forming the diagonally opposite corner. Where encipherment is along a row or column the letter may be combined with 8 other letters, 4 for the row and 4 for the column. Of the 24 possible equations that can be formed by a given letter, as either the initial or final letters of a digraph, five will indicate a corresponding repetition of a given plaintext letter.

d. The effect of the above observation is such to allow the formulation of certain rules in respect to the identification of digraphs produced by a Playfair cipher. These rules are:

(1) *Rule 1.* In all cases if 1.2=3.4
then 2.1=4.3
In case of rectangle if 1.2=3.4
then 2.1=4.3
then 3.4=1.2
then 4.3=2.1

(2) *Rule 2.* Where 1.2p=3.4c, for example $\overline{\text{ENp}}=\overline{CPc}$, there is a minimum probability of one in five that any other cipher digraph beginning with *Cc* has Ep as the initial letter of its corresponding plain digraph. Also, any cipher digraph which ends in *Pc* has the same probability of Np as the last letter of the corresponding plain digraph.

(3) *Rule 3.* In those equations where 1.2p=3.4c, 1 and 3 can never be identical, nor can 2 and 4 ever be identical.

(4) *Rule 4.* In those equations 1.2p=3.4c where 2 and 3 are identical, the letters are all in the same row or column, and in the relative order 1–2–4, 2 and 3 in this case being synonymous. For example, in the matrix above, $\overline{\text{BCp}}=\overline{CDc}$. There are five cyclic permutations which will produce the proper sequence. They are:

```
B C D - -
- B C D -
- - B C D
D   - - B C
C D - - B
```

(5) *Rule 5.* In an equation where 1.2p=3.4c and 1 and 4 are identical, the letters are again in the row or column but in the order 2–4–3. For example in the matrix above $\overline{\text{DCp}}=\overline{\textit{EDc}}$; thus the order is CDE. The five possible cyclic permutations of this absolute order are:

C D E - -
D E - - C
E - - C D
- - C D E
- C D E -

e. The importance of these rules are that they will allow the formulation of an assumption concerning the arrangement of values within the cipher matrix and the elimination of equivalencies in the cryptogram.

Example:

(1) Rule 1, where 1.2=3.4 and 2.1=4.3, gives rise to digraphic idiomorphs which may be used in the assumption of probable words. Thus the word ATTACK can be enciphered by the matrix in figure 11–25:

$$\begin{array}{lll} & \overline{\text{AB}}\ \overline{\text{BA}} & \\ \text{P} & \text{AT TA CK} & \\ \text{C} & \overline{\textit{DQ}}\ \overline{\textit{QD}}\ \overline{\textit{EH}} & \overline{\text{ATp}}=\overline{\textit{DQc}} \\ & & \overline{\text{TAp}}=\overline{\textit{QDc}} \end{array}$$

(2) Rule 2, where the probability of similarity exists, indicates that once each common combination as ERp, ORp, and ENp have been assumed or determined, the rules can be used in discovering additional digraphs and partial words.

(3) Rule 3, where 1 and 3, and 2 and 4 can never be identical, aids in the elimination of possibilities when a specific message is being studied.

(4) Rules 4 and 5 permit the establishment of values and their correct sequencing in the recovery of the matrix.

11-8. (C) Analysis of Playfair Cipher

a. To illustrate the steps and process involved in the solution of a Playfair cipher, the following example will be used. Assume that the analyst has previously identified the message as the product of a Playfair cipher on the basis that it contains an even number of letters, that repeats and spacings are multiples of two, that no doublets occur, that several letters are missing, and finally the discovery of what appears to be Playfair idiomorphs in the repeated sequence. Moreover, for the purpose of this illustration, it is assumed that the analyst has divided the plaintext into its digraphic units, prepared a frequency distribution, and tabulated significant repeated sequences, figure 11–27① and 11–27②. With the preliminary studies completed, analysis may commence.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
A	EC	OG	EC	UR	RO	VQ	AD	ZB	FG	MG	AW	CE	WO	DY	AO
B	EQ	QM	CT	MG	KN	RA	AR	IQ	MG	RB	IR	IK	NM	KB	CY
C	AR	IQ	MG	YF	UY	UY	BT	LG	UP	EP	ME	FK	BR	AC	KR
D	CY	AR	AH	RA	WA	EM	CI	EC	AW	CE	SW	CE	QE	PO	ME
E	EM	VO	ME	LD	CU	QA	PQ	RE	LQ	UY	GT	TV	PB	XC	QP
F	EA	YF	UY	BN	GO	NC	LD	PK	RF	LZ	CI	DT	KR	EA	QI
G	GT	TV	EC	LF	OR	LR	QA	PQ	AR	BD	LG	QL	OZ	QI	BN
H	CF	TG	FK	DN	CR	FK	GR	PZ	ZA	AE	GF	DQ	RG	CY	EQ
I	CW	QU	QF	AL	EC	BS	CI	EM	LU	PC					

Figure 11–27① (C). Ciphertext prepared for analysis (U).

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A			—		—			—				—			=			≣					=			
B				—										=				—	—	—						
C					≡	—			≡											—			—		≡	
D														—			—			—					—	
E	—		≢										≡			—	=									
F							—				≡															
G						—									—			—		=	—					
H																										
I											—						=	—								
J																										
K		—												—												
L				=		—	—										—	—			—					
M					≡	=	≡																			
N			—										—													
O							—											—								—
P		—	—							—					—		—									—
Q	=				—	—			=			—	—			—					—					
R	=	—			—	—	—								—											
S																							—			
T																						=				
U							—									—		—							≣	
V															—		—									
W	—														—											
X			—																							
Y						=																				
Z	—	—																								

Figure 11–27② (~~C~~). *Digraphic frequency distribution Playfair cipher* (*U*).

b. A close examination of the text reveals the following repeated sequences:

Line B5	*KN RA AR IQ MG*
B14–C3	*KB CY AR IQ MG*
C15–D4	*KR CY AR AH RA*
D14–E3	*PO ME EM VO ME*
E6–G8	*QA PQ*
E11–G1	*GT TV*

(1). The first sequence, with its ABBA pattern suggests the word BATTALION digraphically divided as:

+B AT TA LI ON
KN RA AR IQ MG

If these values are correct, the second listed repeats may also be the same words, enciphered with an X between the TT doublet, divided as:

BA TX TA LI ON
KB CY AR IQ MG

By using the values assumed in the first two sequences, the third sequence equals:

TX TA AT
KR CY AR AH AR

It is obvious that this sequence can hardly be "BATTALION," but another common word in which the TT doublet occurs is "ATTACK." If this is the correct word for the sequence, the $\overline{\text{CKp}}=\overline{AHc}$ and $\overline{\text{-Ap}}=\overline{KRc}$.

(2) The repeats *QA PQ*, and *GT TV* are suggestive of the word STOP. However, at this point, the assignment of plaintext values to either would be sheer guess work; therefore, for the moment they are bypassed. The values that have been assumed may now be inserted in the text and again studied for further exploitable patterns. On line B, immediately preceding the assumed word "BATTALION," the digraph $\overline{MGc}$ is noted, which equals $\overline{\text{ONp}}$. Aware that "BATTALION" is often preceded by a number, the possible $\overline{\text{ONp}}$ is suggestive of SECOND. The acceptance of this would permit the expansion of the sequenee to:

```
QM CT MG KN RA AR IQ MG
-S EC ON DB AT TA LI ON
```

If BATTALION in the first instance is preceded by a number, it is very likely to be the case in the second instance as well. From the fact that there normally are only three battalions to a regiment, the analyst may infer that either "FIRST" or "THIRD" probably is the second number. In dealing with numbers, one tends to keep them in order. Therefore, the word THIRD would be assumed. This sequence then can be expanded to:

```
IR IK NM KB CY AR IQ MG
-T HI RD BA TX TA LI ON
```

Thus the remaining digraphs *RB IR*, may equate to the word "AND," as

```
RB IR
AN DT
```

c. Once a few values have been tentatively established, the analyst can, using the rules of encipherment discussed in the previous chapter, expand the values recovered. First a tabulation of all assumed values is made and, using rule 1 where 1.2=3.4 then 2.1=4.3, the reversals are shown in figure 11-28.

Assumed Values	Rule 1 Reversal
$\overline{\text{-Sp}} = \overline{QMc}$	$\overline{\text{ESp}} = \overline{MQc}$
$\overline{\text{ECp}} = \overline{CTc}$	$\overline{\text{CEp}} = \overline{TCc}$
$\overline{\text{ONp}} = \overline{MGc}$	$\overline{\text{NOp}} = \overline{GMc}$
$\overline{\text{DBp}} = \overline{KNc}$	$\overline{\text{BDp}} = \overline{NKc}$
$\overline{\text{ATp}} = \overline{RAc}$	$\overline{\text{TAp}} = \overline{ARc}$
$\overline{\text{LIp}} = \overline{IQc}$	$\overline{\text{ILp}} = \overline{QIc}$
$\overline{\text{ANp}} = \overline{RBc}$	$\overline{\text{NAp}} = \overline{BRc}$
$\overline{\text{DTp}} = \overline{IRc}$	$\overline{\text{TDp}} = \overline{RIc}$
$\overline{\text{HIp}} = \overline{IKc}$	$\overline{\text{IHp}} = \overline{KIc}$
$\overline{\text{RDp}} = \overline{NMc}$	$\overline{\text{DRp}} = \overline{MNc}$
$\overline{\text{BAp}} = \overline{KBc}$	$\overline{\text{ABp}} = \overline{BKc}$
$\overline{\text{TXp}} = \overline{CYc}$	$\overline{\text{XTp}} = \overline{YCc}$
$\overline{\text{-Ap}} = \overline{KRc}$	$\overline{\text{A-p}} = \overline{RKc}$
$\overline{\text{CKp}} = \overline{AHc}$	$\overline{\text{KCp}} = \overline{HAc}$

Figure 11-28 (C). Use of rule 1 to determine plaintext values (U).

(1) The next step is to apply rules 4 and 5 to the above equations in order to recover possible row and column sequences of the enciphering matrix. Both lists are examined for equation of 1.2=3.4 where 2 and 3, and 1 and 4 are identical. The following equations are noted.

$\overline{\text{ECp}}=\overline{CTc}$ $\qquad$ $\overline{\text{BAp}}=\overline{KBc}$

$\overline{\text{TAp}}=\overline{ARc}$

$\overline{\text{LIp}}=\overline{IQc}$

$\overline{\text{HIp}}=\overline{IKc}$

Rule 4 states that in the equation 1.2=3.4 where 2 and 3 are identical, the relative order from left to right or top to bottom is 1–2–4. Thus the equations shown become:

$$\overline{\text{ECp}}+\overline{CTc}=\text{ECT}$$
$$\overline{\text{TAp}}+\overline{ARc}=\text{TAR}$$
$$\overline{\text{LIp}}+\overline{IQc}=\text{LIQ}$$
$$\overline{\text{HIp}}+\overline{IKc}=\text{HIK}$$

Rule 5 states that in an equation 1.2=3.4 where 1 and 4 are identical, the relative order is 2–4–3 from left to right or top to bottom. Then the equation $\overline{\text{BAp}}=\overline{KBc}$ becomes ABK.

(2) Note that only the assumed values are used. The values obtained by rule 1 could have been used equally as much. However, the results would have only been the reversal of what has been established. As a rule, in the beginning stages it is not wise to mix the two, as it tends to introduce too many possibilities of deriving the same value. Moreover, note that only the absolute order of a sequence is being used, not all of its permutations. At this stage, their introduction would again only result in confusion. As analysis continues, and if the accepted absolute permutation is not consistent with the matrix dimensions and enciphering process observed, the other permutations can be used.

(3) Examination of the sequences, noting their common letters, indicates that they can be chained, figure 11–29, to form a pseudo-matrix.

ECT	*E*	*C*	*T*	*A*	*R*
TAR			*L*	*B*	
LIQ		*H*	*I*	*K*	
HIK			*Q*		
ABK					

or

E			
C		*H*	
T	*L*	*I*	*Q*
A	*B*	*K*	
R			

Figure 11–29 (~~C~~). *Construction of preliminary matrix* (*U*).

Note that in each case the values that can be obtained are the same and that the sequential order of each sequence is maintained. Only their arrangement differs.

(4) Using the pseudo-matrix the analyst can now scan the list of assumed values above in figure 11–27 and add values to the pseudo-matrix, where required, to complete an equation. For example $\overline{\text{ANp}}=\overline{RBc}$ is noted, as well as its reversal $\overline{\text{NAp}}=\overline{BRc}$. With this the N can be placed as shown below. By continuing the same process, the equations $\overline{\text{DTp}}=\overline{IRc}$, $\overline{\text{DBp}}=\overline{KNc}$, and $\overline{\text{RDp}}=\overline{NMc}$ are located in the list and, once fitted, permit the expansion of the matrix as shown in figure 11–30.

E	*C*	*T*	*A*	*R*
		L	*B*	*N*
	H	*I*	*K*	*D*
		Q		*M*
	X	*Y*		

Figure 11–30 (~~C~~). *First expansion of matrix* (*U*).

d. With a partially recovered matrix which will logically produce all the assumed values listed, it is now possible to return to the text and attempt to break out further portions. With so few values it is not expected to produce any degree of intelligibility other than bits and parts. These again will be the basis of further assumptions and consequent expansion of the matrix. Following the partial decipherment of the message, the following significant passages are observed.

```
C-15  KR CY AR AH RA WA EM CI EC AW CE SW CE QE
       A TX TA CK AT    R– TH RE    ER    ER –T
F-13  KR EA QI GT TV EC LF OR LR QA PQ
      –A RT IL       RE       NT ST
G-9   AR BD LG QL OZ QI BN
      TA NK    IT    IL LB
```

(1) In each of the passages above, sufficient plaintext values are at hand to lend substance to good assumptions. The first phrase is obviously a time reference relating to the time of the planned attack. The plaintext bit THRE can only be a part of the word "THREE." The digraph $\overline{AWc}$ preceding $\overline{\text{ERp}}$ is likely to be EZ to form ZERO. Logically expanding, the phrase shown below can be developed "ATTACK AT ZERO THREE ZERO ZERO." With this phrase, the following equations, figure 11–31, can be developed and the matrix expanded as shown.

$\overline{ZEp} = \overline{WAc}$

$\overline{ROp} = \overline{EMc}$

$\overline{THp} = \overline{CIc}$

$\overline{EZp} = \overline{AWc}$

$\overline{OZp} = \overline{SWc}$

$\overline{OTp} = \overline{QEc}$

E	C	T	A	R
		L	B	N
	H	I	K	D
O		Q	S	M
W	X	Y	Z	

Figure 11–31 (C). Second expansion of matrix (U).

(2) The second phrase obviously consists of the words ARTILLERY REGIMENT, probably followed by STOP.

For example:

```
F13  KR  EA  QI  GT    TV    EC  LF    OR    LR  QA  PQ
     -A  RT  IL  (LE)(RY)  RE  (GI)(ME)  NT  ST  (OP)
```

On this basis, the following equations can be produced, figure 11–32, and the matrix expanded again.

$\overline{LEp} = \overline{GTc}$

$\overline{RYp} = \overline{TVc}$

$\overline{GIp} = \overline{LFc}$

$\overline{STp} = \overline{QAc}$

$\overline{OPp} = \overline{PQc}$

E	C	T	A	R
G		L	B	N
F	H	I	K	D
O	P	Q	S	M
W	X	Y	Z	V

Figure 11–32 (~~C~~). Third expansion of matrix (U).

(3) The third phrase TANK UNITS WILL, where $\overline{UNp} = \overline{LGc}$ provides the one additional value. Thus, the matrix is completed as shown in figure 11–33. It is now a simple matter to decipher the cryptogram.

11–9. (~~C~~) Completion of the matrix

a. In the preceding example, the proposition that recovery of the text and reconstruction of the matrix proceeds simultaneously is shown. The question yet to be answered is whether it is the correct matrix. The fact that a message can be deciphered does not prove its correctness. This condition arises out of the fact that for each specific matrix there are 24 additional cyclic permutations which will give exactly the same results. The importance of the recovery of the original matrix lies in the possibility of predicting future matrix values given the knowledge of current matrix arrangement.

b. In the case of a keyword mixed sequence as the Playfair matrix, recovery of the permutation of the square presents little difficulty, using as a base the UVWXYZ cluster which rarely forms a part of the keyword. To observe this, examine again the matrix in figure 11–34, just previously recovered.

E	C	T	A	R
G	U	L	B	N
F	H	I	K	D
O	P	Q	S	M
W	X	Y	Z	V

Figure 11–33 (~~C~~). Reconstructed Playfair matrix (U).

E	C	T	A	R
G	U	L	B	N
F	H	I	K	D
O	P	Q	S	M
W	X	Y	Z	V

Figure 11–34 (~~C~~). Playfair matrix reconstructed (U).

The last three rows are obviously out of sequence, *V* should precede the *W*, *M* should precede the *O*, and *D* should precede the *F*. By a simple shift of the last column to the first position, the matrix is reordered and now in its correct sequence. This can be noted in the appearance of the keyword RECTANGULAR. This is a simplified example, but it serves to illustrate the point that in keyword mixed sequences, the alphabetic sequence of that part of the alphabet outside the keyword sequence serves to reorder the matrix. Other cases are more complicated, but the basic principles remain the same.

c. In the case of Playfair matrices based on a transposition mixed sequence, the recovery of the original presents a different problem for which different procedures must be used. Essentially the process lies in the recognition of patterns in one of the original matrix's permutations and, using this as a base, reconstructing the original. The following illustrates this process.

(1) Given an original matrix, shown in figure 11–35, recovery of a transposition mixed sequence and the keyword follows the same procedures as previously given for transposition ciphers.

A	G	W	C	Q
E	T	F	M	Z
H	S	I	N	L
D	V	P	B	U
R	O	Y	K	X

Figure 11–35 (~~C~~)*. Playfair matrix* (*U*).

By scanning the rows of the matrix, which correspond to the columns of the keyword matrix, several bits which exhibit alphabetic progression can be found. They are: *AGW*, *LDV*, *FMZ*, *PBU*, and *YKX*. Set on end as columns and juxtaposed in alphabetic sequence by last letter, they form the order:

```
P L A Y F
B D G K M
U V W X Z
```

With this, the beginning of the keyword should be obvious, leading to a rapid solution. But if it was not, by shifting to the second row and building further on its sequential pattern, the following sequence would be produced, as shown in figure 11–36.

```
8 7 1 Ø 4 6 9 2 5 3

P L A Y F I R C H E
B D G K M N O Q S T
U V W X Z
```

Figure 11–36 (C)*. Recovery of mixed keyword sequence* (*U*).

(2) Where the analyst works from a permutation of the original enciphering matrix, a modification in this procedure is required as a preliminary step. He must first find some one permutation which shows the sequence characteristics on which he can base the recovery of the keyword. For example, given the matrix permutation of figure 11–37, recovery of the keyword would be difficult, as its rows do not exhibit columnar order of the transposition matrix to the required degree.

F	X	R	M	Y
T	G	A	N	C
Q	I	K	Z	H
W	O	S	L	E
B	U	D	V	P

Figure 11–37 (~~C~~)*. Matrix permutation* (*U*).

Since a permutation of the rows does not affect keyword recovery, the analyst need only permutate the columns. This can be done by constructing a 5 x 9 matrix of repeated columns, as illustrated in figure 11–38.

1	2	3	4	5	1	2	3	4
F	X	R	M	Y	F	X	R	M
T	G	A	N	C	T	G	A	N
Q	I	K	Z	H	Q	I	K	Z
W	O	S	L	E	W	O	S	L
B	U	D	V	P	B	U	D	V

Figure 11–38 (~~C~~)*. Repetition of column permutations* (*U*).

(3) Testing each five by five combination, the analyst will soon find a permutation containing the appropriate sequence. In this case, it is the fifth, shown in figure 11–39.

R	M	Y	F	X
A	N	C	T	G
K	Z	H	Q	I
S	L	E	W	O
D	V	P	B	U

Figure 11–39 (~~C~~). *Selection of correct permutation* (*U*).

From this permutation using the underlined sequences, the original keyword and matrix can be recovered as illustrated in figure 11–40.

8	7	6	Ø	3	9	1	4	5	2
P	O	L	Y	G	R	A	H	I	C
B	D	E	F	K	M	N	Q	S	T
U	V	W	X	Z					

A	N	C	T	G
K	Z	H	Q	I
S	L	E	W	O
D	V	P	B	U
R	M	Y	F	X

Keyword: *POLYGRAPHIC*

Figure 11–40 (~~C~~). *Recovery of keyword mixed sequence and original enciphering matrix* (*U*).

PART FIVE (~~C~~)

POLYALPHABETIC SUBSTITUTION SYSTEMS

CHAPTER 12 (~~C~~)

PERIODIC POLYALPHABETIC SUBSTITUTION

Section I. (~~C~~) INTRODUCTION

12–1. (~~C~~) Mono- and Polyalphabetic Cipher Systems

a. In previous paragraphs, the cipher systems presented used one basic alphabet for the encipherment of messages. Thus they are classified as monoalphabetic ciphers. It is true that certain of those systems provide for variant values, yet they are not classified as polyalphabetic. The essential difference between monoalphabetic and polyalphabetic substitution lies in the primary objective of the system.

(1) In those monoalphabetic substitution systems having variant values, the object is to suppress so far as possible the characteristic frequency of letters and resultant word patterns. Several methods are shown, some which provide several different cipher values as equivalents for all the plaintext letters, and others which provide only variant values as cipher equivalents for the high-frequency letters. In each system there are conditions inherent in the method of encipherment itself, conditions that produce, in the cryptogram, certain definite clues that lead to the establishment of the equivalencies for one plaintext value.

(2) Moreover, each of those systems derives its security from the care with which the cryptographer performs his task. Given the free choice of using variant values, or if he was hurried or slip-shod and used the same variant value consistently, he would materially detract from the security of the system.

(3) In either case, the end result is that cryptograms are produced whose true security lies in the minimum use of the system. Given a number of cryptograms from the same system, or a few combined with poor encryption procedures, solution is relatively easy.

b. In the case of true polyalphabetic substitution systems, the object is to establish a definite procedure for the automatic shifting or changing of a number of cipher alphabets employed in the encipherment of a single message during its encipherment, thus producing variant values. Furthermore, this method, within certain limits, is beyond the whim of the cryptographer. The total result of such a system is to greatly increase the degree of difficulty in establishing the cipher equivalencies of a given plaintext value. There are a number of true polyalphabetic cipher systems, although for military their number is limited for reasons of practicality. All true polyalphabetic systems will exhibit following essential characteristics.

(1) Each plaintext letter is represented by two or more cipher equivalents, their exact identities being determined by the position they occupy in the plaintext.

(2) One and the same cipher letter represents two or more different plaintext letters, the exact equivalencies being determined by the system itself.

12–2. (~~C~~) Example of Polyalphabetic Substitution

a. Polyalphabetic substitution is illustrated in figure 12–1.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*
C2	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*
C3	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*
C4	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*
C5	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*
C6	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*

```
Key:     1 2 3 4 5   6 1 2 3 4 5 6 1 2 3 4 5 6 1   2 3 4 5
         E N E M Y   R E E N F O R C E M E N T S   S E E N
         G V T T C   I G M C M S I E M B L R K U   A T L R

         6 1   2 3 4 5 6 1 2 3   4 5   6 1 2 3   4 5 6
         I N   V I C I N I T Y   O F   H I L L   O N E
         Z P   D X J M E K B N   V J   Y K T A   V R V

         1 2 3 4   5 6 1 2   3 4 5 6   1 2 3 4 5 6 1 2
         Z E R O   Z E R O   N I N E   P O S S I B L E
         B M G V   D V T W   C P R V   R W H Z M S N M

         3 4 5 6 1 2   3 4 5 6 1 2 3 4 5
         A T T A C K   I N D I C A T E D
         P A X R E S   X U H Z E I I L H


         G V T T C   I G M C M   S I E M B   L R K U A   T L R Z P

         D X J M E   K B N V J   Y K T A V   R V B M G   V D V T W

         C P R V R   W H Z M S   N M P A X   R E S X U   H Z E I I

         L H X X X
```

Figure 12–1 (~~C~~). *Example, polyalphabetic substitution* (*U*).

b. In the system above, the cipher equivalent for the first plaintext value is drawn from the first cipher component (Ep=*Gc*), the second from the second (Np=*Vc*), and so forth until the sixth cipher component is reached. At this point, the seventh letter of the message, the first cipher component, is used once again as the source of the cipher equivalency. Thus the frequency of the plaintext letter and any characteristic pattern that might occur in the plaintext are suppressed.

c. The method of encipherment demonstrated above can be duplicated with a simple strip arrangement and a numeric key which corresponds to the different juxtaposition of the cipher and plain sequence above. For example, the alphabet could be reproduced as follows:

P ABCDEFGHIJKLMNOPQRSTUVWXYZ
C *ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRS* etc.

(1) In figure 12–1, the successive juxtapositions of the plain to cipher are Ap=*Cc1*, *Ic2*, *Pc3*, *Hc4*, *Ec5*, and *Rc6*. These juxtapositions can be indicated by the assignment of numeric values to each. Thus, they may be indicated as 3–9–16–8–5–18, where 3 indicates the third letter of the cipher sequence (c), 9 indicates the ninth letter in the cipher sequence (1), and so forth. These numbers indicating the sequential position of the letters are the cyclic setting of the strip.

(2) To encipher the message given above, the keys can be written out horizontally and the message inscribed in column beneath the key. The strip alphabet is set at its first key setting (3), where Ap=*Cc* and all letters below this key are enciphered. The setting is then changed to the next key, 9, when Ap=*Ic* and all letters below this key are enciphered. The same process is continued until the entire message is enciphered; then it is transferred to five-

letter groups. A partial example is shown below in figure 12–2 using the same data as in figure 12–1.

3	9	16	8	5	18
E	N	E	M	Y	R
$\underline{G}$	*V*	$\underline{T}$	*T*	*C*	$\underline{I}$
E	E	N	F	O	R
$\underline{G}$	$\underline{M}$	*C*	*M*	*S*	$\underline{I}$
C	E	M	E	N	T
E	$\underline{M}$	*B*	$\underline{L}$	$\underline{R}$	*K*
S	S	E	E	N	I
U	*A*	$\underline{T}$	$\underline{L}$	$\underline{R}$	*Z*

Ciphertext : *GVTTC IGMCM SIEMB LRKUA TLRZ.* ... etc.

Figure 12–2 (~~C~~). Columnar encipherment duplicating key period (U).

12–3. (~~C~~) Classification of Polyalphabetic Substitution Systems

a. Polyalphabetic substitution ciphers can be classed into two distinct types, periodic systems and aperiodic systems. The periodic systems include those whose cryptographic treatment results in the production of cyclic phenomena in the cryptographic text. Note, for example, the columnar encryption process just demonstrated. Therein, the cyclic nature of periodic polyalphabetic substitution can be seen in the repetition of constant plain to cipher equivalencies in each column, i.e. in the first column Ep=*Gc*, in the second, Ep=*Mc*, in the third Ep=*Tc*, and in the fourth Ep=*Lc*. The cryptographic process of aperiodic systems on the other hand is designed to eliminate this cyclic phenomena. The specifics of this system and its analysis are treated in chapter 14.

b. The cyclic phenomena inherent to a periodic system may be exhibited externally, as in the system above. In these cases, the phenomena is said to be patent. In some ciphers the cyclic phenomena is not exhibited in the cryptographic text, in which case they are said to be latent. The periodicity of the cipher under these conditions must be uncovered by a step to be explained, preliminary to analysis.

(1) The periodicity of a given system may be quite definite, determinable with mathematical preciseness, in which case the periodicity is said to be fixed. The example above fits this definition, the period there being fixed at six.

(2) In other instances, the periodicity may be more or less flexible, depending upon the system, but subject to definite limits imposed by that system. In such a case the periodicity is said to be flexible.

c. A primary classification of periodic systems is by the number and method of usage of the cipher alphabets. All periodic systems are considered to be either a repeating key or a progressive alphabet system.

(1) In a repeating key system, only a few of a whole possible set of cipher alphabets are used in enciphering a given message. These alphabets used in a fixed sequence determined by the key are employed repeatedly until the message is enciphered. Possibly the same key may be used to encipher a second message, or a new key may be used for each message. The key itself may be a secret word, a phrase, or a number. In any case, it determines the numbers, identity, and sequence of use of the cipher alphabets.

(2) In a progressive alphabet system, all the cipher alphabets comprising the complete set for the system are used one after the other, in turn, for the encipherment of a message. When the last alphabet is used, the sequence of use is begun anew.

12–4. (~~C~~) Classification of Cipher Alphabets

a. The substitution process in polyalphabetic ciphers involves the use of a number of alphabets which can be derived by a number of methods. The exact nature of their preparation, which determines their characteristics, plays an important role in the solution of polyalphabetic ciphers. Cipher alphabets for polyalphabetic substitution are classified as independent and derived.

(1) Independent or unrelated cipher alphabets contain separate and distinct plain and cipher sequences having no relationship to one another. Such sequences can be derived by any of the methods previously discussed, i.e. they may be keyword mixed columnar, keyed columnar mixed, or decimated alphabets. The solution of cryptograms produced with independent alphabets is made more difficult by the very reason that no relationship exists between them. For this reason, in the course of analysis, values are not transferable. However, since their production and handling in the cryptographic process poses problems affecting their practicability, they are not as favored as interrelated cipher alphabets. Hence, they are not as often encountered.

(2) Derived or interrelated alphabets, as the names imply, are produced by the interaction of two primary components which, when juxtaposed at various points, yield a number of secondary alphabets. The number of secondary alphabets, given two constant primary components, is equal to the number of different points of coincidence. In effect then, what is brought about is either a strip system, such as the one shown in paragraph 12–2*c*, or a

cipher alphabet, also shown in paragraph 12–2*a*, which has one plain component and several cipher sequences, all of like structure, joined together at varying points of coincidence. The cipher sequences generated by the juxtaposition are termed secondary alphabets.

b. For the purpose of cryptanalysis, some of the more common configurations of the primary components and secondary alphabets derived therefrom are given in the following:

(1) *Case I.* The primary components are both normal sequences.

(*a*) The sequences proceed in the same direction; the secondary alphabets produced are direct standard alphabets offset at points of juxtaposition.

(*b*) The sequences proceed in opposite directions; the secondary alphabets are reversed standard alphabets and are reciprocal with the same limitations as discussed in paragraph 7–6*a*.

(2) *Case II.* The primary components are not both normal alphabets.

(*a*) The plain component is a standard alphabet and the cipher component is a mixed sequence; the secondary alphabets are then mixed alphabets.

(*b*) The plain component is a mixed alphabet and the cipher component is a normal alphabet; the secondary alphabets are again mixed alphabets.

(3) *Case III.* Both components are mixed sequences.

(*a*) Components are identical mixed sequences proceeding in the same direction; the secondary alphabets are also mixed sequences.

(*b*) Components are identical mixed sequences proceeding in opposite directions; the secondary alphabets are mixed sequences and also are reciprocal, again with the limitations discussed in paragraph 7–6*a*.

(*c*) Components are different mixed sequences either proceeding in the same or opposite directions; the secondary alphabets are mixed alphabets.

12–5. (~~C~~) Repeating Key

a. It is the use of a repeating key which imparts the cyclic pattern, or periodicity, to periodic polyalphabetic substitution. Repeating keys are used to indicate the number, identity, and the sequence of the cipher alphabets used. The key itself, as shown in preceding examples, can be expressed in terms of numbers or letters, both derived from the other, and the letters usually spelling out a word. The literal key may be a word, a phrase, or even a sentence, usually being easily recalled.

b. In the key proper, its total number of elements determine the number of alphabets to be used. The identity of each element determines the specific cipher alphabet used, and its relative order in the key determines the sequence of the cipher alphabets. The total number of cipher alphabets available for use in a given system may be unlimited, except for practical purposes. However, where alphabets are reproduced by sliding two primary alphabets against one another, only 25 cipher alphabets, in the case of English alphabets, are possible. The key then, in some respects, is unlimited as to length. However, in most cases it will be found to correspond to a word, phrase, or sentence, usually one that is easily remembered.

c. To use a key in finding equivalents with sliding primary components, four elements must be known. They are the key letter (k), the index letter (i), the plaintext letter (p), and the cipher letter (c).

(1) The key letter and the index letters indicate the point of coincidence of the cipher and plain component. For example:

```
             Ok=Ai
                              (i)
P                             ABCDEFGHIJKLMNOPQRSTUVWXYZ
C           ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
                              (k)
```

(2) The meanings associated previously with c and p remain unchanged, c indicating the cipher value and p the plaintext value. Thus to find one value, an equation using these elements may be written as:

Ok=Ai; Ep=*Sc*

(3) Note that in the above, two tacit assumptions are involved. First it is accepted that the index letter (i) is found in the plain component and that it is the letter A, and second that the key letter (k) is found in the cipher component. Normally this is the case. However, it need not be so. The index letter used, and the relative location of k, i, p, and c can be easily changed, only a fixed agreement between the correspondents being required. Thus in a key and equivalency equation, the key and index letter must be specified and the relative location of all elements shown. This can be accomplished very simply, merely by adding a number (1) for the plain component, and (2) for the cipher component to the

equation given above. Thus the conventional method of finding an equivalency is shown as:

Ok/2=Ai/1; Ep/1=*Sc*/2

(4) As mentioned previously, the normal method of finding equivalencies need not always be followed. In fact, employing 2 sliding components and the 4-element equation, 12 possible combinations result. However, as the method above is most widely used, only it will be given.

Section II. (~~C~~) THEORY OF SOLUTION OF PERIODIC POLYALPHABETIC SUBSTITUTION

12–6. (~~C~~) The Three Steps of Analysis

a. The cryptography of periodic polyalphabetic substitution, as illustrated previously, is such that its solution may be effected by the completion of three steps in succession. These steps are:

(1) *Determining the period.* The analyst attempts to determine the length of the key which imparts the cyclic periodicity to the system. This is done through the isolation and analysis of groups found repeated in the message. The repeats used in this approach must not be accidental repeats, but repeats which have resulted through a cyclic juxtaposition of similar sequences in the plaintext and similar sequential periods of key usage. In effect, the determination of the period identifies the number of alphabets used in the system as the cyclic periodicity is a result of the use of a number of alphabets.

(2) *Reduction to monoalphabetic terms.* In this step, once the period has been identified, the analyst can divide the text into a number of segments equal to the number of alphabets involved, each of these segments representing that portion of the ciphertext produced by one of the cipher sequences. Thus a polyalphabetic text is reduced to its monoalphabetic bits and is susceptible to analysis on those terms.

(3) *Identification of ciphertext values.* The third step is that of analyzing each of the monoalphabetic ciphertext distributions produced by the second step in order to determine their respective plaintext values. In this step, essentially the same techniques are used as for the analysis of any monoalphabetic cipher.

b. The foregoing steps comprise the general outline of solution for any periodic polyalphabetic substitution cipher systems, regardless of the kind of cipher alphabets involved. There is, of course, some modification required for each particular case.

c. As a matter of course, prior to the analysis, any cryptosystem must first be identified. Identification, in the case of periodic polyalphabetic substitution cipher systems, rests upon the two characteristics of the system, its polyalphabeticity which imparts a relative flatness to the frequency distribution, and the cyclic phenomena within the text. Statistically, computations will indicate that the message text is random. The cyclic use of a number of alphabets will result in cyclic phenomena indicated by one or more of the following conditions:

(1) Length of message and repeats will not be divisible by a constant factor.

(2) Distance between repeats will be a factor of the period length.

(3) Small cyclic periods, particularly those of even numbers, are apt to produce significantly higher than random digraphic indexes of coincidence.

(4) Statistical computation of each monoalphabetic sequence, the result of step two, usually indicates plaintext, though this is subject to variation due to relative numbers of letters enciphered by each sequence.

12–7. (~~C~~) Basis for Determining the Period

a. The external phenomena on which the determination of a system's periodicity is based, is a result of the encipherment of an identical plaintext letter by the same cipher sequence, several times. The repetitions so produced are called casual repetitions since their cause is a direct result of the use of a periodically repeating key. It also happens that different plaintext letters, enciphered by a different cipher sequence, will produce identical cipher letters in the ciphertext. In this case, since the repetitions are produced by the accidental juxtaposition of different values, they are termed accidental repetitions.

b. As the determination of the period length depends upon the analysis of repetition which occurs in the ciphertext, it is obvious that a distinction must be made between causal and accidental repetitions. In the case of single letters, this becomes very difficult as accidental repetitions can occur as frequently as causal repetitions. Thus no basis for distinguishing one from the other is provided. However, in the case of digraphs and polygraphs, the chances of a number of different plaintext letters and cipher sequences coinciding sequentially several times to produce accidental repetitions of ciphertext is greatly reduced. Statistically, the chances of repetitions of varying length occurring in a given number of letters of random text can be computed. Thus the repetitive phenomenon which may be expected as a result of pure chance can be duplicated, and provides a means of evaluating the significance of repetitions observed in a ciphertext. If the observed repetitions are no more than would be expected by chance, generally they would not be considered significant. However, if the repetitions exceed the value of chance repetitions, they would be open to interpretation and exploitation as causal repetitions.

c. A summary of the expected number of appearances of digraphs, trigraphs, tetragraphs, and pentagraphs in samples of random text of 100 to 1000 letters, in increments of 100 is shown in figure 12–3.

Number of letters	Expected number of digraphs occurring exactly x times								
	E(2)	E(3)	E(4)	E(5)	E(6)	E(7)	E(8)	E(9)	E(10)
100	6.21	0.298	0.011						
200	21.8	2.12	0.154	0.009					
300	42.5	6.23	0.683	0.060	0.004				
400	65.3	12.8	1.87	0.220	0.022	0.002			
500	88.1	21.6	3.97	0.582	0.071	0.008			
600	110	32.3	7.11	1.25	0.184	0.023	0.003		
700	129	44.3	11.4	2.35	0.403	0.059	0.008	0.001	
800	145	57.1	16.8	3.96	0.777	0.130	0.019	0.003	
900	158	70.1	23.2	6.16	1.36	0.257	0.043	0.006	0.001
1000	169	83.0	30.6	9.03	2.21	0.466	0.085	0.014	0.002

Number of letters	Exp. number of trigraphs			Number of letters	Tetragraphs		Number of letters	Penta-graphs
	E(2)	E(3)	E(4)		E(2)	E(3)		E(2)
100	0.269	0.001		100	0.010		100	
200	1.10	0.004		200	0.043		200	0.002
300	2.48	0.014		300	0.096		300	0.004
400	4.40	0.033		400	0.171		400	0.007
500	6.85	0.064		500	0.270		500	0.011
600	9.81	0.111	0.001	600	0.389		600	0.015
700	13.3	0.175	0.002	700	0.530		700	0.021
800	17.3	0.261	0.003	800	0.693		800	0.027
900	21.8	0.371	0.005	900	0.877		900	0.034
1000	26.8	0.505	0.008	1000	1.08	0.001	1000	0.042

Figure 12–3 (~~C~~). Table of expected polygraphs (U).

The numbers in columns E(2), E(3), etc., refer to the numbers of times a given number of digraphs can be expected to occur by chance in the sampling of letters given in the column at the left margin. Thus in a sample of 300 letters of random text, i.e. periodic polyalphabetic substitution, 43 digraphs can be expected to appear twice, 6 digraphs can be expected to appear 3 times, and 1 digraph can be expected to appear 4 times. The decimal fractions that follow in the succeeding columns of the same row may be interpreted as follows: the value 0.683 under column E(4) means that in 100 samples of 300 letters each, about 68 of them will have a digraph which occurs 4 times; 0.060 under column E(5) indicates that in 100 samples of 300 random letters, 6 samples will contain a digraph occurring 5 times. Thus in the tables, the number within the brackets indicates the number of polygraphs, and the number in each column below that symbol indicates the number of times of their occurrence in a message or messages.

12–8. (~~C~~) Determining Periodicity

a. Using the statistical information contained in the foregoing table, the determination of periodicity of a cryptogram is a relatively simple matter. As an illustration, the following cryptogram shown in figure 12–4 with repeated groups underlined, will be used.

	5	10	15	20	25
A	*USYES*	*ECPMP*	*LCCLN*	*XBWCS*	*OXUVD*
D	*SCRHT*	*HXIPL*	*IBCIJ*	*USYEE*	*GURDP*
C	*AYBCX*	*OFPJW*	*JEMGP*	*XVEUE*	*LEJYQ*
D	*MUSCX*	*JYMSG*	*LLETA*	*LEDEC*	*GBMFI*

Figure 12–4 (*C*). *Ciphertext with evidence of periodicity* (*U*).

b. In the message above, the observed repetitions are far in excess of those normally expected. For example, 7 digraphs are observed being repeated twice (*EC, PL, SC*, BC, *JY*, US, and CX), about the expected values for a message of 100 letters. However, note that 2 other digraphs (LE and US) are repeated 3 times, a rate of repetition expected in the case of a message of 200 letters. Finally, the repeat of the tetragraph (*USYE*), statistically expected in a random text message of 1000 letters, establishes almost beyond any doubt that the repeats are causal rather than accidental. The only explanation is that the plaintext value for *USYE* must fall in exactly the same relative position to the key in both instances.

12–9. (~~C~~) Factoring To Determine Length of the Period

a. Since periodicity, as reflected in causal repetitions, is a result of enciphering identical letters by identical cipher sequences, it follows that the length of the period can be ascertained by determining the constant interval between repeated occurrences of the same digraph or polygraph. For example, by counting the letters intervening between each repeat, the count to include the letters of the first but not the second appearance of the repeat, the following intervals and factors will be found (fig. 12–5).

Repetition	Interval	Factors
1st *USYE* to 2d *USYE*	40	2, 4, 5, 8, 10, 20
1st *BC* to 2d *BC*	16	2, 4, 8
1st *CX* to 2d *CX*	25	5
1st *EC* to 2d *EC*	88	2, 4, 11, 22, 44
1st *LE* to 2d *LE*	16	2, 4, 8
2d *LE* to 3d *LE*	4	2
1st *LE* to 3d *LE*	20	2, 4, 5, 10
1st *JY* to 2d *JY*	8	2, 4
1st *PL* to 2d *PL*	24	2, 3, 4, 6, 8, 10, 12
1st *SC* to 2d *SC*	52	2, 4, 13, 26
(1st *SY* to 2d *SY*, already included in *USYE*.)		
(1st *US* to 2d *US*, already included in *USYE*.)		
2d *US* to 3d *US*	36	2, 3, 4, 6, 9, 18
1st *US* to 3d *US*	76	2, 4, 19, 38
(1st *YE* to 2d *YE*, already included in *USYE*.)		

Figure 12–5 (~~C~~). *List of repetitions and factors* (*U*).

b. After determining the interval between all repetitions, each in turn is factored, the object here being to locate one factor which is common to all. Recall that a given key length, synonymous with the number of cipher sequences, determines the periodicity of a system. Further, note that any given causal repetition occurs as the result of the encipherment of a group of identical letters by the same key sequence. Now this may occur at the first, second, third, etc., cycle of key usage. In any case, it must be a permutation of a fixed number, the key length. Therefore, factoring the intervals should reveal the true key length. Similarly, if one or more intervals are found which cannot be factored by some number as the majority of the intervals, they can be assumed to be accidental repetitions. With this in mind, examine the factors given in figure 12–5.

c. It will be noted that with the exception of *CX*, all the repetitions can be factored by either 2 or 4. In the case of *CX*, since its factor is both different and isolated, its repetition can be ascribed to accidental rather than causal reasons and can, therefore, be dropped from further study. Thus only the factors 2 and 4 are left for consideration. Since these factors are common to all intervals between repetitions and since the repetitions have been determined to be causal rather than accidental, the key length, or number of cipher alphabets, must be one or the other of these numbers.

d. In this particular case, the final choice for the key length cannot be resolved except by reducing the ciphertext to its monoalphabetic components. However, on the basis of practicability, it can be assumed that the key length is four rather than two. In cases of multiples it is better to assume the larger number initially.

12–10. (~~C~~) Reduction to Monoalphabetic Terms

a. In foregoing paragraphs, the inherent monoalphabeticity of segments of a periodic polyalphabetic cipher are demonstrated. As this monoalphabeticity arises from the cyclic encipherment of the plaintext by a fixed number of alphabets, a polyalphabetic ciphertext can be reduced to monoalphabetic terms when it is divided into segments by a number which corresponds to the key length. The division of the ciphertext can be accomplished by either setting the message down in columnar form, each column representing the use of one enciphering alphabet, or by transcribing the message into groups equal in length to the key. Each group then represents one periodic cycle of cipher alphabet usage. In either case, the results are the same, the choice of method left to the analyst. Using the latter method the example message would be transcribed as:

```
USYE  SECP  MPLC  CLNX  BWCS  OXUV  DSCR
HTHX  IPLI  BCIJ  USYE  EGUR  DPAY  BCXO
FPJW  JEMG  PXVE  UELE  JYQM  USCX  JYMS
GLLE  TALE  DECG  BMFI
```

b. Each group above represents the periodic cycle of the cipher sequence. Thus all first letters of each group are produced by the first cipher alphabet, the second letter by the second alphabet, and so forth. With the monoalphabetic segment of the ciphertext now isolated, a separate uniliteral frequency distribution is made for each. Theoretically, if each distribution is great enough, and contains no abnormal variation from common usage, each frequency distribution should result in the characteristic peaks and troughs of monoalphabetic substitution. Under normal circumstances, where the correct period has been determined, this occurs and seems to prove the correctness of the assumption of period lengths. However in more difficult cases, where the sample is small, and contains an insufficient number of polygraphic repetitions, or where a clear cut choice between two possible factors of periods cannot be made, other monoalphabetic substitution tests may be used.

Section III. (~~C~~) STATISTICAL TEST FOR DETERMINING PERIODICITY

12–11. (~~C~~) The Phi (φ) Test

a. The monoalphabetic φ test, previously discussed in paragraph 2–15, may be applied to the distribution of periodic polyalphabetic ciphers to confirm the monoalphabeticity of the distribution made on the assumption of a given period. This test is particularly applicable in difficult cases where each distribution is noncommittal in respect to peaks and troughs, as where the factoring process results in the choice of two possible period lengths. When the correct period is assumed, then the φ test of each distribution should approach fairly closely and consistently the values for φp. On the other hand, if an incorrect period is assumed, the calculated φo should approximate the value of φr rather than φp.

b. To illustrate this process, φo of the distributions made of the example cryptogram is calculated in figure 12–6 using the formula φo=Σf(f−1).

```
                                                          N-25
A  B C D E F G H I J K L M N O P Q R S T  U V W X Y Z
0 12 0 6 0 0 0 0 0 6 0 0 0 0 0 0 0 0 0 0 12 0 0 0 0 0
    φp = .0667N(N-1) = 40.02              φo = Σf(f-1) = 36
    φr = .0385N(N-1) = 23.10

                                                          N-25
A B C D  E F G H I J K L M N O  P Q R  S T U V W X Y Z
0 0 2 0 12 0 0 0 0 0 0 2 0 0 0 12 0 0 12 0 0 0 0 2 2 0
    φp = .0667N(N-1) = 40.02              φo = Σf(f-1) = 44
    φr = .0385N(N-1) = 23.10

                                                          N-25
A B  C D E F G H I J K  L M N O P Q R S T U V W X Y Z
0 0 20 0 0 0 0 0 0 0 0 20 2 0 0 0 0 0 0 2 0 0 0 2 0
    φp = .0667N(N-1) = 40.02              φo = Σf(f-1) = 46
    φr = .0385N(N-1) = 23.10

                                                          N-25
A B C D  E F G H I J K L M N O P Q R S T U V W X Y Z
0 0 0 0 30 0 2 0 2 0 0 0 0 0 0 0 0 2 2 0 0 0 0 6 0 0      f(f-1)
    φp = .0667N(N-1) = 40.02              φo = Σf(f-1) = 44
    φr = .0385N(N-1) = 23.10
```

Figure 12–6 (C). The φ test for factored periods (U).

c. In this case, the results of the ϕ test are indications that each alphabet represents a case of monoalphabetic substitution, which in turn proves the validity of the original determination of the cipher's period. Note that in some cases a ϕ test conducted on the multiple of a true period will result in the appearance of monoalphabeticity. An example occurs in this particular case where, if eight was assumed, the resultant distribution and their ϕ tests indicate monoalphabeticity. However, an inspection of the distribution reveals that on the basis of similar characteristics distributions 1 and 5, 2 and 6, 3 and 7, and 4 and 8, could be combined into 4. Whatever the method used, the result is the same, the reduction of the ciphertext to monoalphabetic terms.

12–12. (~~C~~) The Index of Coincidence (I.C.)

a. Another method of proving the apparent validity of the factoring process is through the use of the index of coincidence. The I.C. was previously defined as the ratio of ϕo to ϕr, expressed in formula as I.C.$=\frac{\phi o}{\phi r}$. The monographic I.C. of English plaintext is 1.73 as compared with the I.C. of 1.00 for random text. Using this text, the individual distributions, if the factoring process is correct, will tend to conform more closely to the expected I.C. of plaintext than to the I.C. of random text.

b. To demonstrate the operation of the formula and show its results for comparison with those obtained by the ϕ test, the foregoing distributions and the calculated values of ϕo and ϕr will be used (fig. 12–7).

IC for Distribution No. 1	1.00	IC of English Random Test
$\frac{\phi o}{\phi r}$ = IC or $\frac{36}{23}$ =	1.56 1.73	 IC of English Plain Text
IC for Distribution No. 2	1.00	IC of English Random Text
$\frac{\phi o}{\phi r}$ = IC or $\frac{44}{23.1}$ =	1.91 1.73	 IC of English Plain Text
IC for Distribution No. 3	1.00	IC of English Random Text
$\frac{\phi o}{\phi r}$ = IC or $\frac{46}{23.1}$ =	1.99 1.73	 IC of English Plain Text
IC for Distribution No. 4	1.00	IC of English Random Text
$\frac{\phi o}{\phi r}$ = IC or $\frac{44}{23.10}$ =	1.91 1.73	 IC of English Plain Text

Figure 12–7 (~~C~~). Index of coincidence for factored periods (U).

c. In all four cases above, it can be seen that the I.C. calculated for each distribution more closely approximates the I.C. of plaintext than that of random text. Thus, as in the case of the ϕ test, the results, i.e. the monoalphabeticity of each distribution is indicated, further indicate that the initial assumption of a period of four is correct.

12–13. (~~C~~) Table of Expected Values

As an aid in the calculation of either monographic I.C. or ϕ values, a table of the expected values of ϕp and ϕr for sample sizes from 11 to 100 is given below in figure 12–8. To use the table (fig. 12–8), only the value of N, the total number of letters occurring in a given distribution, need be tabulated and the values of ϕo determined.

N	ϕ_r	ϕ_p	N	ϕ_r	ϕ_p	N	ϕ_r	ϕ_p	N	ϕ_r	ϕ_p	N	ϕ_r	ϕ_p
11	4.23	7.34	29	31	54	47	83	144	65	160	277	83	262	454
12	5.08	8.80	30	33	58	48	87	150	66	165	286	84	268	465
13	6.00	10.4	31	36	62	49	90	157	67	170	295	85	275	476
14	7.00	12.1	32	38	66	50	94	163	68	175	304	86	281	488
15	8.08	14.0	33	41	70	51	98	170	69	180	313	87	288	499
16	9.23	16.0	34	43	75	52	102	177	70	186	322	88	294	511
17	10.5	18.1	35	46	79	53	106	184	71	191	331	89	301	522
18	11.8	20.4	36	48	84	54	110	191	72	197	341	90	308	534
19	13.2	22.8	37	51	89	55	114	198	73	202	351	91	315	546
20	14.6	25.3	38	54	94	56	118	205	74	208	360	92	322	558
21	16.2	28.5	39	57	99	57	123	213	75	213	370	93	329	571
22	17.8	30.8	40	60	104	58	127	221	76	219	380	94	336	583
23	19.5	33.8	41	63	109	59	132	228	77	225	390	95	343	596
24	21.2	36.8	42	66	115	60	136	236	78	231	401	96	351	608
25	23.1	40.0	43	69	120	61	141	244	79	237	411	97	358	621
26	25.0	43.4	44	73	126	62	145	252	80	243	422	98	366	634
27	27.0	46.8	45	76	132	63	150	261	81	249	432	99	373	647
28	29.1	50.4	46	80	138	64	155	269	82	255	443	100	381	660

Figure 12–8 (~~C~~). Expected values of ϕr and ϕp (U).

12-14. (C) Statistical Tests to Determine Periodicity

a. A variation of the φ test may be used for the initial determination of periodicity, as opposed to proving a prior assumption as illustrated above. This particular method is quite useful in those cases where the length of the period is long as compared to ciphertext length, and where there is no pronounced repetition pattern in the text itself. For example, given the cryptogram below where the length of the key is between 40 and 50, it can be treated as shown.

(1) First, an arbitrary key length is selected and the cryptogram is written out horizontally to conform to that width. Selecting a key width of 40, the ciphertext is inscribed as follows in figure 12-9 and the φoΣf(f−1), of each column is computed, using only repeated letters.

```
                  1         1         2         2         3         3         4
        5         0         5         0         5         0         5         0
H S K̲ U S P̲ M F H D U J J̲ I X M S P̲ T P O̲ I P C I W K Z V U Y P P N E̲ U S̲ A I G
B O O G A O P G P R H B O̲ U C S H P̲ V G H Q̲ X Z S A C̲ K̲ R K V̲ B G H N V S̲ F R Y
T̲ T K̲ H K V W Z X V L I̲ J̲ H W A R̲ L K F I J S L T M H K̲ A H Q T U V T X S̲ M E C
F C S K T̲ G O O Y B X Z V L I J̲ R̲ Y A C D W E J M S C̲ A F P I E A X O K A Q̲ D W
E X P Y P Q H̲ D N O̲ J I̲ X N Z J̲ G N̲ U D̲ O̲ A R F U E R J O Y B D O̲ K E̲ I K D U V
T̲ D V E V L E T D O̲ A F R O U N Y N̲ B D̲ V Q̲ O B E G G S H Q H X O̲ P U Z C O C U
K̲ K Z I T̲ P̲ H̲ K R T C C O̲ A S B Z U G B U B B U N O V T P O V̲ M I Z D E P Q̲ F V̲
K̲ Z

4 0 2 0 2 2 2 0 0 2 0 2 4 0 0 2 2 4 0 2 2 2 0 0 0 0 2 2 0 0 2 0 2 0 2 0 6 2 0 2
```

Figure 12-9 (C). Computation of φo long periodic key (U).

(2) To compute the φo, the normal formula is used, i.e. $\phi o = \Sigma f(f-1)$. Note that in the diagram above, there are 2 columnar lengths; one of 8 letters (2 columns) and the other of 7 letters (38 columns), which must be kept separate. This data contained in the diagram is then tabulated as shown below. The column labeled φ is the observed value of φ from the table above. The column labeled x is the number of times the particular φ value occurred, and φx is the product of the two columns φ and x.

Columns N=8

φ	x	φx
0	1	0
2	1	2
	2	2

Columns N=7

φ	x	φx
0	17	0
2	19	38
4	1	4
6	1	1
	38	43

(3) Having derived the φx value by tabulating the data as shown above, it then can be used to determine the average value of φ (symbolized by $\bar{\phi}$, which is read as Phi Bar). This is done using the formula $\bar{\phi}=\frac{\phi x}{x}$ for each N value. The average value of φ ($\bar{\phi}$) is derived by adding up all the φx values for a given column length, and then dividing by the number of occurrences of columns of that length. Thus $\bar{\phi}$ for the above are:

N=8	N=7
$\bar{\phi}=\frac{\phi x}{x}=\frac{2}{2}=1$	$\bar{\phi}=\frac{\phi x}{x}=\frac{43}{38}=1.16$
$\bar{\phi}=1$	$\bar{\phi}=1.16$

(4) For comparison purposes, the value of φr and φp must be computed using the formulas:

$$\phi p = 0.0667N(N-1) \quad \text{or} \quad 0.0667 \times 8 \times 7 = 3.73$$
$$\phi r = 0.0385N(N-1) \quad \text{or} \quad 0.0385 \times 8 \times 7 = 2.15$$

and

$$\phi p = 0.0667N(N-1) \quad \text{or} \quad 0.0667 \times 7 \times 6 = 2.80$$
$$\phi r = 0.0385N(N-1) \quad \text{or} \quad 0.0385 \times 7 \times 6 = 1.61$$

The information now is set up in a table for comparison purposes as shown below:

	N=8		N=7	
Observed	φ	1.00	φ	1.16
Expected plain	φp	3.73	φp	2.80
Expected random	φr	2.15	φr	1.61

(5) On the basis of the comparison above, a key width of 40 is rejected. The next step then is to assume another key length, reinscribe the message to that width, and recompute all values again. This same process is repeated until a good match is attained. In this specific case the process would

be repeated until a width of 43 was reached. The computation at this point would appear as shown in figure 12–10.

```
H S K U S P M F H D U J J I X M S P T P O I P C I W K Z V U Y P P N E U S A I G B O O
G A O P G P R H B O U C S H P V G H Q X Z S A C K R K V B G H M V S F R Y T T K H K V
W Z X V L I J H W A R L K F I J S L T M H K A H Q T U V T X S M E C F C S K T G O O Y
B X Z V L I J R Y A C D W E J M S C A F P I E A X O K A Q D W E X P Y P Q H D N O J I
X N Z J G N U D O A R F U E R J O Y B D O K E I K D U V T D V E V L E T D O A F R O U
N Y N B D V Q O B E G G S H Q H X O P U Z C O C U K K Z L T P H K R T C C O A S B Z U
G B U B B U N O V T P O V M I Z D E P Q F V K Z

2 0 2 4 4 4 2 4 2 6 4 0 2 4 2 4 6 0 4 0 4 4 4 6 2 0 4 8 2 2 0 4 2 0 4 2 2 2 4 2 4 6 2
```

Figure 12–10 (~~C~~). φo long periodic key computation (U).

(6) Again the average value of ϕ ($\bar{\phi}$) is computed, as are ϕr and ϕp, using the formulas previously given, and the derived data is set forth in tabular form as below:

Columns
N=7

ϕ	x	ϕx
0	4	0
2	6	12
4	11	44
6	3	18
	24	74

$$\bar{\phi}=\frac{\phi x}{x}=\frac{74}{24}=3.08$$

Columns
N=6

ϕ	x	ϕx
0	3	0
2	9	18
4	4	16
6	1	6
8	1	8
14	1	14
	19	62

$$\bar{\phi}=\frac{\phi x}{x}=\frac{62}{19}=3.26$$

		N=7		N=6
Observed	$\bar{\phi}$	3. 08		3. 26
Expected plain	ϕp	2. 80		2. 00
Expected random	ϕr	1. 66		1. 15

b. The results of the last test leave little doubt that the key length of the cipher is 43. Consequently, analysis is based on that assumption. Obviously this process is rather involved in terms of repeated application of the same test. However, in those cases where the key is long, or where no repeats occur in the text to indicate key length, it is an effective tool.

CHAPTER 13 (C)

SOLUTION OF PERIODIC POLYALPHABETIC SUBSTITUTION SYSTEMS

Section I. (C) SYSTEMS USING STANDARD CIPHER ALPHABETS

13–1. (C) Determination of Type Cipher Alphabet

a. Once a given periodic polyalphabetic cipher has been reduced to monoalphabetic terms, the question arises as to what type cipher alphabet is involved. This should be determined in the initial stage of analysis as it directly affects the techniques employed, and moreover, determines the relative difficulty of the task of recovering plaintext values.

b. In practice, the type cipher alphabet used in a given system may be one of the forms given in paragraph 12–4 preceding. As the cipher letters, of themselves, give no hint of the exact form used, the analyst must determine this. As in the case of normal monoalphabetic substitution ciphers, a uniliteral frequency distribution may be used for this determination. Such a frequency distribution made of each factored segment, given sufficient depth for each, will usually indicate whether the cipher alphabets involved are standard (direct or reversed) or mixed.

c. In some cases only two or three distributions are necessary for the initial determination of the type cipher alphabet involved. However, for subsequent analysis a distribution must be made for each. Additionally, if the alphabet appears to be a mixed cipher alphabet, then it is helpful for subsequent analysis to prepare triliteral frequency distributions for each. Note that because of the reduced size of the distribution, the characteristics which permit the identification of the type alphabet may not be as pronounced as those given in previous examples. However, if one takes into consideration the reduced size of the sample, identification can usually be made.

d. Once the identification of the alphabets involved has been made, an analysis of each to determine their plaintext values can begin. Basically the techniques involved are similar to those previously explained for the analysis of monoalphabetic substitution ciphers. There is one difference which arises out of the use of several cipher alphabets which may or may not be related, and which therefore permits the use of an additional method. Generally, although the actual analysis may be more involved, it is difficult only in those cases where a reduced depth of material is encountered. The difficulty stems from the lack of data, not from its complexity. However, where messages are long, or where several messages have been enciphered in the same key, each distribution should contain sufficient elements to permit a ready identification of ciphertext values.

13–2. (C) Preliminary Identification and Factoring

a. Using the principles for analysis set forth in the preceding chapter, a cryptogram is prepared in the normal manner as illustrated in figure 13–1.

```
            5          10          15          20          25

A   A U K H Y   J A M K I   Z Y M W M   J M I G X   N F M L X
B   E T I M I   Z H B H R   A Y M Z M   I L V M E   J K U T G
C   D P V X K   Q U K H Q   L H V R M   J A Z N G   G Z V X E
D   N L U F M   P Z J N V   C H U A S   H K Q G K   I P L W P
E   A J Z X I   G U M T V   D P T E J   E C M Y S   Q Y B A V
F   A L A H Y   P O I X W   P V N Y E   E Y X E E   U D P X R
G   B V Z V I   Z I I V O   S P T E G   K U B B R   Q L L X P
H   W F Q G K   N L L L E   P T I K W   D J Z X I   G O I O I
J   Z L A M V   K F M W F   N P L Z I   O V V F N   Z K T X G
K   N L M D F   A A E X I   J L U F M   P Z J N V   C A I G I
L   U A W P R   N V I W E   J K Z A S   Z L A F M   H S
```

Figure 13–1 (C). Ciphertext prepared for analysis (U).

b. After the cryptogram is set down, it is inspected for repeated sequences, and those found are underlined as shown. In this particular case where a number of trigraphs and polygraphs are repeated, it is not necessary to bother with the digraphs. The reason for this can be understood if reference is made to the table of expectancy in paragraph 12–7*c*. In this message of 271 groups, five trigraphs are observed occurring twice each, better than twice that expected. Moreover, the odds for the observed recurrence of the pentagraph is on the order of 1 in 50. The point is that these repetitions would almost certainly be causal rather than accidental and therefore could be used for factoring to determine the period of the key.

c. On this basis the repetitions may be set down in tabular form with their locations, interval, and factors for study as shown below.

Repetition	*Location*	*Interval*	*Factors*
LUFMPZJNVC	D2, K12	160	2, 4, 5, 8, 10, 16, 20, 32, 40, 80
JZXIG	E2, H17	90	2, 3, 5, 6, 9, 10, 15, 18, 30, 45
EJK	B20, L10	215	5, 43
PTE	E12, G12	50	2, 5, 10, 25
QGK	D18, H3	85	5, 17
UKH	A2, C7	55	5, 11
ZLA	J1, L16	65	5, 13

d. Only the briefest inspection of the list of factors is required to reach the assumption that the period length is five. This being the case, a uniliteral frequency distribution is made of the text at an interval of five. Note that it is not necessary to retranscribe the text when group length, or its multiple, corresponds to assumed key length. Accordingly, the following distributions would be produced (fig. 13–2).

(1) Distribution 1.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
5	1	2	3	3	0	3	2	2	6	2	1	0	6	1	5	3	0	1	0	2	0	1	0	0	6
20	0	2	6	6	0	6	2	2	30	2	0	0	30	0	20	6	0	0	0	2	0	0	0	0	30

N = 55 φo = 164

φr = 114 φp = 198 IC = 1.44

(2) Distribution 2.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
5	0	1	1	0	3	0	3	1	2	4	9	1	0	2	5	0	0	1	2	4	4	0	0	4	3
20	0	0	0	0	6	0	6	0	2	12	72	0	0	2	20	0	0	0	2	12	12	0	0	12	6

N = 55 φp = 184

φr = 114 φp = 198 IC = 1.61

(3) Distribution 3.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3	3	0	0	2	0	0	0	8	2	2	4	8	1	0	1	2	0	0	3	4	5	1	1	0	5
6	6	0	0	0	0	0	0	56	2	2	12	56	0	0	0	2	0	0	6	12	20	0	0	0	20

N = 54 φo = 200

φr = 110 φo = 190 IC = 1.8

(4) Distribution 4.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3	1	0	1	3	4	4	4	0	0	2	2	3	3	1	1	0	1	0	2	0	2	4	9	2	2
6	0	0	0	6	12	12	12	0	0	2	2	6	6	0	0	0	0	0	2	0	2	12	72	2	2

N = 54 φo = 174

φr = 110 φp = 190 IC = 1.58

(5) Distribution 5.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	0	0	0	6	2	4	0	9	1	3	0	7	0	1	2	1	4	3	0	0	5	2	2	2	0
0	0	0	0	30	2	12	0	72	0	6	0	42	0	0	2	0	12	6	0	0	20	2	2	2	0

N = 54 φo = 210

φr = 110 φp = 190 IC = 1.91

Figure 13–2 (~~C~~). Uniliteral frequency distribution of ciphertext on period of five (U).

13–3. ~~(C)~~ Fitting the Distribution to the Normal

a. The statistical tests completed show that each distribution is apparently plaintext, exhibiting the expected characteristics of monoalphabetic substitution and thereby proving the assumption of a period of five. This being the case, the next logical step is to determine if a mixed or standard sequence was used. If the latter, the solution would be greatly simplified by a determination of the point of coincidence between the plain and cipher sequences which would establish all equivalent values. Although the peaks and troughs of the above distribution are suppressed, a closer inspection reveals their presence, and shows that they are distributed linearly rather than being bunched; an indication that the sequences are standard rather than mixed. With this in mind, an attempt can be made to fit them to the normal by the usual process of locating high frequency equivalencies.

b. By noting the relative distances between the peaks and troughs and their trend, i.e. direct or reversed of distribution 1, it appears that *Wc*=Ap. Note that at this point of coincidence the normally expected high frequency plaintext letters conform to the high frequency cipher letters thusly:

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*

Continuing the same process of comparison of the peaks and troughs of each cipher sequence with that expected for plaintext, it becomes apparent that the remaining points of coincidence are:

Distribution 2	Ap=*Hc*
Distribution 3	Ap=*Ic*
Distribution 4	Ap=*Tc*
Distribution 5	Ap=*Ec*

c. At this point it is obvious that the KEY is WHITE and that the arrangement of the several sequences is as shown in figure 13–3.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*
C2	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*
C3	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*
C4	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*
C5	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*	*D*

Figure 13–3 ~~(C)~~. Recovered enciphering matrix (U).

The text then may be deciphered to read:

ENCOUNTERED RED INFANTRY ESTIMATED AT ONE
REGIMENT AND MACHINE GUN COMPANY IN TRUCKS
NEAR EMMITSBURG(.) AM HOLDING MIDDLECREEK NEAR
HILL FIVE FOUR THREE SOUTHWEST OF FAIRPLAY(.)
WHEN FORCED BACK WILL CONTINUE DELAYING REDS
AT MARSH CREEK(.) HAVE DESTROYED BRIDGES ON
MIDDLECREEK BETWEEN EMMITSBURG TANEYTOWN
ROAD AND RHODES MILL(.)

13–4. ~~(C)~~ Completing the Plain Component

a. As in the case of monoalphabetic substitution where direct standard sequences are used, so too can periodic polyalphabetic substitution systems, if using direct standard sequences, be solved by completing the plain component. The underlying principle in the latter case is the same, i.e. the cipher sequences are nothing more than direct standard sequences offset as numbers of positions. Thus by simply inscribing a direct standard sequence vertically below each cipher letter using it as a point of origin, a columnar matrix is developed in which one line of plaintext appears. Note that as in the case of simple monoalphabetic substitution, but using either a reversed standard cipher sequence or a known mixed cipher sequence, solution is also possible, but slightly different techniques are required.

b. In respect to the solution of periodic polyalphabetic ciphers by this method, there is one difference based upon the number of generatrices. In monoalphabetic, only one generatrix, that is, the cipher sequence, was used constantly throughout. In the case of periodic polyalphabetic systems there are of course several generatrices involved, each used at a constant interval in a fixed sequential order determined by the period of the key. Thus a slightly different approach is required. If for example the former method was used it would be quite difficult to pick out the individual generatrices. This is shown in figure 13–4 below, where the plain component was

```
A U K H Y J A M K I Z Y M W M J M I G X N F M L X
B V L I Z K B N L J A Z N X N K N J H Y O G N M Y
C W M J A L C O M K B A O Y O L O K I Z P H O N Z
D X N K B M D P N L C B P Z P M P L J A Q I P O A
E Y O L C N E Q O M D C Q A Q N Q M K B R J Q P B
F Z P M D O F R P N E D R B R O R N L C S K R Q C
G A Q N E P G S Q O F E S C S P S O M D T L S R D
H B R O F Q H T R P G F T D T Q T P N E U M T S E
I C S P G R I U S Q H G U E U R U Q O F V N U T F
J D T Q H S J V T R I H V F V S V R P G W O V U G
K E U R I T K W U S J I W G W T W S Q H X P W V H
L F V S J U L X V T K J X H X U X T R I Y Q X W I
M G W T K V M Y W U L K Y I Y V Y U S J Z R Y X J
N H X U L W N Z X V M L Z J Z W Z V T K A S Z Y K
O I Y V M X O A Y W N M A K A X A W U L B T A Z L
P J Z W N Y P B Z X O N B L B Y B X V M C U B A M
Q K A X O Z Q C A Y P O C M C Z C Y W N D V C B N
R L B Y P A R D B Z Q P D N D A D Z X O E W D C O
S M C Z Q B S E C A R Q E O E B E A Y P F X E D P
T N D A R C T F D B S R F P F C F B Z Q G Y F E Q
U O E B S D U G E C T S G Q G D G C A R H Z G F R
V P F C T E V H F D U T H R H E H D B S I A H G S
W Q G D U F W I G E V U I S I F I E C T J B I H T
X R H E V G X J H F W V J T J G J F D U K C J I U
Y S I F W H Y K I G X W K U K H K G E V L D K J V
Z T J G X I Z L J H Y X L V L I L H F W M E L K W
```

Figure 13–4 (~~C~~). Completion of the plain component (U).

completed for the first 25 letters of the foregoing cryptogram.

c. With the prior knowledge of the period (5), and the plaintext, it is possible to pick out plaintext from the matrix above, but even so it would be a difficult task. Where the period or plaintext were not known it would be practically impossible. Thus it is necessary to first separate the ciphertext into its individual generatrices. Now this will of course result in the factoring of the plaintext at a constant interval, that of the period length. So the question of how plaintext would be recognized is posed. The answer to this lies in the association of high-frequency letters normal to plaintext. Each correct generatrix will normally contain a greater and better assortment of high-frequency letters than the other generatrices and thus is distinguishable. To reconstitute the plaintext, the selected generatrices are reordered according to their order of appearance in the ciphertext. To show this process, the example cryptograms will again be used. In this instance the first 50 letters, decimated at the period of five, is set down in columnar form, each column conforming to the use of one cipher alphabet as shown in figure 13–5.

Gen.	Alphabet 1	Alphabet 2	Alphabet 3	Alphabet 4	Alphabet 5
1	AJZJNEZAIJ	UAYMFTHYLK	KMMIMIBMVU	HKWGLMHZMT	YIMXXIRMEG
2	*BKAKOFABJK*	*VBZNGUIZML*	*LNNJNJCNWV*	*ILXHMNIANU*	*ZJNYYJSNFH*
3	*CLBLPGBCKL*	*WCAOHVJANM*	*MOOKOKDOXW*	*JMYINOJBOV*	*AKOZZKTOGI*
4	*DMCMQHCDLM*	*XDBPIWKBON*	*NPPLPLEPYX*	*KNZJOPKCPW*	*BLPAALUPHJ*
5	ENDNRIDEMN	*YECQJXLCPO*	*OQQMQMFQZY*	*LOAKPQLDQX*	*CMQBBMVQIK*
6	*FOEOSJEFNO*	*ZFDRKYMDQP*	*PRRNRNGRAZ*	*MPBLQRMERY*	*DNRCCNWRJL*
7	*GPFPTKFGOP*	*AGESLZNERQ*	*QSSOSOHSBA*	*NQCMRSNFSZ*	*EOSDDOXSKM*
8	*HQGQULGHPQ*	*BHFTMAOFSR*	*RTTPTPITCB*	ORDNSTOGTA	*FPTEEPYTLN*
9	*IRHRVMHIQR*	*CIGUNBPGTS*	*SUUQUQJUDC*	*PSEOTUPHUB*	*GQUFFQZUMO*
10	*JSISWNIJRS*	*DJHVOCQHUT*	*TVVRVRKVED*	*QTFPUVQIVC*	*HRVGGRAVNP*
11	*KTJTXOJKST*	*EKIWPDRIVU*	*UWWSWSLWFE*	*RUGQVWRJWD*	*ISWHHSBWOQ*
12	*LUKUYPKLTU*	*FLJXQESJWV*	*VXXTXTMXGF*	*SVHRWXSKXE*	*JTXIITCXPR*
13	*MVLVZQLMUV*	*GMKYRFTKXW*	*WYYUYUNYHG*	*TWISXYTLYF*	*KUYJJUDYQS*
14	*NWMWARMNVW*	*HNLZSGULYX*	*XZZVZVOZIH*	*UXJTYZUMZG*	*LVZKKVEZRT*
15	*OXNXBSNOWX*	*IOMATHVMZY*	*YAAWAWPAJI*	*VYKUZAVNAH*	*MWALLWFASU*
16	*PYOYCTOPXY*	*JPNBUIWNAZ*	*ZBBXBXQBKJ*	*WZLVABWOBI*	*NXBMMXGBTV*
17	*QZPZDUPQYZ*	*KQOCVJXOBA*	*ACCYCYRCLK*	*XAMWBCXPCJ*	*OYCNNYHCUW*
18	*RAQAEVQRZA*	*LRPDWKYPCB*	*BDDZDZSDML*	*YBNXCDYQDK*	*PZDOOZIDVX*
19	*SBRBFWRSAB*	*MSQEXLZQDC*	CEEAEATENM	*ZCOYDEZREL*	*QAEPPAJEWY*
20	*TCSCGXSTBC*	NTRFYMARED	*DFFBFBUFON*	*ADPZEFASFM*	*RBFQQBKFXZ*
21	*UDTDHYTUCD*	*OUSGZNBSFE*	*EGGCGCVGPO*	*BEQAFGBTGN*	*SCGRRCLGYA*
22	*VEUEIZUVDE*	*PVTHAOCTGF*	*FHHDHDWHQP*	*CFRBGHCUHO*	*TDHSSDMHZB*
23	*WFVFJAVWEF*	*QWUIBPDUHG*	*GIIEIEXIRQ*	*DGSCHIDVIP*	UEITTENIAC
24	*XGWGKBWXFG*	*RXVJCQEVIH*	*HJJFJFYJSR*	*EHTDIJEWJQ*	*VFJUUFOJBD*
25	*YHXHLCXYGH*	*SYWKDRFWJI*	*IKKGKGZKTS*	*FIUEJKFXKR*	*WGKVVGPKCE*
26	*ZIYIMDYZHI*	*TZXLESGXKJ*	*JLLHLHALUT*	*GJVFKLGYLS*	*XHLWWHQLDF*

Figure 13–5 (~~C~~). Completion of the plain component, text arranged by period (U).

When the high-frequency generatrices underlined above are set down in columns, the now consecutive letters of intelligible plaintext are readily recognizable.

1	2	3	4	5	ALPHABET
5	20	19	8	23	GENERATRIX
E	N	C	O	U	
N	T	E	R	E	
D	R	E	D	I	
N	F	A	N	T	
R	Y	E	S	T	
I	M	A	T	E	
D	A	T	O	N	
E	R	E	G	I	
M	E	N	T	A	
N	D	M	A	C	

13-5. (~~C~~) Selection of Generatrices

a. The foregoing demonstrates how quickly a solution may be reached using this technique once the system has been identified and the period determined. However, the real key to the solution lies in the selection of the correct generatrix from each alphabetic column. As shown, it was selected on the basis of the appearance of high-frequency letters in the generatrix. Another method of selection may be used which involves a more systematic approach than mere visual inspection, again using frequency characteristics of plaintext. The probability of the low-frequency letters J, K, Q, X, and Z appearing two or more times in a given generatrix is unlikely so they may be immediately dropped from consideration. For example, the generatrices of alphabet 1 shown crossed out in figure 13-6 could be dropped.

Gen.	ALPHABET 1
1	~~A J Z J N E Z A I J~~
2	~~B K A K O F A B J K~~
3	C L B L P G B C K L
4	D M C M Q H C D L M
5	E N D N R I D E M N
6	F O E O S J E F N O
7	G P F P T K F G O P
8	~~H Q G Q U L G H P Q~~
9	I R H R V M H I Q R
10	~~J S I S W N I J R S~~
11	~~K T J T X O J K S T~~
12	~~L U K U Y P K L T U~~
13	~~M V L V Z Q L M U V~~
14	N W M W A R M N V W
15	~~O X N X B S N O W X~~
16	P Y O Y C T O P X Y
17	~~Q Z P Z D U P Q Y Z~~
18	~~R A Q A E V Q R Z A~~
19	S B R B F W R S A B
20	T C S C G X S T B C
21	U D T D H Y T U C D
22	V E U E I Z U V D E
23	W F V F J A V W E F
24	~~X G W G K B W X F G~~
25	~~Y H X H L C X Y G H~~
26	~~Z I Y I M D Y Z H I~~

Figure 13-6 (~~C~~). Generatrix identification (U).

Gen.	ALPHABET 1	SUM TOTALS
1	~~A-J-Z-J-N-E-Z-A-I-J~~	
2	~~B-K-A-K-O-F-A-B-J-K~~	
3	C L B L P G B C K L	0
4	D M C M Q H C D L M	0
5	E N D N R I D E M N	7
6	F O E O S J E F N O	7
7	G P F P T K F G O P	2
8	~~H-Q-G-Q-U-L-G-H-P-Q~~	
9	I R H R V M H I Q R	5
10	~~J-S-I-S-W-N-I-J-R-S~~	
11	~~K-T-J-T-X-O-J-K-S-T~~	
12	~~L-U-K-U-Y-P-K-L-T-U~~	
13	~~M-V-L-V-Z-Q-L-M-U-V~~	
14	N W M W A R M N V W	4
15	~~O-X-N-X-B-S-N-O-W-X~~	
16	P Y O Y C T O P X Y	3
17	~~Q-Z-P-Z-D-U-P-Q-Y-Z~~	
18	~~R-A-Q-A-E-V-Q-R-Z-A~~	
19	S B R B F W R S A B	5
20	T C S C G X S T B C	4
21	U D T D H Y T U C D	2
22	V E U E I Z U V D E	4
23	W F V F J A V W E F	2
24	~~X-G-W-G-K-B-W-X-F-G~~	
25	~~Y-H-X-H-L-G-X-Y-G-H~~	
26	~~Z-I-Y-I-M-D-Y-Z-H-I~~	

Figure 13–7 (C). Generatrix identification using arbitrary values (U).

b. The choice of generatrices is now considerably lessened by the elimination of the generatrices lined through. The choice can now be further reduced by assigning an arbitrary value of 1 to each of the normal high-frequency letters E T N R O A I S and ϕ to all others. By summing the values, an indication of the correct generatrix is then given. For an example of this note, figure 13–7.

The choice of either generatrix 5 or 6 is obvious. The exact determination of which to use is made by a comparison of generatrices selected by the same process from the other plain component columns.

13–6. (C) Logarithmic Test for Generatrix Selection

a. A somewhat more precise method of determining the correct sequence by measurement may be arrived at by using the logarithmic weights of plain English reproduced below:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
8	4	7	7	9	6	5	7	8	1	2	7	6	8	8	6	2	8	8	9	6	5	5	3,	6	0

b. These values are based on the relative frequency of each letter in telegraphic text and therefore are especially effective where the generatrix contains very few values. The procedure for testing the probability of the correct generatrix is essentially the same as that given in the preceding example. A portion of the ciphertext sufficient in size to produce recognizable plaintext is decimated to form a base composed of the cipher values of one period. A column of generatrices is then produced by completing the plain component. Each generatrix of that column then is tested by summing the total values assigned to each of its letters by the values shown above. The generatrix then showing the highest total value is considered the best probability. Upon the selction of a generatrix from each plain component column, the letters are juxtaposed at the interval corresponding to the period to produce plaintext. Of course where doubt exists between several generatrices they may be played against each other to determine the correct one to use.

c. A modification of this system and the one preceding it is to combine the two tests. The first, which is much quicker, may be used to initially select those generatrices which are easy to identify because of their own make up of letters. This test then can be used to select one generatrix from those previously isolated which would not be readily identifiable by the simpler method.

13–7. (C) Theory of Probable Word Method

a. The probable word method, similar to that used in monoalphabetic substitution, may be used to effect a solution where the foregoing methods are of no avail, or where there is an insufficiency of external evidence to indicate the number of alphabets involved. This method is predicated on the use of a plaintext word or words as the cryptographic key and may be used when standard or known mixed alphabets are used.

b. Essentially the method consists of assuming the presence of a word in the text of the message.

The word is then fitted in turn at various positions in the message. At each point a plain and cipher sequence is juxtaposed to produce the observed cipher values. If the probable word is correct and is placed in the correct position of the message, the key letters produced by the juxtaposed plain and cipher sequences will yield a plaintext keyword. To demonstrate the theory of the solution, the following short message will be used.

PGSGG DNRUH VMBGR YOUUC WMSGL VTQDO

c. Assuming that the word REGIMENT appears in the above cipher and that it was produced using reversed standard alphabets, it may be set down as follows:

(1) The plaintext is set beneath the ciphertext as shown to the right:

```
P G S G G D N R
R E G I M E N T
```

(2) Using two sliding strips, one direct as the plain sequence, the other reversed as the cipher sequence, they are juxtaposed so as to produce the equivalent cipher-plaintext values shown.

```
      (i)
P     A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
C     G F E D C B A Z Y X W V U T S R Q P O N M L K J I H
      (k)
```

Thus for the first equivalency the key letter shown below is produced:

```
C     P G S G G D N R
P     R E G I M E N T
K     G
```

(3) The same two strips are now repositioned to where Ep=*Gc*, and the second key letter derived.

```
P     A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
C     K J I H G F E D C B A Z Y X W V U T S R Q P O N M L
C     P G S G G D N R
P     R E G I M E N T
K     G K
```

(4) The same process is continued for each letter until all the key letters are determined. A continuation of the process will result in the following:

```
C     P G S G G D N R
P     R E G I M E N T
K     G K Y O S H A K
```

Obviously the key so produced does not result in an intelligible word so the assumed word is shifted one position to the right relative to the text and the process repeated. This trial, using the same sliding strips juxtaposed as appropriate, results in:

```
C     G S G G D N R U
P     R E G I M E N T
K     X W M O P R E N
```

(5) Again an intelligible keyword is not produced; therefore continue to shift the probable word to the right, one letter at a time, each time deriving a possible key. When the point of juxtaposition shown below is reached, a keyword becomes evident.

```
P G S G G D N R U H V M B G R Y O W U C W M S G L V T Q D O
                R E G I M E N T
                L L B U N K E R
```

d. It should be noted that the key is a cyclic permutation of BUNKER HILL. Since the keyword or phrase repeats itself during the encipherment of a message it will appear periodically throughout the message determined by the position of the probable word in the text. Thus the keyword may well appear as a cyclic permutation, complete or in part.

13–8. (~~C~~) Application of the Probable Word Method

a. In actual practice the application follows somewhat different lines. Using the previous example this can be seen in the following. First the message is written horizontally on cross-section paper and the probable word is written in a column, one space below and to the left of the ciphertext as shown in figure 13–8.

	P	G	S	G	G	D	N	R	U	H	V	M	B	G	R	Y	O	U	U	C	W	M	S	G	L	V	T	Q	D	O
R	x								x								x													
E		x								x								x												
G			x								x								x											
I				x								x								x										
M					x								x								x									
E						x								x								x								
N							x								x								x							
T								x								x								x						

Figure 13–8 (~~C~~). Location of probable word (U).

b. If the probable word assumed does exist in the message it may be located beginning at any one of the positions indicated by an x in the matrix above. Rp being the equivalent of the cipher value appears in the text directly above that point. Moreover, the remaining letters of the probable word are represented by the cipher letter to the right of that point. Thus if the key is a plaintext word or a phrase it will appear long the diagonal line, as this diagonal represents the successive encipherment of the probable word. The possible cyclic permutations of the keyword can be noted in the diagonal arrangement of the x's.

c. Again two alphabetic strips, one direct, and one reversed, to correspond with the .previous assumption that a reversed standard alphabet is involved, are used. However, since we have assumed that a plaintext word or phrase is being used as a keyword, it is not necessary to derive the key letter of each juxtaposition. Only the amount needed to prove the unacceptability of the relative location of the probable word to a position in the ciphertext is required. This being predicated on the proposition that an incorrect position and the consequent derivation of key letters will produce impossible combinations of letters for a keyword. With this in mind, the strip may be juxtaposed and the keys shown in figure 13–9 below derived.

	P	G	S	G	G	D	N	R	U	H	V	M	B	G	R	Y	O	U	U	C	W	M	S	G	L	V	T	Q	D	O
R	G	X	J	X	X	U	E	I	L	Y	M	D	S	X	I	P	F	L	L	T	N	D	J							
E		K	W	K	K	H	R	V	Y	L	Z	Q	F	K	V	C	S	Y	Y	G	A	Q	W	K						
G			Y	M	M	J	T	X	A	N	B	S	H	M	X	E	U	A	A	I	C	S	Y	M	R					
I																														
M																														
E																														
N																														
T																														

Figure 13–9 (~~C~~). Key derivation (U).

d. Examination of the trigraphs occurring along the diagonal, produced by successive juxtaposition of the two sequences, reveals several which may represent a portion of a keyword. For example, note the trigraphs EVA, LLB, XVE, ICU, PSA, LYI, and TAS which appear on the basis of vowel-consonant combinations to represent part of a possible keyword. However, it is also important to remember that seemingly improbable combinations, due to cyclic permutation, may well be the true keyword as in the case of the trigraph LLB appearing under UC above. At this point the analyst needs only to complete those diagonals which show possibilities of containing a keyword, again finding the same keyword. This is illustrated in figure 13–10.

	P	G	S	G	G	D	N	R	U	H	V	M	B	G	R	Y	O	U	U	C	W	M	S	G	L	V	T	Q	D	O
R	G	X	J	X	X	U	E	I	L	Y	M	D	S	X	I	P	F	L	L	T	N	D	J							
E		K	W	K	K	H	R	V	Y	L	Z	Q	F	K	V	C	S	Y	Y	G	A	Q	W	K						
G			Y	M	M	J	T	X	A	N	B	S	H	M	X	E	U	A	A	I	C	S	Y	M	R					
I										P		U					W	C	C		E		A							
M											H		N							O				S						
E														K																
N															E															
T																R														

Figure 13–10 (~~C~~). Key derivation, step 2 (U).

e. Once the keyword has been found, solution is a simple matter, for the process of determining the keyword has of itself proved the assumption concerning the structure of the alphabet used. In this case a matrix is constructed containing one standard alphabet as the plain component and seven reversed standard alphabets as the cipher sequence juxtaposed to form the keyword BUNKER HILL below A of the plain. With this, the ciphertext can be deciphered to read:

"MOVE YOUR REGIMENT TO RJ FIVE TWO SIX."

f. In the foregoing a whole cryptogram was used for example purposes. However, the technique may be applied to a portion of a longer cryptogram. In this case only a few prerequisites are required. First, a reasonably accurate probable word, then an idea of where this word is located in the message. Then, by trial and error as shown above, the keyword can be derived. Further, although the example above used a reversed standard cipher sequence, the method is equally applicable to cases where a direct standard sequence is used, and also when a mixed sequence is used, if it is a known sequence, and the repeating key begins under Ap.

Section II. (~~C~~) SYSTEMS USING MIXED CIPHER ALPHABETS

13–9. (~~C~~) Characteristics of Mixed Alphabets

a. Polyalphabetic systems which use standard alphabets as cipher and plain sequences, because of their inherent simplicity, are not widely used. The reason for their vulnerability to analysis is threefold. First, only relatively few alphabets are normally used. Second, in this type system they are used periodically, imparting the cyclic phenomena in the text which in turn provides the means of determining the number of alphabets involved. Third, the alphabets used are known alphabets, i.e. the relative sequence of their individual letters are known. This with a limited number of alphabets greatly simplifies the process of equating cipher and plaintext values.

b. In preceding paragraphs, when monoalphabetic substitution using mixed alphabets was discussed, it was pointed out that the use of mixed alphabets greatly increased the difficulty of solution. So it also is in the case of polyalphabetic substitution. However, there are certain characteristics in the type mixed alphabets used which permits a fairly easy solution.

c. In paragraph 12–4 the common configurations of primary components, and of the derived secondary alphabets, used as cipher alphabets were given. In the preceding section, case I was used and the analysis based on the characteristics of those secondary alphabets produced in that case. In this section, alphabets of case II will be treated and their characteristics exploited as the basis for analysis.

d. Alphabets of case II are those whose primary components are not both normal sequences. That is, the plain component may be a standard alphabet and the cipher component a mixed sequence; or the plain component may be a mixed alphabet and the cipher component a normal alphabet. In either case the resulting secondary alphabets are mixed alphabets. An example of the former configuration may be seen below in figure 13–11.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1	B	C	D	F	G	I	J	K	M	P	Q	S	U	X	Y	Z	L	E	A	V	N	W	O	R	T	H
C2	L	E	A	V	N	W	O	R	T	H	B	C	D	F	G	I	J	K	M	P	Q	S	U	X	Y	Z
C3	U	X	Y	Z	L	E	A	V	N	W	O	R	T	H	B	C	D	F	G	I	J	K	M	P	Q	S
C4	E	A	V	N	W	O	R	T	H	B	C	D	F	G	I	J	K	M	P	Q	S	U	X	Y	Z	L

Figure 13–11 (~~C~~). Case II secondary alphabets (U).

13–10. (~~C~~) Direct Symmetry of Position

a. The secondary alphabets above were produced by a juxtaposition of two alphabets. A standard sequence as the plain component and 4 of a possible 26 positional juxtapositions of a keyword mixed alphabet based on the keyword LEAVENWORTH. The four shown, as well as the other 22 possible are in reality only one sequence, each being displaced relative to the plain component. Thus in each a direct symmetry exists, i.e. in each sequence the individual letters follow one another in a fixed order at a fixed distance. Since each cipher sequence is offset a predetermined distance from the index letter of the plain component, symmetry exists between the individual letters of each sequence.

b. The implication of this direct symmetry of position can be shown in the example below. Let us first assume that in the course of analysis of a polyalphabetic cipher that we have determined that a period of four is being used, that the cipher sequence used is mixed, and further that the following values have been recovered.

ALPHABET 1
Ep=*Gc* Op=*Yc* Tp=*Vc*
ALPHABET 2
Ep=*Nc* Op=*Gc* Tp=*Pc*
ALPHABET 3
Ep=*Lc* Op=*Bc* Tp=*Ic*
ALPHABET 4
Ep=*Wc* Op=*Ic* Tp=*Qc*

The equivalencies shown for the secondary alphabets can be set down in a matrix reconstruction diagram as shown in figure 13–12.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1					G										Y					V						
C2					N										G					P						
C3					L										B					I						
C4					W										I					Q						

Figure 13–12 (~~C~~). Letter placement, direct symmetry of position (U).

c. As the individual letters of a mixed sequence follow one another in a fixed order and as each secondary alphabet is the same in respect to the sequence of their letters, only positioned at different points, it follows then that the letters of one can be transferred to another on the basis of constant distance and sequence. For example, in cipher sequence 1 above, *Gc*, *Yc*, and *Vc* are noted in sequence at 10 and 5 letters distance respectively. This same sequence then can be transferred to cipher sequence 2 where a *Gc* also appears. By counting 10 spaces to the right of *Gc*, *Yc* can be inserted below Yp. Continuing the count around the alphabet, *Vc* can be located below Dp. For example, note the placement of the values in figure 13–13.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1					G										Y					V						
C2				V	N										G					P					Y	
C3					L										B					I						
C4					W										I					Q						

Figure 13–13 (~~C~~). Placement transfer, direct symmetry of position (U).

d. By continuing the process of the reconstruction of the secondary alphabets through the principle of direct symmetry of position, the following additional placements can be made as shown in figure 13–14. Note that two elements must be known. First and foremost, one of the components, the cipher or the plain, must be a known sequence. It is unimportant whether it is mixed or standard, only the the exact sequential progression of the letters be known. If either is unknown, direct symmetry even if present, cannot be detected. Secondarily, given one known sequence where the other is unknown, only a few equivalencies are required to use the principle of direct symmetry.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1					G					P					Y					V	N					
C2				V	N										G					P					Y	
C3					L					W					B					I					Q	
C4					W					B					I					Q						L

Figure 13–14 (~~C~~). Placement transfer (U).

e. The importance of direct symmetry of position in the analysis of a cryptogram should be obvious. The new values for each cipher alphabet discovered by the process can of course be inserted in the ciphertext, thereby leading to the recovery of further cipher to plain equivalents. This in turn enables the analyst to further develop his matrix reconstruction diagram. In short, it has a snowballing effect, each step leading to additional recovery until a final solution is reached.

13–11. (~~C~~) Preliminary Steps

a. In the solution of polyalphabetic ciphers using mixed alphabets, the same general preliminary techniques as those previously given are followed prior to the exploitation of the characteristic of direct symmetry. Assuming that a cryptogram has been identified tentatively as polyalphabetic, it is laid out and repeats are underlined as in figure 13–15.

```
            5          10          15          20          25
A   Q W B R I   V W Y C A   I S P J L   R B Z E Y   Q W Y E U
B   L W M G W   I C J C I   M T Z E I   N I B K N   Q W B R I
C   V W Y I G   B W N B Q   Q C G Q H   I W J K A   G E G X N
D   I D M R U   V E Z Y G   Q I G V N   C T G Y C   B P D B L
E   V C G X G   B K Z Z G   I V X C U   N T Z A O   B W F E Q
F   Q L F C O   M T Y Z T   C C B Y Q   O P D K A   G D G I G
G   V P W M R   Q I I E W   I C G X G   B L G Q Q   V B G R S
H   M Y J J Y   Q V F W Y   R W N F L   G X N F W   M C J K X
J   I D D R U   O P J Q Q   Z R H C N   V W D Y Q   R D G D G
K   B X D B N   P X F P U   Y X N F G   M P J E L   S A N C D
L   S E Z Z G   I B E Y U   K D H C A   M B J J F   K I L C J
M   N F D Z T   C T J R D   M I Y Z Q   A C J F R   S B G Z N
N   Q Y A H Q   V E D C Q   L X N C L   L V V C S   Q W B I I
P   I V J R N   W N B R I   V P J E L   T A G D N   I R G Q P
Q   A T Y E W   C B Y Z T   E V G Q L   V P Y H L   L R Z N Q
R   X I N B A   I K W J Q   R D Z F Y   K W F Z L   G W F J Q
S   Q W J Y Q   I B W R X
```

Figure 13–15 (~~C~~). Ciphertext prepared for analysis (U).

b. Once the repeated groups of letters are underlined, they are extracted, set in columnar form, the intervals noted, and the factors derived. Note that, in figure 13–16 only the factors to 26 are included. Beyond that, additional factors would be merely repeated cycles of the basic 26 possible alphabets.

POLYGRAPH	INTERVAL	FACTORS
QWBRIVWY	45	3, 5, 9, 15
CGXGB	60	2, 3, 4, 5, 6, 10, 12, 15, 20
PJEL	95	5, 19
ZZGI	145	5
BRIV	330	2, 3, 5, 6, 10, 11, 15, 22
BRIV	285	3, 5, 15, 19
KAG	75	3, 5, 15, 25
QRD	165	3, 5, 15
QWB	45	3, 5, 9, 15
QWB	275	5, 11, 25
WIC	130	2, 5, 10, 13, 26
XNF	45	3, 5, 9, 15
YZT	225	3, 5, 15, 25
ZTC	145	5

Figure 13–16 (~~C~~). Determination of period (U).

The constant factor of five is indicative that all repeated appearances are probably causal rather than accidental. Further, their number and size reinforces this assumption. Therefore it may be accepted that the period, i.e. the number of alphabets, is five.

c. Having determined a probable period length the next step is to make a distribution of the ciphertext, one for each period in order to ascertain the type of alphabet involved, see figure 13–17.

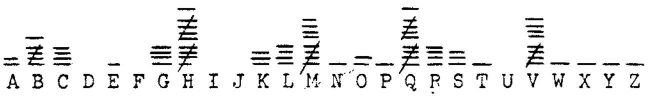


Figure 13–17 (U). Uniliteral frequency distribution alphabet 1 (U).

In this case the distribution of alphabet 1 is indicative that the period of five is a correct assumption. If further confirmation is required, a similar distribution for each alphabet could be made and the statistical tests previously explained could be used as confirmation. This is the accepted procedure in most cases. However, accepting the assumed period, the distribution is compared to the normal. In this comparison, two facts should immediately become apparent. First, the pronounced peaks and troughs are indicative of monoalphabetic substitution, as it should be, assuming the period to be correct. Yet the spatial relationship between the peaks and troughs does not conform to the normal. That is, it cannot be fitted to the normal. Thus, the use of mixed sequences is indicated.

d. If the distribution cannot be fitted to the normal, recovery of each value in each alphabet then must be determined on an individual basis. Later, as values are inserted in the text, additional values may be assumed on word patterns, probable words, etc. This individual identification may be accomplished through a study of frequencies of occurrence, a study of a triliteral frequency distribution, or even a study of repetitions and assumptions based thereon. However, for reasons previously explained, it is best to consider all factors. Accordingly, it then becomes necessary to develop a triliteral frequency distribution.

e. A triliteral frequency distribution made of a polygraphic cipher must be somewhat different than that made previously in the case of monoalphabetic substitution systems. It must show each letter prefix and suffix, and yet account for the fact that there are a number of different alphabets involved. In order to do this, one distribution must be made for each cipher alphabet. In this case, since the period length conforms to group size, each successive letter of each group is listed in its own distribution, the letter preceding and following it is listed below in columnar form as a diagraph. Thus a frequency distribution for each alphabet and a triliteral distribution involving three different alphabets is combined. In the example shown below note that the horizontal line A–Z represents those letters from the first alphabet. The prefix and suffix listed below each letter represents letters of the 5th and 2nd alphabets. Thus for reference purpose *QAC*, the first trigraph of alphabet 1, may be annotated 512, as may all
Q A C
trigraphs from that distribution. In like manner the following patterns apply.

Alphabet 2 1 2 3
S A N
Alphabet 3 2 3 4
Y A H
Alphabet 4 3 4 5
Z A O
Alphabet 5 4 5 1
C A I

Note that the annotated numbers are merely a cyclic permutation of the periodic sequence 1–2–3–4–5. Thus the completed triliteral distribution would appear as shown in figures 13–18① through 13–18⑤.

Alphabet 1

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
QC	*GW*	*NT*		*TV*		*AE*		*AS*		*UD*	*UW*	*IT*	*UT*	*QP*	*NX*	*-W*	*LB*	*LA*	*LA*		*IW*	*NN*	*QI*	*UX*	*QR*
PT	*OP*	*TC*				*AD*		*WC*		*FI*	*QX*	*II*		*UP*		*YW*	*YW*	*DE*			*IW*				
	GK	*TT*				*LX*		*HW*		*FW*	*LV*	*OT*				*NW*	*QD*	*RB*			*UE*				
	OW	*WB*				*LW*		*ND*			*LR*	*SY*				*QC*	*QD*				*LC*				
	GL							*GV*				*WC*				*GI*					*GP*				
	GX							*WC*				*GP*				*QL*					*QB*				
								XD				*AB*				*RI*					*NW*				
								GB				*JF*				*YV*					*QE*				
								IV				*DI*				*NY*					*IP*				
								NR								*SW*					*UP*				
								AK								*QW*									
								QB																	

Figure 13–18① (~~C~~). Triliteral frequency distribution, alphabet 1 (U).

Alphabet 2

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
SN	RZ	IJ	IM	GG	MD			MB		IW	QF		WB		BD		ZH	IP	MZ		IX	QB	GN	MJ	
TG	VG	QG	GG	VZ				QG		BZ	BG				OD		IG		CG		QF	VY	BD	QA	
	IE	VG	ID	SZ				QI							VW		LZ		NZ		LV	QY	PF		
	MJ	CB	RG	VD				KL							OJ				MY		IJ	LM	YN		
	SG	IG	KH					MY							MJ				CJ		EG	QB	LN		
	CY	MJ	RZ					XN							VJ				AY			VY			
	IW	AJ													VY							BN			
																						IJ			
																						BF			
																						RN			
																						VD			
																						QB			
																						KF			
																						GF			
																						QJ			

Figure 13–18② (~~C~~). *Triliteral frequency distribution, alphabet 2* (*U*).

Alphabet 3

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
YH	WR		PB	BY	WE	CQ	RC	IE	CC		IC	WG	WB		SJ						WV	PM	VC	WC	BE
	IK		PK		LC	EX	DC		WK			DR	WF									KJ		WE	TE
	WR		DR		VW	IV			YJ				XF									BR		WI	EY
	CY		WY		XP	TY			CK				XF											TZ	KZ
	WI		XB		WZ	CX			PQ				AC											IZ	TA
	NR		FZ		WJ	DI			PE				XC											TE	EZ
			EC			CX			PJ				IB											BZ	RN
						LQ			TR															PH	DY
						BR			CR																
						DD			VR																
						BZ			PE																
						AD			WY																
						RQ																			
						VQ																			

Figure 13–18③ (~~C~~). *Triliteral frequency distribution, alphabet 3* (*U*).

Alphabet 4

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ZO	NQ	YA	GG	ZY	NL	MW	AQ	YG	PL	BN		WR	ZQ		FU	GH	BI				GN	FY	GN	ZG	ZG
	DL	JI	GN	YU	NW		XL	GG	JY	JA						GQ	BI						GG	GO	YT
	DN	XU		ZI	NG			BI	JF	DA						JQ	MU						GG	BQ	ZG
	NA	FO		FQ					WQ	JX						GP	GS							DQ	DT
		HN		IW					FQ							GU	DU							EU	YQ
		ND		JL													JD							ZF	GN
		HA		JL													JR							JQ	YT
		LJ		YW													JN								FL
		DQ															BI								
		NL															WX								
		VS																							

Figure 13–18④ (~~C~~). *Triliteral frequency distribution, alphabet 4* (*U*).

Alphabet 5

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
CI			*CS*		*JK*	*IB*	*QI*	*RV*	*CM*		*JR*		*KQ*	*YB*	*QA*	*BQ*	*MQ*	*RM*	*ZC*	*EL*		*GI*	*KI*	*EQ*	
KG			*RM*		*YK*	*YQ*		*CM*			*BV*		*XI*	*AB*		*EQ*	*RS*	*CQ*	*ZC*	*RV*		*EI*	*R-*	*JQ*	
KG						*XB*		*EM*			*FG*		*VC*	*CM*		*YO*			*ZE*	*CN*		*FM*		*WR*	
CM						*ZI*		*RV*			*ES*		*CV*			*QV*				*RO*		*EC*			
BI						*IV*		*II*			*CL*		*BP*			*QZ*				*PY*					
						XB		*RV*			*ET*		*ZQ*			*YR*				*YK*					
						DB					*HL*		*RW*			*ZA*				*QV*					
						FM					*ZG*		*DI*			*HV*									
						ZI										*CL*									
																NX									
																JR									
																JQ									
																YI									

Figure 13–18⑤ (~~C~~). Triliteral frequency distribution, alphabet 5 (U).

f. In addition to the triliteral frequency distribution a condensed table of repetitions is prepared in .which all polygraphs are listed and the alphabet of each letter is indicated. A format of this is shown in figure 13–19.

```
1 2 3 4 5 1 2 3
Q W B R I V W Y-2
Q W B          -3
Q W            -5
V P            -3
V W            -3

3 4 5 1
B R I V-3
Z Z G I-2
Y Z T  -2
B R    -3
G Q    -4
G X    -3
J R    -3
N F    -3
Y Z    -3

4 5 1
K A G-2
Z T C-2
R I  -3
Y Q  -3
Z T  -3
```

```
2 3 4 5 1
C G X G B-2
P J E L  -2
X N F    -2
C G      -3
C J      -3
P J      -3
W B      -3
W F      -3
W Y      -3
X N      -3

5 1 2
Q R D-2
W I C-2
G B  -4
I V  -3
Q Q  -3
```

Figure 13–19 (~~C~~). Condensed table of repetitions (U).

13–12. (~~C~~) Identification of Cipher Values

a. With the completion of the preliminary step, the analysis of the cryptogram may now begin. Using the same analytic techniques as were used in the case of mixed monoalphabetic ciphers, one now attempts to establish the identification of cipher values, doing this for each alphabet. The first step is to separate the vowels from the consonants—through frequency of occurrence alone, or by the consonant line method in doubtful cases. On the basis of the former it appears that $\overset{2}{\overline{W}}c$ and $\overset{5}{\overline{Q}}c$ are the equivalents of Ep. In the other alphabets this distinction is not so clear-cut. Using the same yardstick of frequency as a measure $\overset{1}{\overline{I}}c$, $\overset{3}{\overline{G}}c$, and $\overset{4}{\overline{C}}c$ appear as likely candidates for Ep.

b. In paragraph 13–11*e* it was stated that the triliteral distribution of alphabet 1 represents the letters of alphabets 512 as prefix, base, and suffix letters respectively. As the cipher value of Ep has been assumed with some certainty for alphabets 2 and 5 ($\overset{2}{\overline{W}}c$ and $\overset{5}{\overline{Q}}c$), we may use this to determine the vowels and consonants of alphabet 1. The basis for the identification being the familiar diagraph permutations of E, that is:

E as beginning letter	E D	E N	E R	E S		1
E as ending letter		N E	R E	S E	T E V E	1

In terms of the 512 pattern, possible cipher to plain equivalencies may be set down as illustrated in figure 13–20.

51	51	51	51
EDp	ENp	ERp	ESp
Q-c	*Q-c*	*Q-c*	*Q-c*

12	12	12	12	12
NEp	REp	SCp	TEp	VEp
-Wc	*-Wc*	*-Wc*	*-Wc*	*-Wc*

Figure 13–20 (~~C~~). *Identification of cipher to plain equivalencies* (*U*).

Thus it can be seen that some of the high frequency letters of alphabet 1; *I, M, Q, V, B, G, L, R, S,* and *C* respectively, probably represent the plaintext consonants D, N, R, S, T, and V. Moreover if the consonants can be identified, then the remaining high-frequency cipher letters of alphabet 1 most likely will be limited to vowels.

c. The prefixes of $\overset{2}{\overline{W}}c$ and the suffix of $\overset{5}{\overline{Q}}c$ (both assumed Ep) are shown in the following tabulation figure 13–21, drawn from the triliteral distribution of alphabet 1.

Prefixes of $\overset{2}{\overline{W}}c$

Q	*G*	*K*	*V*	*R*	*B*	*I*	*L*	*C*
𝍸	–	–	≡	–	=	–	–	

Suffixes of $\overset{5}{\overline{Q}}c$

I	*Q*	*R*	*X*	*L*	*V*	*A*	*Z*	*O*
–	≡	=	–		=	–	–	–

Figure 13–21 (~~C~~). *Identification of vowels and consonants* (*U*).

Using the data established, it is now possible to study the high-frequency letters, I, M, Q, V, B, G, L, R, S, and C of alphabet 1 in turn, to determine their identity as either a vowel or consonant, and perhaps ascertain their exact plaintext value.

(1) $\overset{1}{\overline{I}}c$ previously established as a possible cipher value for Ep may be set aside immediately.

(2) $\overset{2}{\overline{M}}c$ is noted as not appearing either as a suffix or prefix in the tables above which indicates that it may be a vowel. Moreover its frequency tends credence to this. If it is a vowel, it may well be Op, as Ep has been excluded, though its identification as either an Ip or Ap cannot yet be discounted.

(3) $\overset{1}{\overline{Q}}c$ is observed five times as a prefix of $\overset{2}{\overline{W}}c$ and three times as a suffix of $\overset{5}{\overline{Q}}c$. The frequency of its combination with assumed Ep indicates both that it is probably a consonant and that it is the equivalent of Rp.

(4) The letter $\overset{1}{\overline{V}}c$ occurs three times as a prefix and twice as a suffix indicating that it, too, is probably a consonant. On the basis of its frequency it then may be assigned the plaintext value of T.

(5) The letter $\overset{1}{\overline{B}}c$ occurs only as a prefix of $\overset{2}{\overline{W}}c$, then only twice. As its frequency is neither low nor high, it may be a consonant.

(6) $\overset{1}{\overline{G}}c$ appears but once, as a prefix; its identity is questionable, though it may be either Ap or Ip.

(7) $\overset{1}{\overline{L}}c$ appears one time as both a prefix and a suffix, therefore it is probably a consonant, yet its exact identity cannot be ascertained.

(8) $\overset{1}{\overline{R}}c$, because it appears once as a prefix and twice as a suffix of the assumed Ep, is most certainly a consonant.

(9) Neither $\overset{1}{\overline{S}}c$ nor $\overset{1}{\overline{C}}c$ appears as a suffix or a prefix; therefore, both may be vowels or consonants, though a study of their combinations later, in other sequences, shows that $\overset{1}{\overline{C}}c$ may be a vowel leaving $\overset{1}{\overline{S}}c$ unclassified.

d. The same process is applied to each distribution in turn classifying the cipher letters either as vowels or consonants, and identifying specific plain to cipher values where possible. Also, as the process is continued, it then becomes possible to expand the classification and identification by playing one assumed value of one alphabet against an unidentified vowel or consonant in another, thus leading to additional identifications. The completed process could result in the following classification of vowels and consonants. Also previous identifications could be placed in a reconstruction matrix as shown in figure 13–22.

Alphabet	*Vowels*	*Consonants*
1	I, M, C	Q, V, B, L, R, G?
2	W, P, I	B, C, D, T
3	G, Z	J, N, D, Y, F
4	C; E?, R?, B?	Y, Z, J, Q
5	Q, U	G, N, A, I, W, L, T

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1	*C*				*I*										*M*			*Q*		*V*						
C2					*W*																					
C3					*G*																					
C4					*C*																					
C5					*Q*																					

Figure 13–22 (~~C~~). Reconstruction matrix (U).

13–13. (~~C~~) Application of the Principle of Direct Symmetry of Position

a. At first glance the values recovered to this point seem somewhat sketchy. However, on a closer examination the appearance of *Qc* in both alphabets 1 and 5 is noted as well as the *Cc* in alphabets 1 and 4. If the cipher system involves the use of one mixed component juxtaposed a number of times against a known standard sequence, the resultant secondary alphabets (cipher alphabets) can be recovered by applying the principle of direct symmetry of position presented above. If this is the case then the values of alphabet 1 can be transferred to alphabet 5 using the $\overset{5}{\overline{Q}}c$ as point of reference. It would appear as shown in figure 13–23.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1	*C?*				*I*				*C?*						*M*			*Q*		*V*						
C5		*M*			*Q*		*V*							*C?*				*I*				*C?*				

Figure 13–23 (C). Recovered value transfer (U).

b. This process immediately reveals three additional values; $\overset{5}{\overline{M}}c$=Bp, $\overset{5}{\overline{V}}c$= Gp, and $\overset{5}{\overline{I}}c$= Rp. Note that Bp and Gp are normally low-frequency letters. If the values derived by this process are correct, *Mc* and *Vc* of alphabet 5 should appear infrequently. A check of alphabet 5's distribution reveals that neither appear, which tends to support the assumption. Note that $\overset{5}{\overline{C}}c$ in alphabet 5 appears under Np and Vp. Both are consonants, but are significantly different in that if $\overset{5}{\overline{C}}c$=Np, H can be expected to appear quite frequently. If on the other hand $\overset{5}{\overline{C}}c$ is Vp it will appear infrequently. Examining the distribution for alphabet 5, it does not appear at all, therefore it must be equivalent of Vp rather than Np. The definite placement of $\overset{5}{\overline{C}}c$ now permits the placement of values in alphabet 4. The total values now consolidated in the reconstruction matrix appear in figure 13–24.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1					*I*				*C*						*M*			*Q*		*V*						
C2					*W*																					
C3					*G*																					
C4	*I*				*C*						*M*			*Q*		*V*										
C5		*M*			*Q*		*V*											*I*				*C*				

Figure 13–24 (~~C~~). Additional value placement (U).

c. At this point it is possible to transfer the values found to the cryptogram. It is possible to continue along the same lines, i.e. determining the value of individual cipher letters through association with those already found, confirmed by their use in other alphabets. However, with the number of values already recovered it may be more profitable to approach the problem directly through the analysis of word patterns in the ciphertext.

13–14. (~~C~~) Reconstruction of the Matrix

a. Using the partially recovered matrix, the following plaintext values can be inserted in the cipher work sheet (fig. 13–25).

```
        5       10       15       20       25

A   QWBRI   VWYCA   ISPJL   RBZEY   QWYEU
    RE  R   TE E    E               RE
B   LWMGW   ICJCI   MTZEI   MIBKN   QWBRI
     E      E  ER   O   R   O       RE  R
C   VWYIG   BWNBQ   QCGQH   IWJKA   GEGXN
    TE A     E  E   R EN    EE        E
D   IDMRU   VEZYG   QIGVN   CTGYO   BPDBL
    E       T       R EP    I E
E   VCGXG   BKZZG   IVXCU   NTZAO   BWFEQ
    T E             E  E             E  E
F   QLFCO   MTYZT   CCBYQ   OPDKA   GDGIG
    R  E    O   I   I   E             EA
G   VPWMR   QIIEW   ICGXG   BLGQQ   VBCRS
    T  K    R       E E       ENE   T E
H   MYJJY   QVFWY   RWNFL   GXNFW   MCJKX
    O       R        E              O
J   IDDRU   OPJQQ   ZRHCN   VWDYQ   RDGDG
    E          NE      E    TE  E     E
K   BXDBN   PXFPU   YXNFG   MPJEL   SANCD
                            O          E
L   SEZZG   IBEYU   KDHCA   MBJJY   KILCJ
            E          E    O          E
M   MFDZT   CTJRD   MIYZQ   ACJRR   SBGZN
    O       I       O   E             E
N   QYAHQ   VEDCQ   LXNCL   LVVCS   QWBII
    D   E   T  EE      E       E    RE AR
P   IVJRN   WNBRI   VPJEL   TAGDN   IRGQP
    E           R   T         E     E EN
Q   ATYEW   CBYZT   EVGQU   VPYHL   LRZNQ
            I         EN    T           E
R   XINBA   IKWJQ   RDZFY   KWFZL   GWFJQ
            E   E            E       E  E
S   QWJYQ   IBWRX
    RE  E   E
```

Figure 13–25 (C). Partially recovered plaintext (U).

b. Possible words are somewhat sketchy, but no impossible combinations are noted. Therefore the plaintext values would be carefully scanned in an attempt to locate possible words. In line A, a word fragment is at once noted.

```
           5        10        15
A   Q W B R I   V W Y C A   I S P J L
    R E - - R   T E - E     E
```

(1) The same pattern occurs on line B as:

```
    1 2 3 4 5   1 2 3 4 5   1 2 3 4 5
B   Q W B R I   V W Y I G   B W N B Q
    R E - - R   T E - A       E     E
```

Considering possible words which may be used as the beginning of a message, the word REPORT is quickly selected. Note that the E which follows it may be expanded to REPORTED. Thus the following cipher to plain value may be assumed.

$\frac{3}{Bc}=\text{Pp}$

$\frac{4}{Rc}=\text{Op}$

$\frac{3}{Yc}=\text{Dp}$

(2) A similar pattern is noted on line L

```
5   1 2 3 4 5   1
S   Q W B I I   I
    R E   A R   E
```

Having established the values of $\frac{3}{Bc}$ as Pp it leads immediately to the assumption that this plaintext fragment represents PREPARE and that $\frac{5}{Sc}=\text{Pp}$.

(3) Another pattern of interest occurs on lines E and F. Note the word fragment:

```
1 2 3 4 5   1 2 3 4 5
C D G I G   V P W M R
    E A     T     K
```

This may represent the word ATTACK, and if so the following values could be assumed:

$\frac{5}{Gc}=\text{Tp}$

$\frac{2}{Pc}=\text{Ap}$

$\frac{3}{Wc}=\text{Cp}$

The assumption that $\frac{5}{Gc}=\text{Tp}$ is confirmed at the second appearance of REPORTED. Note that this value completes the phrase REPORTED AT.

(4) Reexamining the text in light of the previous assumptions, additional values may be gleaned. For example, beginning at A9 another possible word is noted.

```
     1 0         1 5
A1   4 5   1 2 3 4 5
     C A   I S P J L
     E     E
```

With a little imagination the word ENEMY can be seen in the similarity of the placement of the E.

Further, it seems to make sense in that the phrase REPORTED ENEMY would appear at the opening of the message. If the assumption is correct then:

$$\frac{5}{Ac}=\text{Np},\ \frac{2}{Sc}=\text{Mp}\ \text{ and }\ \frac{3}{Pc}=\text{Yp}$$

c. The process outlined can be continued, as long as probable words can be seen in the text. However there is danger in this unless the assumptions are checked periodically for validity against other factors. In this case, the assumed values shown below can be compared to their respective frequency distributions. If no significant differences are noted, then they may be placed in the reconstruction matrix:

New assumed values

Alphabet 1	
Alphabet 2	*Pc*=Ap, *Sc*=Mp
Alphabet 3	*Bc*=Pp, *Yc*=Dp, *Wc*=Cp, *Pc*=Yp
Alphabet 4	*Rc*=Op
Alphabet 5	*Sc*=Pp, *Gc*=Tp, *Ac*=Np

13–15. (~~C~~) The Reconstruction Matrix

a. The values previously established when inserted in the reconstruction matrix would result in the matrix shown in figure 13–26.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1					*I*				*C*						*M*			*Q*		*V*						
C2	*P*				*W*								*S*													
C3			*W*	*Y*	*G*										*G*	*B*									*P*	
C4					*C*						*M*			*Q*	*R*	*V*										
C5		*M*			*Q*		*V*							*A*		*S*		*I*		*G*		*C*				

Figure 13–26 (~~C~~). Insertion of recovered values (U).

In so doing an inconsistency becomes apparent. Note the sequences $\overset{P}{\text{C}}\ \overset{C}{W}\overset{D}{Y}\overset{F}{G}$ in alphabet 3 and $\overset{P}{\text{C}}\ \overset{R}{I}\overset{S}{-}\overset{T}{G}$ in alphabet 5. If, as has been assumed, the same sequences are being dealt with, this is an impossible situation. One or the other must be wrong. Therefore the value of each must be reexamined. In alphabet 3 the values $\frac{C}{W}$ and $\frac{D}{Y}$ were derived by analysis while the position of *Gc* below Ep was purely on the basis of inspection of the frequency distribution. The placement of *Gc* below the $\frac{5}{\text{Tp}}$ was on the basis of assuming the word ATTACK. Therefore it is now determined that the initial assumption of $\frac{3}{Gc}$ as Ep is incorrect. Yet, as seen in the triliteral frequency distribution, $\frac{3}{Gc}$ behaves like a vowel, therefore it should be replaced beneath a vowel other than E But which one? Perhaps an answer can be found by ignoring the *Gc* in alphabet 3 for the moment and applying the principles of direct symmetry of position to transfer vowels. Thus the matrix would now appear as shown in figure 13–27.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1	*A*		*S*		*I*		*G*		*C*						*M*		*Q*	*R*	*V*							
C2	*P*				*W*								*S*													
C3			*W*	*Y*												*B*									*P*	
C4	*I*		*G*		*C*						*M*			*Q*	*R*	*V*							*A*		*S*	
C5		*M*			*Q*	*R*	*V*							*A*		*S*		*I*		*G*		*C*				

Figure 13–27 (C). Insertion of recovered values, step 2 (U).

b. The relative position of letters in each sequence is such that the use of a keyword mixed alphabet as the secondary component can be safely assumed. In particular, note the sequence *M – – QRV* in alphabets 1, 2, 4, and 5, *WY* in alphabet 3. Note also the *A–S–I–G–C* sequence, again in alphabets 1, 2, 4, and 5. These sequences are reminiscent of portions of a keyword; *A–S–I–G–C* being the keyword, possibly the *G* marking its end; the *QRV* being a mid portion, and *WY* of alphabet 3 marking its end. Previously in alphabet 3, *G* was incorrectly placed immediately following the *Y*. Perhaps, instead, a *Z* should be placed there. In the case of the sequence *M – – QRV, O* and *P* should be placed between the *M* and *Q*; thus, *N* could be placed between the *I* and *G* of the sequence *A–SOI–G–C*. If this was done *G* would then fall beneath a vowel in alphabet 3 as required. This placement would then allow the reconstruction matrix to be expanded (fig. 13–28).

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1	*A*		*S*		*I*	*N*	*G*	*B*	*C*						*M*	*O*	*P*	*Q*	*R*	*V*	*W*	*Y*	*Z*			
C2	*P*	*Q*	*R*	*V*	*W*	*Y*	*Z*				*A*		*S*		*I*	*N*	*G*	*B*	*C*							
C3	*R*	*V*	*W*	*Y*	*Z*				*A*		*S*		*I*	*N*	*G*	*B*	*C*						*M*	*O*	*P*	*Q*
C4	*I*	*N*	*G*	*B*	*C*						*M*	*O*	*P*	*Q*	*R*	*V*	*W*	*Y*	*Z*				*A*		*S*	
C5		*M*	*O*	*P*	*Q*	*R*	*V*	*W*	*Y*	*Z*				*A*		*S*		*I*	*N*	*G*	*B*	*C*				

Figure 13–28 (~~C~~). Expansion of matrix (U).

13–16. ~~(C)~~ Completion of the Solution

a. Having reached this point in the analysis, the next step is to again transfer the newly assumed plaintext values to the cryptogram being studied. The object is twofold. First, by so doing the validity of the assumptions may be proved or disproved, according to the structure of the resultant plaintext produced. Second, if the assumptions are proven valid, their insertion into the cryptogram will enable the analyst to assume new plain-to-cipher values. Accordingly, this will produce the following partially recovered cryptogram (fig. 13–29).

```
            5      10      15      20      25

A       QWBRI   VWYCA   ISPJL   RBZEY   QWYEU
        REPOR   TEDEN   EMY     SRE I   RED
B       LWMGW   ICJCI   MTZEI   MIBKN   QWBRI
         EWCH   ESTER   O E R   OOP S   REPOR
C       VWYIG   BWNBQ   QCGQH   IWJKA   GEGXN
        TEDAT   HENDE   RSON    EE  N   G O S
D       IDMRU   VEZYG   QIGVN   CTGYO   BPDBL
        E WO    T ERT   ROOPS   I ORC   HA D
E       VCGXG   BKZZG   IVXCU   NTZAO   BWFEQ
        TSO T   H EST   ED E    F EWC   HE  E
F       QLFCO   MTYZT   CCBYQ   OPDKA   GDGIG
        R  EC   O DS    ISPRE   PA  N   G O T
G       VPWMR   QIIEW   ICGXG   BLGQQ   VBCRS
        TACKF   ROM H   ESO T   H ONE   TROOP
H       MYJJY   QVFWY   RWNFL   GXNFW   MGJKX
        OF  I   RD QI   SEN     G N H   OS
J       IDDRU   OPJQQ   ZRHCN   VWDYQ   RDGDG
        E  O    PA N    WC ES   TE RE   S O T
K       BXDBN   PXFPU   YXNFG   MPJEL   SANCD
        H  DS   Q  M    V N T   OA      CKNE
L       SEZZG   IBEYU   KDHCA   MBJJY   KILCJ
        C EST   ER R       EN   OR       O E
M       MFDZT   CTJRD   MIYZQ   ACJRR   SBGZN
        O  S    I  O    OODSE   AS OF   CROSS
N       QYAHQ   VEDCQ   LXNCL   LVVCS   QWBII
        RFI E   T  EE      NE    DBEP   REPAR
P       IVJRN   WNBRI   VPJEL   TAGDN   IRGQP
        ED OS   UPPOR   TA       KO S   ECOND
Q       ATYEW   CBYZT   EVGQU   VPYHL   LRZNQ
        A D H   IRDS     DON    TAD      CEBE
R       XINBA   IKWJQ   RDZFY   KWEZL   GWFJQ
         ONDN   E C E   S ER     E S    GE  E
S       QWJYQ   IBWRX
        RE RE   ERCO
```

Figure 13–29 (~~C~~). Plaintext partially recovered (U).

b. With the wealth of plaintext values now added to the cryptogram, the final solution is quite simple. With but little effort, the plaintext can be inferred. For example, line A and the first group of line B reads:

> REPORTED ENEMY HAS RETIRED TO NEWCHESTER

Using the values established by this assumption, the basic cipher sequence, again through the process of direct symmetry of position, can be expanded to:

C1. *AUS INGBC J LMNOPQRVWYZE*

with only the letters D, F, H, K, T, and X unplaced, recovery of the keyword follows immediately. Considering the positional limitations of the sequences, the keyword mixed sequence is derived as:

EXHAUSTINGBCDFJKLMOPQRVWYZ

and the repeating key is APRIL under Ap.

c. A reconstruction of the cipher matrix using the above key and sequences reveals the message as:

> REPORTED ENEMY HAS RETIRED TO NEWCHESTER(.) ONE TROOP IS REPORTED AT HENDERSON MEETING HOUSE(.) TWO OTHER TROOPS IN ORCHARD AT SOUTHWEST EDGE OF NEWCHESTER(.) SECOND SQ IS PREPARING TO ATTACK FROM THE SOUTH(.) ONE TROOP OF THIRD SQ IS ENGAGING HOSTILE TROOP AT NEWCHESTER(.) REST OF THIRD SQ IS MOVING TO ATTACK NEWCHESTER FROM THE NORTH(.) MOVE YOUR SQ INTO WOODS EAST OF CROSSR(OADS) FIVE THREE NINE AND BE PREPARED TO SUPPORT ATTACK OF SECOND AND THIRD SQ(.) DO NOT ADVANCE BEYOND NEWCHESTER(.) MESSAGES HERE(.) TREER, COL(.)

Section III. (~~C~~) SPECIAL CASES AND THEIR SOLUTION

13–17. (~~C~~) Solution of Message Using the Same Alphabets—Different Key—Completing the Plain Component

a. It sometimes happens that correspondents will use the same primary components to encipher a series of messages, only using a different key for each message. In this case, if one message is recovered and the primary components are reconstructed, the situation is then one of a message enciphered using a known sequence. Thus the possibility arises that all subsequent messages can be solved by completing the plain component.

b. In previous paragraphs it was shown that, in the case of monoalphabetic ciphers, completion of the plain component was based on inscribing a normal alphabetic sequence below the plain component equivalents, the plaintext then appearing on one generatrix. Also, as was shown in the case of polyalphabetic ciphers using standard alphabets, the plaintext equivalents of each alphabet involved reappeared on the same generatrix; thus it was only necessary to combine the proper generatrices to reproduce the plaintext. In the situation under discussion both processes are combined. The techniques involved are explained in the following paragraphs.

c. Presupposing that the message in figure 13–30 was enciphered using the same primary components as were used in the preceding example, the first step is to determine the period or number of alphabets involved.

	5	10	15	20	25
A	*SFDZR*	*YRRKX*	*MIWLL*	*AQRLU*	*RQFRT*
B	*IJQKF*	*XWUBS*	*MDJZK*	*MICQC*	*UDPTV*
C	*TYRNH*	*TRORV*	*BQLTI*	*QBNPR*	*RTUHD*
D	*PTIVE*	*RMGQN*	*LRATQ*	*PLUKR*	*KGRZF*
E	*JCMGP*	*IHSMR*	*GQRFX*	*BCABA*	*OEMTL*
F	*PCXJM*	*RGQSZ*	*VB*		

Figure 13–30 (C). Ciphertext for analysis (U).

(1) The size of the sample and the repetition *MRGQ* occurring at an interval of 21 suggests polyalphabetic encipherment with a period of either 3 or 7. The repeated trigraph *DPT* at an interval of 28 tends to confirm the period as being 7. Thus the message is then transcribed into seven columns—each column corresponding to one period, indicating the use of one alphabet.

1	*2*	*3*	*4*	*5*	*6*	*7*
S	*F*	*D*	*Z*	*R*	*Y*	*R*
R	*K*	*X*	*M*	*I*	*W*	*L*
L	*A*	*Q*	*R*	*L*	*U*	*R*
Q	*F*	*R*	*T*	*I*	*J*	*Q*
K	*F*	*X*	*W*	*U*	*B*	*S*
M	*D*	*J*	*Z*	*K*	*M*	*I*
C	*Q*	*C*	*U*	*D*	*P*	*T*
V	*T*	*Y*	*R*	*N*	*H*	*T*
R	*O*	*R*	*V*	*B*	*Q*	*L*
T	*I*	*Q*	*B*	*N*	*P*	*R*
R	*T*	*U*	*H*	*D*	*P*	*T*
I	*V*	*E*	*R*	*M*	*G*	*Q*
N	*L*	*R*	*A*	*T*	*Q*	*P*
L	*U*	*K*	*R*	*K*	*G*	*R*
Z	*F*	*J*	*C*	*M*	*G*	*P*
I	*H*	*S*	*M*	*R*	*G*	*Q*
R	*F*	*X*	*B*	*C*	*A*	*B*
A	*O*	*E*	*M*	*T*	*L*	*P*
C	*X*	*J*	*M*	*R*	*G*	*Q*
S	*Z*	*V*	*B*			

(2) With the message rearranged to reflect the use of its alphabets, the following step consists of converting each column to a plain component equivalent. This is done by juxtaposing the reconstructed cipher component against the normal plain component at any arbitrary point, then listing the pseudo-plain equivalents in columnar form reading from the cipher component, as follows:

P–P	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
C	*E*	*X*	*H*	*A*	*U*	*S*	*T*	*I*	*N*	*G*	*B*	*C*	*D*	*F*	*J*	*K*	*L*	*M*	*O*	*P*	*Q*	*R*	*V*	*W*	*Y*	*Z*

	1	2	3	4	5	6	7
C	*S*	*F*	*D*	*Z*	*R*	*Y*	*R*
P–P	*F*	*N*	*M*	*Z*	*Y*	*V*	*Y*

For this it is not necessary to convert all rows—just a sufficient number to form a basis for the subsequent step. In this case 10 rows will do:

	1	2	3	4	5	6	7
P–P	*F*	*N*	*M*	*Z*	*V*	*Y*	*V*
	V	*P*	*B*	*R*	*H*	*X*	*Q*
	Q	*D*	*U*	*V*	*Q*	*E*	*V*
	U	*N*	*V*	*G*	*H*	*O*	*U*
	P	*N*	*B*	*E*	*X*	*K*	*F*
	R	*M*	*O*	*Z*	*P*	*R*	*H*
	L	*U*	*L*	*E*	*M*	*T*	*G*
	W	*G*	*Y*	*V*	*I*	*C*	*G*
	V	*S*	*V*	*W*	*K*	*U*	*Q*
	G	*H*	*U*	*K*	*I*	*T*	*V*

(3) Selecting the first five lines of plain component equivalents produced by the preceding step, a generatrix diagram is produced for each by inscribing, in columnar form, the normal alphabetic sequence below each letter. Each generatrix so produced is then rough scored using the methods shown in paragraph 13–5*b*. This process is illustrated in figure 13–31.

Gen.		Alphabet 1		Alphabet 2		Alphabet 3		Alphabet 4		Alphabet 5
Cipher		SRLQKMCVRT		FKAFFDQTOI		DXQRXJCYRQ		ZMRTUZURVB		RILIWKDNBN
1	1	FVQUPRLWVG	4	NPDNNMUGSH	1	MBUVBOLYVU		~~ZRVGEZEVWK~~		~~VHQHXPMIKI~~
2		~~GWRVQSMXWH~~	7	OQEOONVHTI	1	NCVWCPMZWV	3	ASWHFAFWXL		~~WIRIYQNJLJ~~
3		~~HXSWRTNYXI~~	3	PREPPOWIUJ		~~ODWXDQNAXW~~		~~BTXIGBGXYM~~		~~XJSJZROKMK~~
4		~~IYTXSUOZYJ~~		~~QSGQQPXJVK~~		~~PEXYEROBYX~~		~~CUYJHCHYZN~~		~~YKTKASPLNL~~
5		JZUYTVPAZK		~~RTHRRQYKWL~~		~~QFYZFSPCZY~~		~~DVZKIDIZAO~~		~~ZLULBTQMOM~~
6		~~KAVZUWQBAL~~		~~SUISSRZLXM~~		~~RGZAGTQDAZ~~		~~EWALJEJABP~~	3	AMVMCURNPN
7	2	LBWAVXRCBM	6	TVJTTSAMYN	5	SHABHUREBA		~~FXBMKFKBCQ~~	5	BNWNDVSOQC
8	2	MCXBWYSDCN		~~UWKUUTBNZO~~	4	TIBCIVSFCB	2	GYCNLGLCDR	5	COXOEWTPRP
9		~~NDYCXZTEDO~~	2	VXLVVUCOAP		~~UJCDJWTGDC~~	3	HZDOMHMDES		~~DPYPFXUQSQ~~
10	4	OEZDYAUFEP	0	WYMWWVDPBQ		~~VKDEKXUHED~~	8	IAEPNINEFT		~~EQZQGYVRTR~~
11		~~PFAEZBVGFQ~~		~~WZNXXWEQCR~~	3	WLEFLYVIFE		~~JBFQOJOFGU~~	5	FRARHZWSUS
12	2	QGBFACWHGR	4	YAOYYXFRDS		~~XMFGMZWJGF~~		~~KCGRPKPGHV~~	6	GSBSIAXTVT
13	3	RHCGBDXIHS		~~ZBPZZYGSET~~		~~YNGHNAXKHG~~		~~LDHSQLQHIW~~	2	HTCTJBYUWU
14	5	SIDHCEYJIT		~~ACQAAZHTFU~~	4	ZOHIOBYLIH		~~MEITRMRIJX~~		~~IUDUKCZUXV~~
15		~~TJEIDFZKJU~~	3	BDRBBAIUGV		~~APIJPCZMJI~~		~~NFJUSNSJKY~~	2	JVEVLDAWYW
16		~~UKFJEGALKV~~	2	CESCCBJVHW		~~BQJKQDANKJ~~		~~OGKVTOTKLZ~~		~~KWFWMEBXZX~~
17	0	VLGKFHBMLW		~~DFTDDCKWIX~~		~~CRKLREBOLK~~	1	PHLWUPULMA		~~LXGXNFCYAY~~
18	2	WMHLGICNMX		~~EGUEEDLXJY~~	2	DSLMSFCPML		~~QIMXVQVMNB~~		~~MYHYOGDZBZ~~
19		~~XNIMHJDONY~~		~~FHVFFEMYKZ~~	5	ETMNTGDQNM	5	RJNYWRWNOC		~~NZIZPHEACA~~
20		~~YOJNIKEPOZ~~	3	GIWGGFNZLA	6	FUNOUHERON		~~SKOZXSXOPD~~		~~OAJAQIFBDB~~
21		~~ZPKOJLFQPA~~		~~HJXHHGOAMB~~	4	GVOPVIFSPO	4	TLPAYTFPQE		~~PBKBRJGCEC~~
22		~~AQLPKMGRQB~~	4	IKYIIHPBNC		~~HWPQWJGTQP~~		~~UMQBZUZQRF~~		~~QCLCSKHDFD~~
23	4	BRMQLNHSRC		~~JLZJJIQCOD~~		~~IXQRXKHURQ~~	6	VNRCAVARSG	5	RDMDTLIEGE
24	7	CSNRMOITSD		~~KMAKKJRDPE~~	5	JYRSYLIVSR	4	WOSDBWBSTH	4	SENEUMJFHF
25	6	DTOSNPJUTE		~~LNBLLKSEQF~~		~~KZSTZMJWTS~~		~~XPTECXCTUI~~	4	TFOFVNKGIG
26		~~EUPTOQKVUF~~	3	MOCMMLTFRG		~~LATUANKXUT~~		~~YQUFDYDUVJ~~	1	UGPGWOLHJH

Figure 13–31 (~~C~~). *Rough scoring of generatrices* (*U*).

(4) Those generatrices with the highest score are then set down in columnar form to determine if they will yield plaintext.

Alphabet	1	2	3	4	5
Generatrix	24	2	20	10	12
	C	O	F	I	G
	S	Q	U	A	S
	N	E	N	E	B
	R	O	O	P	S
	M	O	U	N	I
	O	N	H	I	A
	I	V	E	N	X
	T	H	R	E	T
	S	T	O	F	V
	D	I	N	T	T

(5) The presence of plaintext in the matrix is obvious. However, it is also noted that generatrix 12 of alphabet 5, although the highest word, is not correct. Therefore another is selected in its place. Also, since a period of seven was initially assumed, the diagram is expanded to include seven columns, the previous step being completed to produce the necessary generatrices. Thus the text would appear as:

Alphabet	1	2	3	4	5	6	7
	C	O	F	I	R	S	T
	S	Q	U	A	D	R	O
	N	E	N	E	M	Y	T
	R	O	O	P	D	I	S
	M	O	U	N	T	E	D
	O	N	H	I	L	L	F
	I	V	E	N	I	N	E
	T	H	R	E	E	W	E
	S	T	O	F	G	O	O
	D	I	N	T	E	N	T

(6) Comparing the first period of plaintext with the first period of ciphertext, and setting the plain and primary components so as to produce the equivalency shown in each alphabet of the period, the key may be recovered. For example, in

	1	2	3	4	5	6	7
P	C	O	F	I	R	S	T
C	*S*	*F*	*D*	*Z*	*R*	*Y*	*R*

it is observed that Cp=*Sc*. This equation can be duplicated by juxtaposing the two primary sequences so:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
E X H A U S T I N G B C D E F J K L M O P Q R V W Y Z E X H A U S T I N G B C D F J K L M O P Q R V W Y Z

Thus Ap=*Ac*.
Continuing the process of juxtaposing it will be found that

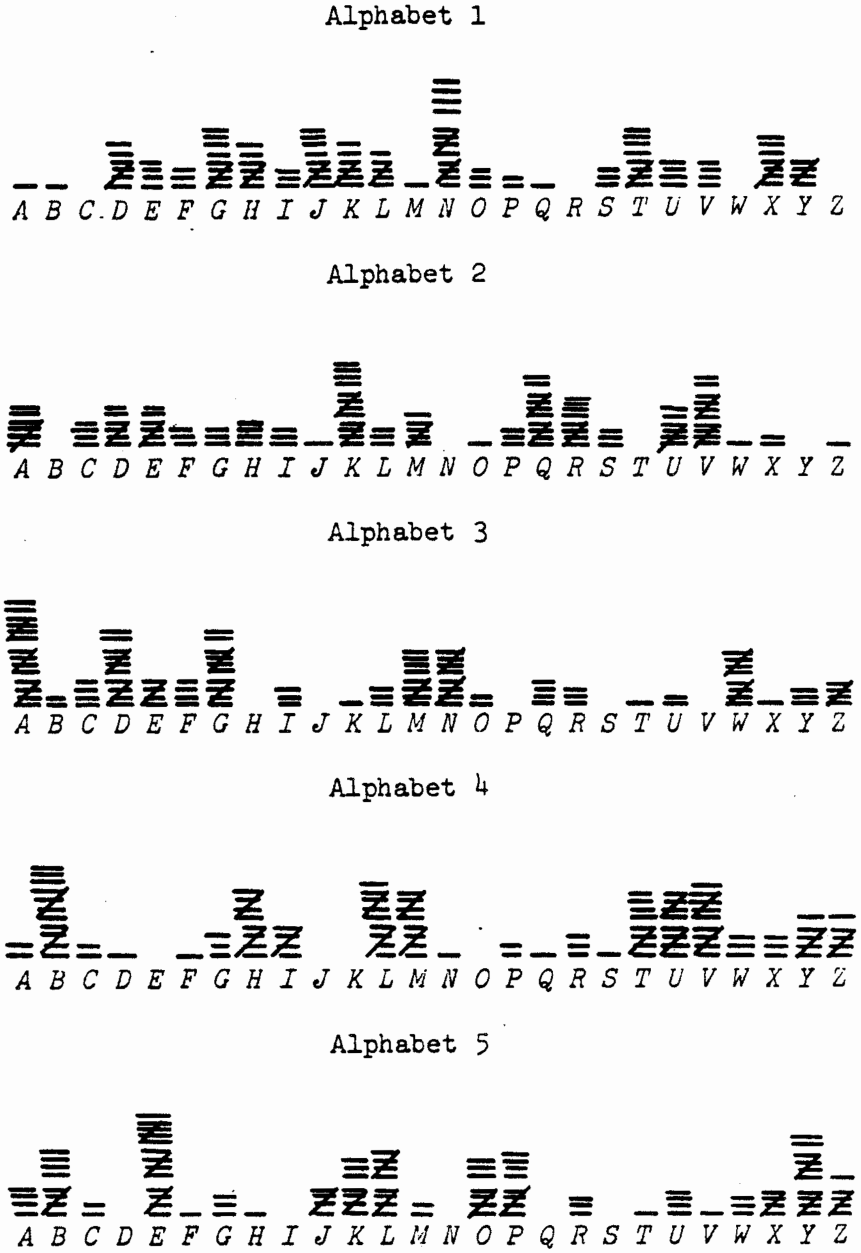
when	then
Cp=*Sc*	Ap=*Ac*
Op=*Fc*	Ap=*Zc*
Fp=*Dc*	Ap=*Ic*
Ip=*Zc*	Ap=*Mc*
Rp=*Rc*	Ap=*Uc*
Sp=*Yc*	Ap=*Tc*
Tp=*Rc*	Ap=*Hc*

The repeating key then is AZIMUTH. Using this, the enciphering matrix can then be reconstructed and the entire message deciphered.

13–18. ~~(C)~~ The Principles of Matching—Solution of Messages Involving an Unknown Component

a. In the preceding example the proposition was the solution of a message where both the primary plain and cipher components were known. The key—which controlled the successive juxtaposition—producing the secondary cipher sequences, was the unknown element. This case is one where only the primary cipher sequence and key length is known, the key is unknown, and the primary plain component is unknown. The normal condition, i.e. where the plain component is known, permits the use of the principle of direct symmetry of positions. In this case where only the cipher sequence is the known element, the use of direct symmetry of position or completing the plain components is prohibited. Instead, the principle of matching may be used.

b. This principle is founded on the fact that a form of symmetry, in this case spatial, exists between the successive peaks and troughs of secondary cipher sequences which are produced by the juxtaposition of the two primary components. This spatial symmetry can be seen in the following distributions, figure 13–32, drawn from a cryptogram produced by the method under discussion which involved five secondary alphabets.



Alphabet 1

Alphabet 2

Alphabet 3

Alphabet 4

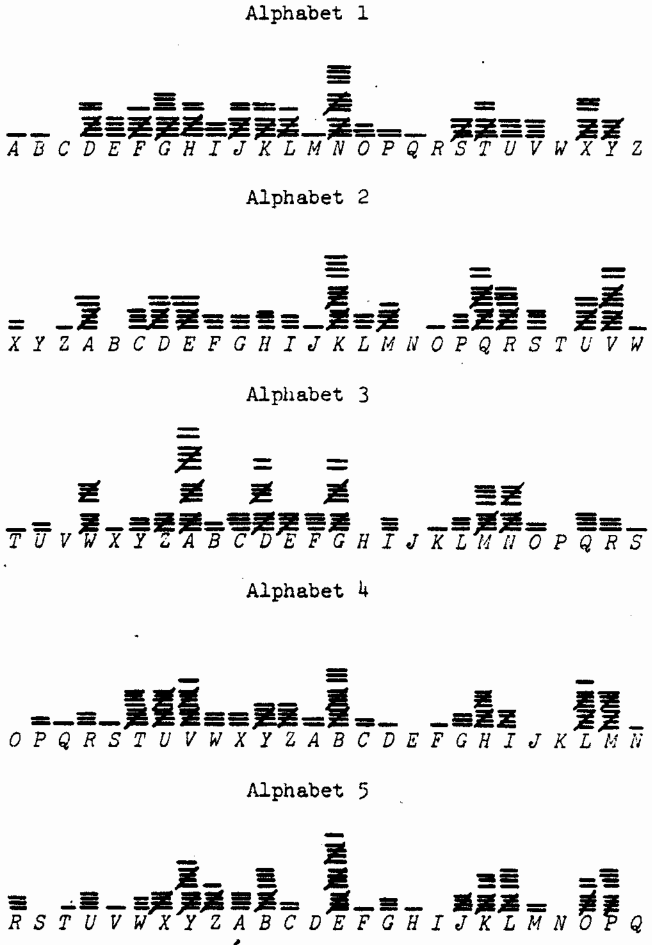
Alphabet 5

Figure 13–32 (~~C~~). *Uniliteral frequency distribution, secondary cipher sequences* (*U*).

Note that in each of the distributions the spatial relationships between the peaks and troughs remain constant, but that between distributions, their positions relative to any given letter differ. In this case, the highest peaks occur in successive alphabets above the *Nc*, *Kc*, *Ac*, *Bc*, and *Ec* in that order. The spatial symmetry is a result of juxtaposing one fixed sequence against another fixed sequence. The difference between the relative location of the peaks and troughs in each distribution is the result of using successively different points of juxtaposition.

c. It was remarked earlier that a periodic polyalphabetic cipher was really nothing more than a series of monoalphabetic substitution ciphers used in a periodic or cyclic manner. Thus each period, as reflected in the distributions, will show to a greater or lesser degree the normal frequencies of monoalphabetic usage. Spatially, in the case where both components are standard, it will be the same as the normal, only offset to the same degree as were the primary components. Where mixed components are used in either or both components, this spatial relationship, relative to the normal, is lost. However, the frequency of usage of individual letters, as reflected in peaks and troughs, remains. The fact that this can be observed at all indicates that the cipher sequence is a known sequence. Note that in the above, the cipher sequence is known, and in this case is a standard alphabet. However, when the cipher alphabet is a mixed alphabet, the same principles will apply if its sequence is known. But in that case, the distribution must be made using this sequence of letters. In either case, if the wrong sequence is used the symmetry between each distribution will be lost.

d. With the knowledge that each distribution is a monoalphabetic distribution reflecting the underlying plaintext, several possibilities are immediately opened. First, by matching the peaks and troughs of each and bringing them into agreement, relative equal values can be determined. That is, *Nc*, *Kc*, *Ac*, *Bc*, and *Ec*, the highest frequency letter of each distribution, can be equated as representing the same plaintext value. If this is so, then, because of the similar spatial relationship between each distribution, all letters can be equated. Second, as the peaks and troughs represent the underlying plaintext frequencies it becomes possible to identify an equated series of letters to one specific plaintext value. Barring the fact that specific identification is possible, the assignment of an arbitrary plaintext value to each set of equated cipher values permits the reduction of the plaintext to monoalphabetic terms. The first step then is matching the distributions. This involves the cyclic shifting of the alphabets as seen in figure 13–33.


Alphabet 1

Alphabet 2

Alphabet 3

Alphabet 4

Alphabet 5

Figure 13–33 (~~C~~). *Matching by cyclic shifting* (*U*).

(1) Note that in the above, the sequence *Nc*, *Kc*, *Gc*, *Bc*, *Ec*, was used rather than the sequence *Nc*, *Kc*, *Ac*, *Bc*, *Ec*, previously used as a frame of reference. This is because the alinement of *Ac* to the other values resulted in the mismatch of the remaining high-frequency letters. This is a reflection of the necessity to gain the best alinement of all peaks and troughs. Once the alphabets have been alined, a set of arbitrary plaintext values can be generated. This can be done by substituting the values of alphabets 2–3–4 and 5 in the ciphertext, for the value directly above it in alphabet 1. Thus whenever *Xc*, *Tc*, *Oc*, and *Rc* occurs in the cyclic positions 2, 3, 4, and 5 respectively, an *Ac* is substituted. This process, the reduction to monoalphabetic terms, converts the ciphertext to the form shown in figure 13–34.

	5	10	15	20	25
A	Q H V H T	L U T X I	J Y N F P	N G S H T	E Y U F H
B	E U T G N	V U G Y X	Y D H Y Y	D N L U S	S I T K X
C	Y K T Y N	G T H Y K	U T H J A	H X M N D	K T F Y D
D	N H S H C	K T P X N	K C I G N	U O P N T	N G H J K
E	X X K S U	L D K H T	P R H K X	D N R K T	L D K T H
F	B Y U R E	U H L Y N	F I T F N	G Y D N H	T Y K L U
G	S S I T K	X Y H L L	U G F G N	L N T Y J	E X K P T
H	N F M E Q	H V H T H	T P N G S	H T E B Y	D N V G N
J	X X X H K	F Y D N G	N A H X K	T F K X V	I Y H M J
K	N V G U U	O Y D H Y	Y D N L U	S K T Y N	G T K T X
L	Y K P H Y	N F Y D N	X N K C I	G N U O P	N T N G H
M	J L D K H	T P H T F	X U S N U	O D K X P	N T N G H
N	J X B S K	J K Y H G	E U M X N	G Z N G X	X H K F Y
P	D N L U I	V A U I J	F D H Z N	M N N T K	S V U X X
Q	K M J N I	T J N X X	P N T N G	H J L D H	T P D X I
R	N T J K H	T P D U Y	D N H F N	F O U G S	N G A H G
S	J U G F U	O S H T L	D I G K H	D H F O U	G S N F H
T	T H J J K	H T L N A	K Y D Y D	N L U S S	I T K X Y
U	J N H F N	G X D N A	H X X I V	V U X N F	Y U M N O
V	K P D Y K	T P B X I	L D H T H	J J K H T	L N Y D N
W	X N U M X	N G Z N G	X F N L J	H G N F U	V N T N F
X	I V H G N	F G U I Y	N O G U S	S U X L U	A Y U T U
Y	G Y D H T	F L N T Y	G H J L D	K T H B	

Figure 13–34 (*C*). *Ciphertext reduced to monoalphabetic terms* (*U*).

(2) By compiling the individual frequency distributions using the same method as was used to

convert the text to monoalphabetic terms, a uniliteral frequency distribution for the text can be generated which in effect is merely a tabulation of the former five. See figure 13–35.

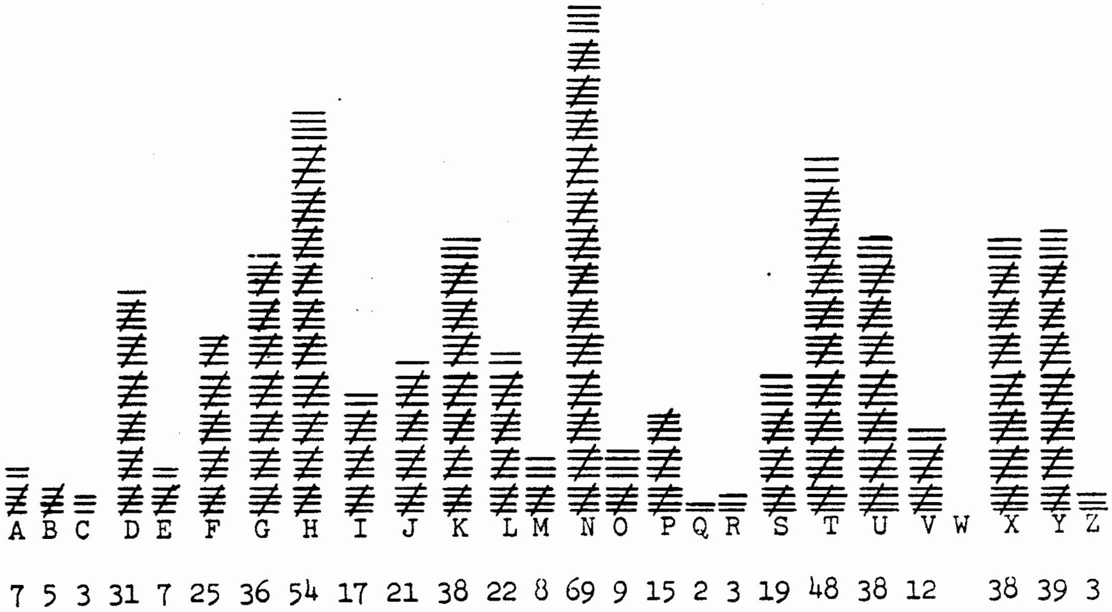


Figure 13–35 (U). Uniliteral frequency distribution of monoalphabetic terms (U).

e. Subsequent analysis of the cryptogram is now quite simple. The text converted to uniliteral terms can be attacked through an analysis of idiomorphic patterns, repeated digraphs, trigraphs, etc. In the course of determining the correct cipher equivalents for the pseudoplaintext, in this case alphabet 1, the mixed-plain component will be found. With this as a base, it only requires that the cipher components and plain components be juxtaposed to produce the values shown in each distribution; the process resulting in the reproduction of the enciphering matrix and the keyword.

13–19. (~~C~~) Application of Principles—Matching

a. In the foregoing paragraph the example involved the use of a standard sequence as the cipher component. In this example a mixed sequence is used. It will be observed that irrespective of the type sequence used, the principle of matching may be applied if the cipher sequence is known. However, if the cipher sequence is unknown, these principles cannot be applied.

b. The first step, as in all cases of the analysis of polyalphabetic ciphers, is to underline observed repeats and tabulate intervals and factors as shown in figure 13–36.

c. The derived factors show that the period involved is probably five. Since the text is in groups of five, its rearrangement is not required. Now, assuming that through preknowledge the primary cipher component is probably a keyword mixed

```
            5          10          15          20          25
A   I C E N X   J J B N L   Q U K D A   N P I Q A   Q J P B T
B   I C P M H   B C M B D   K Z P V Z   W P A B H   Q J M M H
C   B C I F M   J K F S C   T Z P F D   M H S E H   H H C I A
D   N E L A Y   A V F N Y   M I L Y X   J P Q J E   W E K N W
E   A C M B U   W E G G G   K C K G D   Z F E B T   I C P P A
F   J A M X C   Q D N N U   N U C T A   X E M B D   K K O A A
G   I H R G P   J E G E C   M W A X T   J H D V Z   T Z R N X
H   N Q P O A   K E A F Q   Q Z O N M   Q J I I N   I C J Y H
J   N K R G D   V P E C X   N U U A N   W C M W A   U H K K N
K   J P M C Q   V H R Y X   J M L D E   T Y Q E G   M K R R J
L   Q G O E Z   I V P F J   E M L D E   T H N K F   B H A I H
M   Y K Z G C   E P R C B   J P M N G   M K I I C   R H R A X
N   Q D P W F   Z G A F H   N E K E C   W R P E G   Z P Q A B
P   H I B S F   V J P I Y   Y C Q B H   H K X N M   M F E E J
Q   W B A B F   M C P X C   T Q Z G Y   R C D A X   Q M P K Z
R   I C M X X
```

Repeats	Interval	Factors
B T I C P	95	5 19
M H B C	20	2, 4, 5, 10
M B D K	110	5, 10, 11 22
M L D E T	25	5

Figure 13–36 (C). Period determination (U).

alphabet based on the word PURLOIN, five separate distributions using this mixed alphabet are prepared (fig. 13-37).

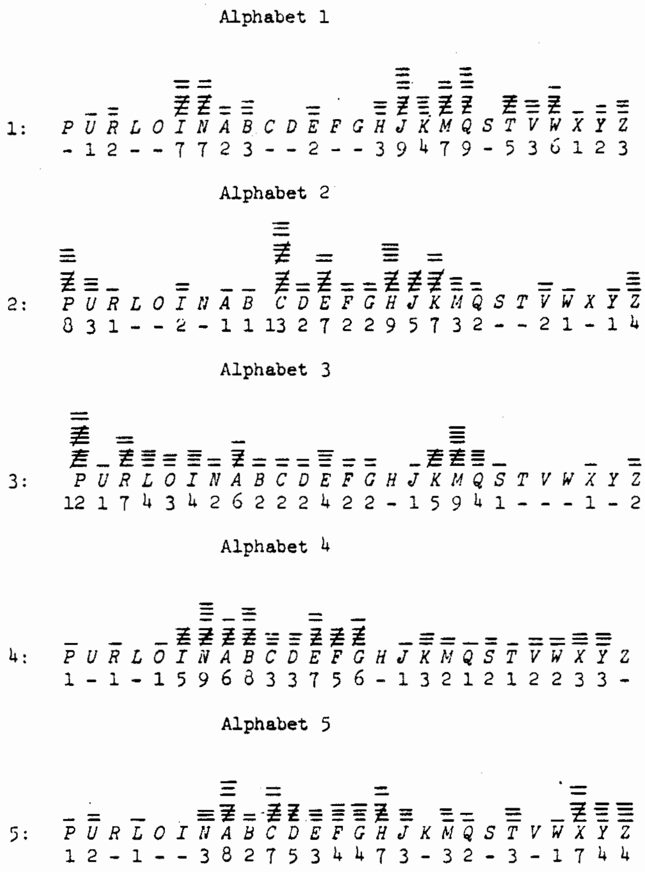


Figure 13-37 (~~C~~). Uniliteral frequency distribution of periodic cipher alphabets (U).

d. Visual inspection shows that the profile of each one is similar. The next step is to aline the alphabets to bring the peaks and troughs of each into conformance. Normally this is a step by step process. Two alphabets are selected and juxtaposed in what appears the most probable alinement. Note the possibility that any one of 26 juxtapositions are possible, but consideration of profiles immediately limits this to but a few. In this case three possible initial matches may be considered (fig. 13-38).

e. Of the three most probable matches, match 3 seems best so it is selected. Using these two alphabets as a base, the third alphabet is compared, again in several probable positions, until one is considered best. Thus in turn all alphabets are matched. The result of the process is shown in figure 13-39.

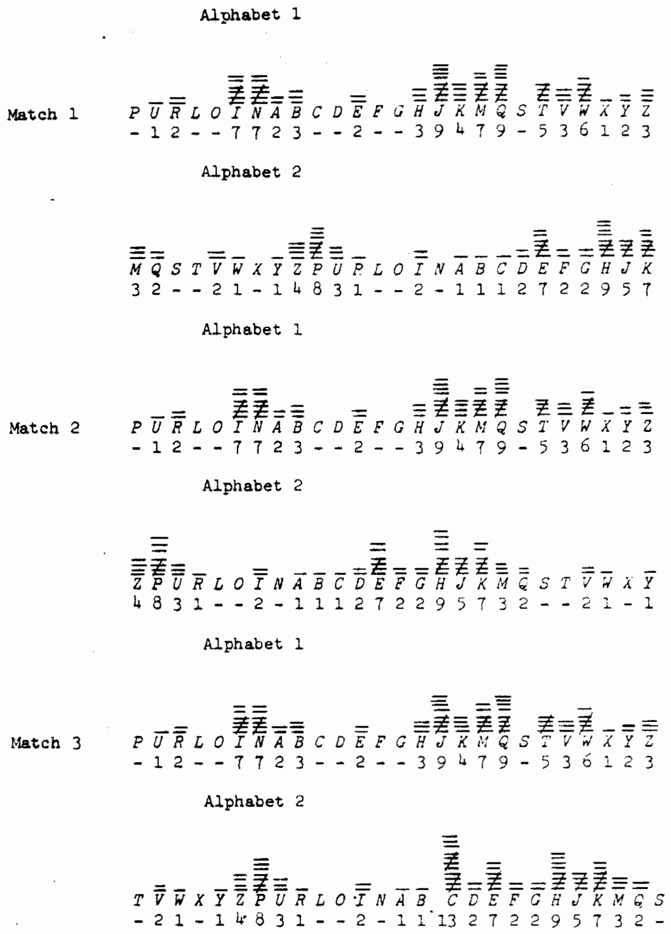


Figure 13-38 (~~C~~). Possible matches, periodic cipher alphabet 1 and 2 (U).

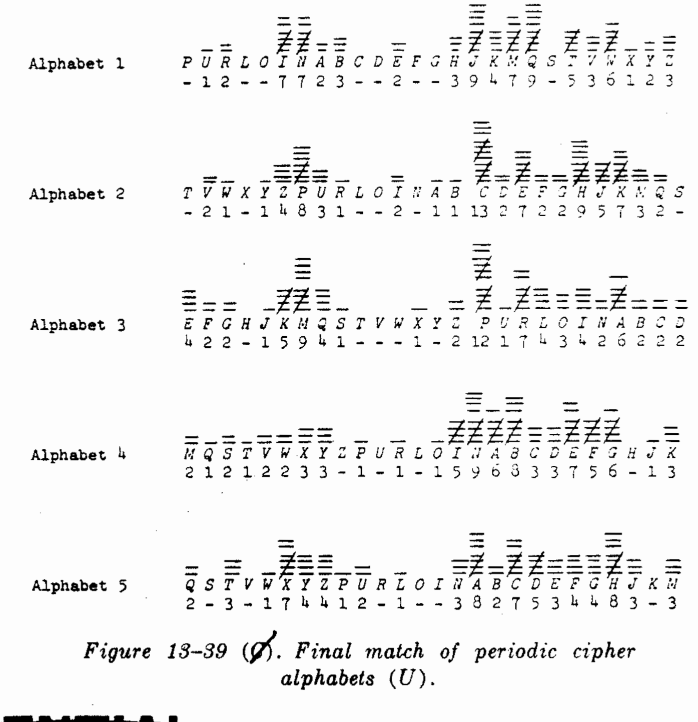


Figure 13-39 (~~C~~). Final match of periodic cipher alphabets (U).

f. If the columns of letters formed by the match are inspected, the repeating key "THIEF" may be observed, which lends credence to the match. Moreover, this might be the point of juxtaposition of the cipher alphabet to Ap. Unaware that the plain component is a mixed sequence, the analyst arbitrarily presumes a direct standard for the purpose of reducing the ciphertext to monoalphabetic terms. Thus Ap equals *Pc*, *Tc*, *Ec*, *Mc*, *Qc;* Bp equals *Uc*, *Vc*, *Fc*, *Qc*, *Sc;* etc. A standard alphabet is inscribed above the matrix shown above, and it is used to reduce the ciphertext to monoalphabetic terms. The reduction produces the text illustrated in figure 13-40.

g. Compiling the individual frequency distributions, a uniliteral frequency distribution for the text is generated (fig. 13-41).

h. Inspection of the text reveals the initial idiomorphic pattern.

```
     A B C B A    B D E B
C    F P A P F    P V X P L
```

Which may be a reflection of the underlying plaintext-REFERENCE; which may be part of the phrase "REFERENCE MY (YOUR) MESSAGE." If this is correct *Pc* would equal Ep, an assumption warranted by the frequency shown for *Pc*. With this an entering wedge, the plaintext and accompanying cipher-to-pseudo-plain equivalent, figure 13-42, can quickly be found.

```
             5          10          15          20          25
A    F P A P F   P V X P L   S H F T P   G G U B P   S V P R C
B    F P P A W   I P G R S   Q F P E H   W G W R W   S V G A W
C    I P U V Z   P W B C R   U F P V S   R U I U W   C U Y O P
D    G R S Q G   H B B P G   R L S H F   P G H Y T   W R F P E
E    H P G R J   W R C W V   Q P F W S   Z S A R C   F P P J P
F    P N G G R   S Q V P J   G H Y D P   X R G R S   Q W T Q P
G    F U R W I   P R C U R   R C W G C   P U Z E H   U F R P F
H    G Y P N P   Q R W V A   S F T P Z   S V U O O   F P E H W
J    G W R W S   V G A S F   G H Q Q O   W P G F P   B U F Z O
K    P G G S A   V U R H F   P X S T T   U E H U V   R W R L X
L    S T T U H   F B P V X   L X S T T   U U V Z U   I U W C W
M    Y W O W R   L G R S Q   P G G P V   R W U O R   C U R Q F
N    S Q P F U   Z T W V W   G R F U R   W I P U V   Z G H Q Q
P    O L X C U   V V P O G   Y P H R W   O W M P Z   R S A U X
Q    W O W R U   R P P G R   U Y O W G   C P Z Q F   S X P Z H
R    F P G X X
```

Figure 13-40 (~~C~~). *Ciphertext reduced to monoalphabetic terms* (*U*).

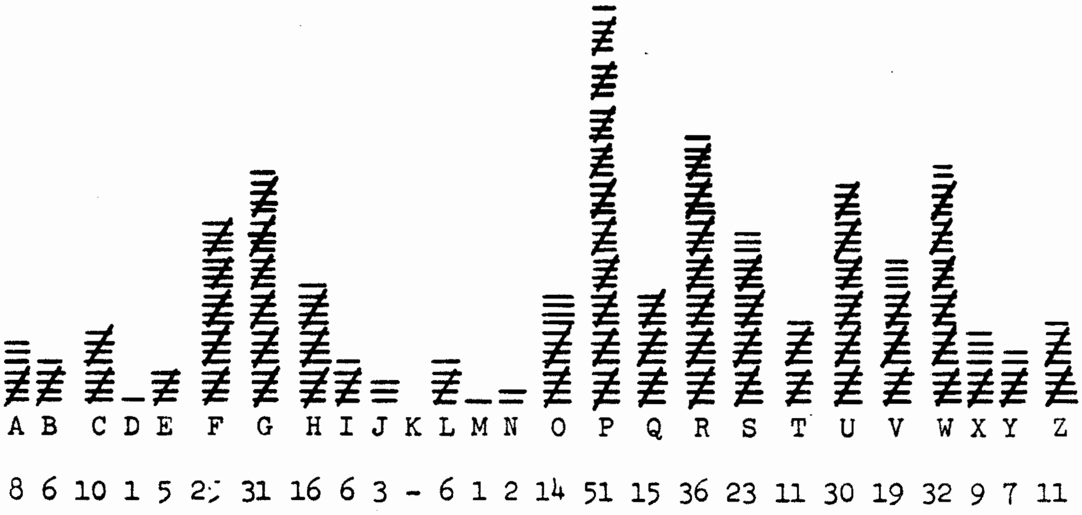


Figure 13-41 (*U*). *Uniliteral frequency distribution of monoalphabetic terms* (*U*).

```
REFER ENCEY OURME SSAGE ONETH
FPAPF PVXPL SHFTP GGUBP SVPRC

REEFI VESTO PREQU ISITI ONSFI
FPPAW IPGRS QFPEH WGWRW SVGAW

VEAND EIGHT ARENO TAVAI LABLE
IPUVZ PWBCR UFPVS RUIUW OUYOP

STOPS UGGES TYOUR ESUBM ITREQ
GRSQG HBBPG RLSHF PGHYT WRFPE

UESTW ITHIN PERIO DOFTH REEWE
HPGRJ WRCWV QPFWS ZSARC FPPJP

CKSST OPNEW SUBJE CTSTO PINPE o o o etc.
PNGGR SQVPJ GHYDP XRGRS QWTQP o o o etc.
```

Plain	F	G	H	J	Q	R	S	U	V	W		Y		K	L	E	P	T	O	M	A	N	I	C	S	D
Pseudo-plain	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*

Figure 13–42 (~~C~~). *Solution of ciphertext* (*U*).

Plain:	K	L	E	P	T	O	M	A	N	I	C	B	D	F	G	H	J	Q	R	S	U	V	W	X	Y	Z
C1:	*G*	*H*	*J*	*K*	*M*	*Q*	*S*	*T*	*V*	*W*	*X*	*Y*	*Z*	*P*	*U*	*R*	*L*	*O*	*I*	*N*	*A*	*B*	*C*	*D*	*E*	*F*
C2:	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*J*	*K*	*M*	*Q*	*S*	*T*	*V*	*W*	*X*	*Y*	*Z*	*P*	*U*	*R*	*L*	*O*	*I*	*N*
C3:	*Y*	*Z*	*P*	*U*	*R*	*L*	*O*	*I*	*N*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*J*	*K*	*M*	*Q*	*S*	*T*	*V*	*W*	*X*
C4:	*O*	*I*	*N*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*J*	*K*	*M*	*Q*	*S*	*T*	*V*	*W*	*X*	*Y*	*Z*	*P*	*U*	*R*	*L*
C5:	*I*	*N*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*J*	*K*	*M*	*Q*	*S*	*T*	*V*	*W*	*X*	*Y*	*Z*	*P*	*U*	*R*	*L*	*O*

Figure 13–43 (~~C~~). *Recovered matrix* (*U*).

i. In the plain sequence the keyword KLEPTOMANIC is observed. By using it then as a base with Kp as the index letter, five cipher sequences may be inscribed below it to reproduce the original enciphering matrix. The juxtaposition of each of these sequences must be used to reproduce the original ciphertext. That is, the letter Ep when enciphered by the five successive cipher alphabets must result in *Jc*, *Cc*, *Pc*, *Nc* and *Ac* respectively. Although any plaintext letter may be used for this alinement process, Ep was chosen because of its frequency. Thus the following matrix is reconstructed, figure 13–43.

CHAPTER 14 (~~C~~)

INTRODUCTION TO SIMPLE APERIODIC CIPHERS

Section I. (~~C~~) SIMPLE APERIODIC SYSTEMS

14–1. (~~C~~) Introduction

a. It was demonstrated in the preceding chapter that the ordered use of a number of alphabets in periodic ciphers resulted in the occurrence of cyclic phenomena in the ciphertext. It was also shown how this cyclic phenomena could be used as the basis for the cryptanalysis of the cipher. This was true even though a greater number or different types of mixed alphabets were involved. The significance of this phenomena was recognized by cryptographers, and means of suppression were soon considered. Two basic methods of suppression are available. First, the cyclic phenomena may be avoided simply by extending the key length to such a point that it repeats itself only a few times in a given message, and second, by the key length extending indefinitely, forming a running or continuous key. This particular solution, however, is impractical for use in all except machine systems. For this reason, and because the analysis of continuous keyed systems involves techniques and methods beyond the scope of this manual, it will not be treated further.

b. An alternate scheme, which permits the use of a matrix or table similar to those of the periodic ciphers, is to vary the period of key usage and thus suppress cyclic phenomena at the outset. Consideration of why periodicity is inherent to periodic polyalphabetic ciphers reveals that it is composed of the two elements involved in its production. That is, successive letters of a number of alphabets controlled by a repetitive key are applied to successive letters of the plaintext. Thus, if either of these components are varied, an aperiodic system is generated. Note that in aperiodic systems cyclic repetition does occur; however, it does so at an irregular interval which serves to suppress its appearance to a greater or lesser degree in the text.

c. Aperiodic systems then may be arbitrarily classified by the cryptographic method used to develop their aperiodicity, that is, by those components selected to vary and those selected to remain constant. Thus, those systems where the plaintext is made variable and the key sequence held constant may be considered as one class, and those systems where the plaintext is held constant and the key sequence used variably may be considered as another. Note that the resultant ciphers produced by either method are similar in that they will yield to the same general technique of analysis.

14–2. (~~C~~) Methods of Variations

a. One method of introducing variation in the plaintext is by word-length encipherment. In this method the key is applied in its sequential order to successive words of the plaintext, i.e. the first word is enciphered from the first alphabet, the second word from the second alphabet, etc. In this manner the key is completely run through, its cyclic reuse beginning anew following the use of the last alphabet.

b. One practical difficulty involved in decipherment of messages of this type by cryptographic personnel was in recognizing the end of a word, as in the case of INFORM, INFORMS, INFORMED, INFORMING, and INFORMATION. This led to the inclusion of a word separator. The word separator was used to mark the end of a word (the resumption of the keying cycle at its initial point), thus aiding the deciphering clerk. A low-frequency letter was selected to be the word separator because it was necessary to preclude the possibility of interrupting the keying cycle at the wrong position. The letter selected as a separator (J or V for example) was often excluded from the enciphering matrix, this being essential to avoid ambiguity in the decryption.

c. This particular method suffers from an obvious fault. Since successive words vary in length in an extremely irregular manner, the process then results in the destruction of obvious periodicity. Note that individual words are being enciphered in monoalphabetic terms. Thus, solution is quite simple. If standard alphabets are involved, completion of the plain component will lead to an immediate solution. If, on the other hand, mixed alphabets are used, idiomorphism remains and provides a relatively. easy entry.

d. In those cases where idiomorphic patterns are not obvious, the word separator may be used as an initial entry. A word separator may be either a plaintext value or a cipher value. The plaintext value will be enciphered and somewhat more difficult to recognize. If, however, it is a constant cipher value, it should be readily apparent. In either case, once isolated, word separators serve to distinguish individual words, thus providing a basis for analysis through a study of the uniliteral characteristics of the words.

14-3. (₵) Numerically Keyed Encipherment

a. Another method of varying the plaintext is by using variable plaintext groupings which are not successive words. In this method the plaintext is divided into segments of predetermined lengths. Again, in the encipherment process, one alphabet is used to encipher each group. The key cycle of encipherment extends through a number of groups, then begins anew at its initial point once one key cycle is completed. Group length may exhibit a patterned regularity as shown in figure 14–1.

Key		1	2	3	4	5	6	1	2	3	4
Group		1	2	3	4	5	1	2	3	4	5
	P	C	OM	MAN	DING	GENER	A	LF	IRS	TARM	YHASI
	C	*Q*	*UW*	*UGT*	*KFAH*	*UWNWJ*	*L*	*HN*	*ARQ*	*NGPU*	*PGNVF*
Key		5	6	1	2	3	4	5	6	1	2
	P	S	SU	EDO	RDER	SEFFE	C	TI	VET	WENT	YFIRS
	C	*I*	*TR*	*OPE*	*RFER*	*OCBBC*	*L*	*HS*	*QHS*	*WOFZ*	*KDARQ*
Key		3	4	5	6	1	2	3	4	5	6
	P	T	AT	NOO	NDIR	ECTIN	G	TH	ATT	ELEP	HONES
	C	*N*	*NU*	*NMM*	*YIDU*	*OQZKF*	*C*	*NZ*	*NUU*	*WPWL*	*EXYHT*
Key		1	2	3	4	5	6	1	2	ooo	
	P	C	OM	MAS	WITC	HBOAR	D	SC	OMM	ooo	
	C	*Q*	*UW*	*UGO*	*RFUL*	*TZMAJ*	*I*	*AQ*	*UWW*	*ooo*	

C *QUWUG TKFAH UWNWJ LHNAR QNGPU PGNVF ITROP ERFER*

OCBBC LHSQH SWOFZ KDARQ NNUNM MYIDU OQZKF CNZNU

UWPWL EXYHT QUWUG ORFUL TZMAJ IAQUW W...

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T
2	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J
3	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H
4	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O
5	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
6	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M

Figure 14-1 (₵). Encipherment by arbitrary group length (U).

Group length may also be varied, the key of the matrix is used for this purpose. For example, assuming a keyword TRACK, a numeric key of 54123 can be generated. Thus, the text would be divided into groups of 5, 4, 1, 2, and 3 letters, the cycle being repeated throughout the message. Encipherment would then follow the same method of encipherment as shown in figure 14–1 above, each group being enciphered by one alphabet. For example:

Alphabet Key	1	2	3	4	5	6	1	2
Group Key	5	4	1	2	3	5	4	1
P	COMMA	DING	G	EN	ERA	LFIRS	TARM	Y
C	*QEGGS*	*FAVC*	*A*	*JA*	*WJA*	*AGDUT*	*ZSBG*	*K*

b. The example in figure 14–1 serves to illustrate one of the faults of arbitrary group division. In theory, when the keying element is kept constant and the plaintext groupings are made variable, even though the key is used cyclically, external periodicity will be suppressed. Note that when the plaintext grouping contains similar letters, and when the cycle of variable grouping is applied several times to the message, periodicity can occur. The two occurrences of *QUWUG* illustrate this point. They are separated by an interval of 90 letters; their plaintext letters, their group size, and their key letters are the same, thus they constitute a true periodic repetition. Also of interest is that 30 groups intervene. Since the length of the key is 6, the cycle is repeated 5 times; thus, in the case of true periodicity, the interval of 90 is the product of the total number of letters in the key multiplied by the number of cycles of the key.

c. The repetition of *ARQN* is of another type, termed partial periodic to distinguish it from the former. In this case the interval is 39 letters. It is true that this repetition involves similar plaintext values IRST, but involves different cyclic groupings. Note also that the points within the two groupings are different. In the first case the repetition begins with the first letter of group 3 and ends on the first letter of group 4. In the second appearance it commences at the third letter of group 5 and ends on group 1. However, it should be observed that the number of key groups intervening between the two repetitions (twelve), is the product of the maximum number of key groups (six), multiplied by the number of repetitions of the key (two).

Section II. ~~(C)~~ SOLUTION OF SIMPLE APERIODIC SYSTEMS

14–4. ~~(C)~~ Solution of Numerically Keyed Encipherment

a. Solution of numerically keyed encipherment follows essentially the same step as that shown in the preceding example regardless of whether the individual groups are of increasing length through the cycle or are irregularly mixed. Initial identification of the system may be somewhat difficult, its recognition resting largely on two characteristics. First, any uniliteral distribution of the ciphertext will be relatively flat, similar to a periodic system. Second, it may be distinguished from a periodic system in that observed repetitions will not factor evenly in all cases. Moreover, in a long message enciphered by either system there are usually many repetitions of both types so that identification might hinge on the availability of outside information to determine the basic system.

b. Once the system is recognized, analysis may take one of two courses depending upon the alphabets used. Where the system involves either the use of standard cipher alphabets or known mixed cipher alphabets produced by the sliding of a mixed component against the normal sequence, solution may be accomplished by completing the plain component. In such cases bits of plaintext will be found on several different generatrices. The number of plaintext letters appearing successively on one generatrix is the same as the number enciphered at one setting of the numerical key. This is illustrated in figure 14–2 which shows the completed plain component and its accompanying matrix.

```
C   B D K T H C B M J Y H V T M B H F S L G F R T

    C E L U I D C N K Z I W U N C I G T M H G S U
    D F M V J E D O L A J X V O D J H U N I H T V
    E G N W K F E P M B K Y W P E K I V O J I U W
    F H O X L G F Q N C L Z X Q F L J W P K J V X
    G I P Y M H G R O D M A Y R G M K X Q L K W Y
    H J Q Z N I H S P E N B Z S H N L Y R M L X Z
    I K R A O J I T Q F O C A T I O M Z S N M Y A
    J L S B P K J U R G P D B U J P N A T O N Z B
    K M T C Q L K V S H Q E C V K Q O B U P O A C
    L N U D R M L W T I R F D W L R P C V Q P B D
    M O V E S N M X U J S G E X M S Q D W R Q C E
    N P W F T O N Y V K T H F Y N T R E X S R D
    O Q X G U P O Z W L U I G Z O U S F Y T S E
    P R Y H V Q P A X M V J H A P V T G Z U T F
                  B
                  C
                  D
                  E
```

Numerical Key 4-3-1-2-6-5
POINTS

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
C2	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
C3	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
C4	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
C5	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
C6	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R

Figure 14–2 (~~C~~). *Numerically keyed encipherment, standard alphabets* (*U*).

	5	10	15	20	25
A	*HZNZH*	*ZPDAF*	*RZVPB*	*XZLCA*	*QBOBV*
B	*RBIGH*	*IIMAR*	*UHBJB*	*YTWVX*	*RSYHI*
C	*XAKWH*	*VHQQE*	*IMMXZ*	*DDWKG*	*YPXFI*
D	*EJFQP*	*VUXRV*	*ABVGC*	*VXQRM*	*BXUGB*
E	*LRDDS*	*LXBAE*	*AFAZQ*	*PAVIC*	*MBAIW*
F	*KVHQP*				

Figure 14–3 (~~C~~). *Aperiodic cipher message* (*U*).

c. In the case where the primary components are a mix of known and unknown sequences, solution is possible through the application of idiomorphism and the principles of direct symmetry of position. To illustrate the methods involved in this approach, the message in figure 14–3 will be used.

(1) A brief inspection of the ciphertext reveals the sequence *HZNZHZ*, which is significant under two conditions. First, the cipher is numerically keyed; the possibility exists that this sequence is the product of the application of one key, the number of letters enciphered corresponding to one setting of the key. If this is true, it represents a period of monoalphabetic encipherment and the idiomorphic pattern ABCBAB may be used in assuming a plaintext word. Second, if a known sequence was used as either component, direct symmetry of position can be used. Assuming both conditions to exist, a list of idiomorphic patterns is searched to locate a word which matches the pattern derived. Among others, the word REFERENCE is noted. This is an ideal word for opening a message. Then, assuming a standard sequence was used for the plain component, the following preliminary matrix may be set down:

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C					*Z*	*N*												*H*								

(2) Thus the above results in the following plaintext insertions:

```
                 5       10
A     C  HZNZH  ZPDAF  RZVPB  XZLCA
      P  REFER  ENCE
```

Logically REFERE should be expanded to REFERENCE, thus providing additional equivalencies. The problem that arises, however, is the determination of the length of the group, i.e. how far does monoalphabeticity extend in this case. A consideration of the word itself reveals that it must break between A6 and A9, for the last Ep value at A9 is *Ac* and the last repeated monoalphabetic bit is Ep=*Zc* at A6. A second cipher component, when Np=*Pc*, may be inscribed in the matrix:

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1					*Z*	*N*												*H*								
C2			*D*		*A*									*P*												

(3) At this point the question of what would be the most profitable method of attack must be considered. Should we expand the plaintext, or apply the principle of direct symmetry of position? Perhaps the two can be incorporated. But first, the matrix should be examined. Note the occurrence of the *Zc* and *Nc* in adjacent positions in cipher alphabet 1. If the initial word assumption is correct, the cipher component is not a standard alphabet. Mixed sequences may be derived by decimation, keyword, transposition, or by random methods. However, if the cipher sequence is keyword mixed, *Zc Nc* is significant in that it may mark the end of the sequence and the beginning of the keyword. The letter *Hc* appearing 12 spaces to the right may represent, in this case, a portion of the sequence where alphabetic sequencing is resumed; its distance from *Nc* makes it improbable as a part of the keyword. In any case, if each successive secondary cipher alphabet is but a different juxtaposition of one basic sequence, then the principle of direct symmetry of position will apply. But to be used, the same letters in several alphabets must be found.

(4) Perhaps such a hit may be discovered by expanding on the assumption of the plaintext. The assumption of the word REFERENCE should lead to the further assumption of the phrase REFERENCE YOUR MESSAGE, or REFERENCE MY MESSAGE. Neither may be right, but they are worthy of consideration until proven untrue. Accordingly, the following may be inscribed:

```
                      5         1 0        1 5        2 0
A     C    H Z N Z H   Z P D A F   R Z V P B   X Z L C A
      P    R E F E R   E N C E Y   O U R M E   S S A G E
```

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1					*Z*	*N*												*H*								
C2														*P*												
C3			*D*																							
C4					*A*																					
C5																									*F*	
C6															*R*											
C7																					*Z*					
C8																		*V*								
C9													*P*													
C10					*B*																					
C11																			*X*							
C12																			*Z*							
C13	*L*																									
C14								*C*																		
C15					*A*																					

Figure 14-4 (~~C~~). Expansion of matrix (U).

Using the equivalencies, the matrix may be expanded further. However, each letter must temporarily occupy a separate horizontal line because the points where the keys are changed are unknown except in the case where SSp=*XCc*. Thus, the matrix would appear as in figure 14-4.

(5) Several interesting patterns indicative of key changes may be observed in the matrix. First is the assumed value of Sp for *Xc* and *Zc* in alphabets 11-12. If the assumption is correct, then this is a point of key change. Note also that there are four values for Ep shown, *Zc* in alphabet 1, *Ac* in 4, *Bc* in 10, and again *Ac* in alphabet 15. Thus four key changes are indicated in a period of 15 letters, one period being a repetition of another in respect to the point of juxtaposition. Moreover, *Hc* in alphabet 1 and *Vc* in alphabet 8 are noted as equalling Rp. On the basis of these patterns an indication of the periods may be shown as follows:

```
C   H Z N Z H   Z/P D A F   R Z/V P B   X/Z L C A
P   R E F E R   E/N C E Y   O U/R M E   S/S A G E
```

It must be understood that this delimitation of periods is arbitrary, only serving to limit some possibilities and providing a basis for either proving or disproving previous assumptions.

(6) The matrix may now be rearranged in order to compare the patterns (fig. 14–5).

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1					*Z*	*N*												*H*								
C2			*D*		*A*									*P*	*R*						*Z*				*F*	
C3					*B*								*P*					*V*	*X*							
C4	*L*				*A*		*C*												*Z*							

Figure 14–5 (¢). Matrix reduction (U).

Examination of alphabet 2 shows the *Zc* followed by *Ec*, *Dc*, and *Ac* at intervals of 4, 8, and 10 spaces respectively. Accepting the *Zc* as the end of the alphabetic sequence, and the space to its right as the beginning of the keyword, these values then can be inserted into the sequence of alphabet 1 using the principle of direct symmetry of position:

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1					*Z*	*N*			*F*			*D*		*A*				*H*								

This leaves the occurrence of the sequence *PRc* as equivalencies of the sequence NOp in alphabet 2 to be explained. It may be possible that Q is part of the keyword, for where else could it appear in light of the assumed *PRc* sequence? This placement is unlikely. Therefore, the sequence in this position may be incorrect. Moreover, note that the *Pc*=Np equivalency appears in the initial reconstruction matrix prior to the *Rc*=Op equivalency in cipher alphabets 2 and 6 respectively. Therefore, they may not have been drawn from the same alphabet. In this case *Qc* could have come from a preceding alphabet. If so, it would fall prior to *Hc*, out of sequence except as a part of the keyword. This does not seem likely, so it may be set aside for the moment.

(7) The third alphabet may now be considered. Four spaces, normally occupied by the letters *QRSTU*, are observed intervening between the letter *Pc* and *Vc*, although no space is noted between *Vc* and *Xc*, which is usually occupied by the *Wc*. Perhaps the *Wc* and one of the letters *RSTU* (*Q* being discounted) may be part of the keyword. Assuming that in the unknown cipher sequence that *Xc* and *Yc* will precede *Zc*, this sequence can be incorporated into the sequence thusly:

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1		*V*	*X*	*Y*	*Z*	*N*			*F*			*D*		*A*	*B*			*H*					*P*			

By maintaining similar spacing *Bc* may also be placed in its proper position relative to *Ac*. The *Pc* now falls into proper sequence.

(8) This leavcs only the fourth sequence to be fitted, which appears to be quite easy as *Ac* and *Zc* have been placed. However, when the fitting is attempted it will be found that the sequential relationships are incorrect. Counting from *Zc* to *Lc* an interval of 8 is noted, thus placing *Lc* below Mp, in the protosequence, and adjacent to *Ac* below Np, yet *Lc* and *Ac* are separated by one space in the fourth sequence. Referring to the ciphertext with its assumed plaintext shown in (5) above, it is observed that the equivalancies of *Lc* and *Ac* are separated by the *Cc*=Gp equivalency. This inconsistency may be explained by another key change, *Zc*, *Lc*, and *Cc* from one alphabet and *Ac* from another. Accepting this for the moment, it is found they can be fitted, thereby retaining the previously established sequence.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1		*V*	*X*	*Y*	*Z*	*N*			*F*			*D*	*L*	*A*	*B*	*C*		*H*					*P*			

d. With the partially recovered cipher sequence, the recovery of the matrix and decipherment of the cryptogram may be started. This is a simultaneous effort, and the values found are transferred from one to the other. First, a matrix which will produce the correct plain-to-cipher equivalencies for the assumed plaintext is constructed. A separate strip is prepared for each period of use, as shown in figure 14–6. Note that in so doing *Rc* can be placed in the third sequence, a value which is immediately transferred. Also, because of spacing, *Qc* is inserted and transferred.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	P	S	T	U	V	W	X	Y	Z
6 C1		*V*	*X*	*Y*	*Z*	*N*			*F*			*D*	*L*	*A*	*B*	*C*		*H*					*P*	*Q*	*R*	
3 C2			*D*	*L*	*A*	*B*	*C*		*H*					*P*					*V*	*X*	*Y*	*Z*	*N*			*F*
7 C3		*D*	*L*	*A*	*B*	*C*		*H*					*P*	*Q*	*R*			*V*	*X*	*Y*	*Z*	*N*			*F*	
2 C4	*L*	*A*	*B*	*C*		*H*					*P*	*Q*	*R*			*V*	*X*	*Y*	*Z*	*N*			*F*			*D*
4 C5			*D*	*L*	*A*	*B*	*C*		*H*					*P*	*Q*	*R*			*V*	*X*	*Y*	*Z*	*N*			*F*

Key	1	2	3	4	5	
Group	6	3	7	2	4	
A	*HZNZH*	*ZPDAF*	*RZVPB*	*XZLCA*	*QBOBV*	*RBIGH*
	REFER	ENCEY	OURME	SSAGE	OF	
B	*IIMAR*	*UHBJB*	*YTWVX*	*RSYHI*	*XAKWH*	
C	*VHQQE*	*IMMXZ*	*DDWKG*	*YPXFI*	*EJFQP*	
D	*VUXRV*	*ABVGC*	*VXQRM*	*BXUGB*	*LRDDS*	
E	*LXBAE*	*AFAZQ*	*PAVIC*	*MBAIW*	*KVHQP*	

Figure 14–6 (~~C~~). Partial matrix and recoveries of plaintext (U).

(1) At the fifth period it is discovered that further decipherment using the juxtapositions found is no longer possible, thus another key change for an undetermined period is indicated. In this case two sliding strips should be constructed to test the assumption of possible words, keeping in mind that one juxtaposition will render plaintext for an undetermined number of letters. In context with the assumed plaintext it seems logical to expect a time reference to follow. Accordingly, the words ZERO, ONE, or TWO may be assumed. The strips are then juxtaposed to produce the required values. If the assumption is correct, then all assumed equivalencies must match.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
C		*D*	*L*	*A*	*B*	*C*		*H*					*P*	*Q*	*R*			*V*	*X*	*Y*	*Z*	*N*			*F*	*O*				

(2) After a short period of experimentation the strip above will be found which will produce the assumed ZERO plus the letters E - - H. This confirms the ZERO assumption and E - - H possibly represents the word EIGHT. Accordingly, the cipher values can be inserted in the matrix (fig. 14–7) which would now appear as:

P		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
6	C1		*V*	*X*	*Y*	*Z*	*N*			*F*	*O*		*D*	*L*	*A*	*B*	*C*	*G*	*H*	*I*				*F*	*Q*	*R*	
3	C2	*O*		*D*	*L*	*A*	*B*	*C*	*G*	*H*	*I*				*P*	*Q*	*R*			*V*	*X*	*Y*	*Z*	*N*			*F*
7	C3		*D*	*L*	*A*	*B*	*C*	*G*	*H*	*I*				*P*	*Q*	*R*			*V*	*X*	*Y*	*Z*	*N*			*F*	*O*
2	C4	*L*	*A*	*B*	*C*	*G*	*H*	*I*				*P*	*Q*	*R*			*V*	*X*	*Y*	*Z*	*N*			*F*	*O*		*D*
4	C5	*O*		*D*	*L*	*A*	*B*	*C*	*G*	*H*	*I*				*P*	*Q*	*R*			*V*	*X*	*Y*	*Z*	*N*			*F*
8	C6		*D*	*L*	*A*	*B*	*C*	*G*	*H*	*I*				*P*	*Q*	*R*			*V*	*X*	*Y*	*Z*	*N*				*O*

Figure 14–7 (~~C~~). Insertion of cipher values (U).

(3) Observation of the periods used show that they are 6–3–7–2–4–8, thus key periods 1 and 5 are missing, also possibly 9 and 0. A glance at the cryptogram reveals that the groups *IIMAR UHBJB* immediately follow that which gives ZERO EIGHT. Then, where Tp of EIGHT equals *Ic*, the second *Ic* must also equal Tp. Therefore, this period could be five. In any event, it can quickly be determined by alining the two sequences so *Ic* equals Tp. In so doing, Wp is found to equal *Mc*. The matrix may now be transcribed as shown in figure 14–8.

P		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
6	C1		*V*	*X*	*Y*	*Z*	*N*			*F*	*O*		*D*	*L*	*A*	*B*	*C*	*G*	*H*	*I*			*M*	*P*	*Q*	*R*	
3	C2	*O*		*D*	*L*	*A*	*B*	*C*	*G*	*H*	*I*			*M*	*P*	*Q*	*R*			*V*	*X*	*Y*	*Z*	*N*			*F*
7	C3		*D*	*L*	*A*	*B*	*C*	*G*	*H*	*I*			*M*	*P*	*Q*	*R*			*V*	*X*	*Y*	*Z*	*N*			*F*	
2	C4	*L*	*A*	*B*	*C*	*G*	*H*	*I*			*M*	*P*	*Q*	*R*			*V*	*X*	*Y*	*Z*	*N*			*F*	*O*		*D*
4	C5	*O*		*D*	*L*	*A*	*B*	*C*	*G*	*H*	*I*			*M*	*P*	*Q*	*R*			*V*	*X*	*Y*	*Z*	*N*			*F*
8	C6		*D*	*L*	*A*	*B*	*C*	*G*	*H*	*I*			*M*	*P*	*Q*	*R*			*V*	*X*	*Y*	*Z*	*N*				*O*
5	C7			*V*	*X*	*Y*	*Z*	*N*			*F*	*O*		*D*	*L*	*A*	*B*	*C*	*G*	*H*	*I*			*M*	*P*	*Q*	*R*

Figure 14–8 (~~C~~). *Transcription of matrix* (*U*).

(4) The values of TTWOZp for *IIMARc*, derived by alphabet C7 above, provide the clue that the juxtaposition of the eighth alphabet in the *Uc* of the group *UHBJBc* must equal Ep to provide an E for ZERO. However, note that no U placement exists for the cipher sequence. Perhaps the U placement may be inferred by elimination from the information at hand. In the sequence *R – – V* above, two spaces intervene which should be occupied by either S, T, or U. Obviously, one of these must be part of the keyword. Considering each vacant space in turn, the following letters can be placed. The remaining letters are assumed to be part of the keyword. This may be observed in the following:

```
N   FO  DLABCGHIJKLMPQ    VXYZ
E  R  S  T  U  W
```

(5) Considered in this light it takes little imagination to recognize a probable keyword in NEWFOUNDLAND. Accordingly, the values are inserted and the matric recovered as shown in figure 14–9. Note that a key is recovered which explains the sequence of periods used.

P		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
6	C1	*T*	*V*	*X*	*Y*	*Z*	*N*	*E*	*W*	*F*	*O*	*U*	*D*	*L*	*A*	*B*	*C*	*G*	*H*	*I*	*J*	*K*	*M*	*P*	*Q*	*R*	*S*
3	C2	*O*	*U*	*D*	*L*	*A*	*B*	*C*	*G*	*H*	*I*	*J*	*K*	*M*	*P*	*Q*	*R*	*S*	*T*	*V*	*X*	*Y*	*Z*	*N*	*E*	*W*	*F*
7	C3	*U*	*D*	*L*	*A*	*B*	*C*	*G*	*H*	*I*	*J*	*K*	*M*	*P*	*Q*	*R*	*S*	*T*	*V*	*X*	*Y*	*Z*	*N*	*E*	*W*	*F*	*O*
2	C4	*L*	*A*	*B*	*C*	*G*	*H*	*I*	*J*	*K*	*M*	*P*	*Q*	*R*	*S*	*T*	*V*	*X*	*Y*	*Z*	*N*	*E*	*W*	*F*	*O*	*U*	*D*
4	C5	*O*	*U*	*D*	*L*	*A*	*D*	*C*	*G*	*H*	*I*	*J*	*K*	*M*	*P*	*Q*	*R*	*S*	*T*	*U*	*X*	*Y*	*Z*	*N*	*E*	*W*	*F*
8	C6	*U*	*D*	*L*	*A*	*B*	*C*	*G*	*H*	*I*	*J*	*K*	*M*	*P*	*Q*	*R*	*S*	*T*	*V*	*X*	*Y*	*Z*	*N*	*E*	*W*	*F*	*O*
5	C7	*S*	*T*	*V*	*X*	*Y*	*Z*	*N*	*E*	*W*	*F*	*O*	*U*	*D*	*L*	*A*	*B*	*C*	*G*	*H*	*I*	*J*	*K*	*M*	*P*	*Q*	*R*
1	C8	*E*	*W*	*F*	*O*	*U*	*D*	*L*	*A*	*B*	*C*	*G*	*H*	*I*	*J*	*K*	*M*	*P*	*Q*	*R*	*S*	*T*	*U*	*X*	*Y*	*Z*	*N*

Figure 14–9 (~~C~~). *Recovered matrix* (*U*).

Using this matrix and the period sequence shown, further decipherment of the cryptogram is merely a cryptographic task.

e. A very important point is that the solution presented above represents but one method which is possible only because of the circumstances involved in producing the cryptogram. First, the message contained a stereotyped beginning. Second, the stereotype was discernible in the ciphertext, as the initial period of key usage 6–3–7–2 was sufficiently long to produce an idiomorphic pattern. Third, the use of a standard sequence for the plain component and a keyword mixed sequence for the ciphertext permitted the use of direct symmetry of position. Thus the solution was relatively simple. However, had one or more of these factors been different, that is, smaller key periods, a different cipher sequence derived by a more complicated method, or two unknown sequences, the final solution would have been more difficult if not impossible. A solution is possible where the analyst has some preknowledge concerning the system, its contents, or operation, in the case of small samples. Where this knowledge is not available with the information presented to this point, only one other means of solution is possible. That is, through the acquisition of sufficient depth, so that values can be played against one another. This particular technique will be illustrated in succeeding paragraphs.

14–5. (~~C~~) Analysis of Variable Length Keying Units

a. The preceding examples dealt with the use of variable length plaintext groupings enciphered with a constant length key element as one means of introducing aperiodicity into a system. Aperiodicity, avoiding external periodicity, may also be introduced by the reversal of the same techniques, that is, by holding the plaintext units constant while applying a variable length keying unit. The most common method of producing a variable length keying unit, where the base keying unit is limited or fixed in length, is by irregularly interrupting it. Thus a cyclic keying sequence, which would normally produce periodic phenomena in the ciphertext, would now introduce an aperiodic element instead.

b. There are several methods which may be used to interrupt a normal cyclic key, all of which may be classified into one of three general types. The types are:

(1) The keying sequence merely stops at some

point in the sequence, succeeding points differing irregularly, and resumes at the initial starting point after each stop. An example of this encipherment is depicted below using the preceding matrix.

Base Key Sequence 1–2–3–4–5–6–7–8

Key Element	1	2	3	4	*	1	2	3	*	1	2	3	4	5	6	*	1	2	* etc.
Letter Number	1	2	3	4		5	6	7		8	9	10	11	12	13		14	15	etc.
Plaintext	R	E	F	E		R	E	N		C	E	M	Y	M	E		S	S	etc.
Ciphertext	*H*	*A*	*C*	*G*		*H*	*A*	*Q*		*X*	*A*	*P*	*U*	*M*	*B*		*I*	*V*	etc.

(2) One or more elements of the base key are dropped irregularly during each keying cycle. On the completion of one cycle the base sequence is resumed again, with different elements dropped by prearrangement between the cryptographers. This method is depicted below.

Base Key Sequence 1–2–3–4–5–6

Key Element	2	3	4	5	*	1	2	5	*	1	3	4	5	6	*	2	3	4	*	1	2 ect.
Letter Number	1	2	3	4		5	6	7		8	9	10	11	12		13	14	15		etc.	
Plaintext	R	E	F	E		R	E	N		C	E	M	Y	M		E	S	S		etc.	
Ciphertext	*T*	*B*	*H*	*A*		*H*	*A*	*P*		*X*	*B*	*R*	*W*	*P*		*A*	*X*	*Z*		etc.	

(3) The base key sequence is applied to the text, alternating irregularly in direction, with or without the omission of elements. The base key sequence is reapplied in the same manner throughout the text. The example below illustrates this method.

Base Key Sequence 1–2–3–4–5–6–7

Key Element	1	2	3	4	5	*	4	3	*	4	5	6	7	*	5	4	3	2	1	etc.
Letter Number	1	2	3	4	5		6	7		8	9	10	11		12	13	14	15	16	etc.
Plaintext	R	E	F	E	R		E	N		C	E	M	Y		M	E	S	S	A	etc.
Ciphertext	*H*	*A*	*C*	*B*	*T*		*G*	*Q*		*B*	*A*	*P*	*Q*		*M*	*G*	*X*	*V*	*T*	etc.

Note that in this method, if no key elements were omitted and the key sequence was repeated, it could be treated as though it was a 16-element key sequence rather than an interrupted system. The cryptographic effect of it is the same.

14-6. ~~(C)~~ Periodic Patterns in Aperiodic Systems

a. Although aperiodicity is introduced into a system by this method, certain patterns are retained which, if recognized, may be exploited for a solution. The first of these patterns arises through the successive use of the same basic key sequence. For example, if the analyst knows the points of interruption, the several cycles of a given message may be stacked upon themselves to produce bits of monoalphabetic encipherment. Of course, the longer the message the greater the size of the bits, and consequently the more useful this method is. The stacking of successive cycles to illustrate the bits of monoalphabetic encipherment is shown below. Note the repeated cipher letters that occur; each represents the encipherment of a single plaintext letter.

(1) Method 1.

Key Element	1	2	3	4	5	6	7	8
Letter Number	1	2	3	4				
Ciphertext	*H*	*A*	*C*	*G*				
	5	6	7					
	H	*A*	*Q*					
	8	9	10	11	12	13		
	X	*A*	*P*	*U*	*M*	*B*		
	14	15	16	17	18	19	20	21
	I	*V*	. . . . etc.					
	22	23						
	24	25	26	27	. . . etc.			

(2) Method 2.

```
Key Element     1   2   3   4    5    6
Letter Number       1   2   3    4
Ciphertext          T   B   H    A
                5   6            7
                H   A            P
                8       9   10   11   12
                X       B   R    W    P
                    13  14  15 . . . etc.
                    A   X   Z
```

(3) Method 3.

```
Key Element     1   2   3   4   5   6   7
Letter Number   1   2   3   4   5
Ciphertext      H   A   C   B   T
                        7   6
                        G   Q
                            8   9   10  11
                            B   A   P   Q
                16  15  14  13  12
                T   V   X   Q   M
```

Obviously the ability to stack successive sections of a message by the successive sections of a keying sequence is predicated on the preknowledge of both the key sequence and its points of interruption. This technique is primarily applicable in those cases where past analysis has resulted in the determination of the system, its key, and its use.

b. Other patterns which may occur in systems of this type are the familiar idiomorphs. They may represent a complete word or a part of a word. These patterns arise as a consequence of similar portions of plaintext being enciphered by similar portions of the keying sequence. Where the point of interruption falls on a given word consistently, particularly in the case of method 1 above, this phenomena is likely to result. For example, note the situation in figure 14–10.

```
                 1 2 3 * 1 2 3 4 * 1 2 3 4 5 6 ... KEY
Message A    P   R E T   R E A T   W I L L B E ... PLAIN
             C   G S B   G S I G   L W T Y U W ... CIPHER

                 1 2 3 4 5 * 1 * 1 2 3 4 5 6 * 1 ... KEY
Message B    P   O U R A T   T   A C K W I L   L ... PLAIN
             C   D I Z N M   I   P Q S J B D   A ... CIPHER

                 1 2 * 1 1 2 3 4 5 6 * 1 2 3 4 ... KEY
Message C    P   A T   T A C K O N O   U R L E ... PLAIN
             C   P H   I P Q S B G G   J F T R ... CIPHER
```

Figure 14–10 (~~C~~). Idiomorphs formed in encipherment (U).

Observe that the patterns so produced may be both idiomorphic, as $\overset{\text{R E T R E}}{}$ in the case of the pattern ABCAB for *G S B G S* in message A, or merely repetitions as in the case of $\overset{\text{T A C K}}{I\ P\ Q\ S}$ in messages B and C. Obviously then, the usefulness of these is limited by the chance of their happening. That is, their production rests upon the accidental occurrence of fortunate circumstances.

c. A more important pattern, in terms of usefulness to the cryptanalyst, lies in the repeated use of the same starting point in a sequence of keying elements in a number of messages. Where this occurs, monoalphabeticity is present in the columns formed when a number of messages of the same system are superimposed. Note that the initial sequence of keying elements must be constant and that the messages superimposed must all be from the same system. Also, the greater the depth, the more pronounced the monoalphabeticity exhibited by each column. This is particularly applicable in the case of short messages, because the number of messages, not their length, is the important criteria when all other factors are constant. To observe the significance of this, note the superimposed messages and the frequency distribution derived from the first 10 columns so formed in figure 14–11.

Message No.	Letter Number 1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	Z	C	T	P	Z	W	Z	P	E	P	Z	Q	X	
2	W	T	E	Q	M	X	Z	S	Y	S	P	R	C	
3	T	C	R	W	C	X	T	B	H	H				
4	E	F	K	C	S	Z	R	I	H	A				
5	Y	A	N	C	I	H	Z	N	U	W				
6	V	Z	I	E	T	I	R	R	G	X				
7	H	C	Q	I	C	K	G	U	O	N				
8	Z	C	F	C	L	X	R	K	Q	W				
9	H	W	W	P	T	E	W	C	I	M	J	S		
10	E	P	D	O	Z	C	L	I	K	S	J			
11	W	T	S	S	Q	Z	P	Z	I	E	T			
12	Z	C	G	G	Y	F	C	S	B	G				
13	C	W	Z	A	O	O	E	M	H	W	T	P		
14	C	I	Y	G	I	F	B	D	T	V	X			
15	E	A	Q	D	R	D	N	S	R	C	A	P	D	T
16	Y	F	W	C	Q	Q	B	Z	C	W	C			
17	W	T	E	Z	Q	S	K	U	H	C				
18	Z	C	V	X	Q	Z	K	Z	Y	D	W	L	K	
19	A	F	E	O	J	T	D	T	I	T				
20	K	P	V	F	Q	W	P	K	T	E	V			
21	Z	A	B	G	R	T	X	P	U	Q	X			
22	Y	H	E	O	C	U	H	M	D	T				
23	C	L	C	P	Z	I	K	O	T	H				
24	A	F	L	W	W	Z	Q	M	D	T				
25	Z	C	W	A	P	M	B	S	A	W	L			
26	H	F	L	M	H	R	Z	N	A	P	E	C	E	
27	C	L	Z	G	E	M	K	Z	T	O				
28	T	P	Y	F	K	O	T	I	Z	U	H			
29	Z	C	C	P	S	N	E	O	P	H	D	Y	L	
30	C	I	Y	G	I	F	T	S	Y	T	L	E		
31	Y	T	S	V	W	V	D	G	H	P	G	U	Z	
32	N	O	C	A	I	F	B	J	B	L	G	H	Y	
33	Z	X	X	F	L	F	E	G	J	L				
34	Z	C	T	M	M	B	Z	J	O	O				
35	H	C	Q	I	W	S	Y	S	B	P	H	C	Z	V

Letter Number

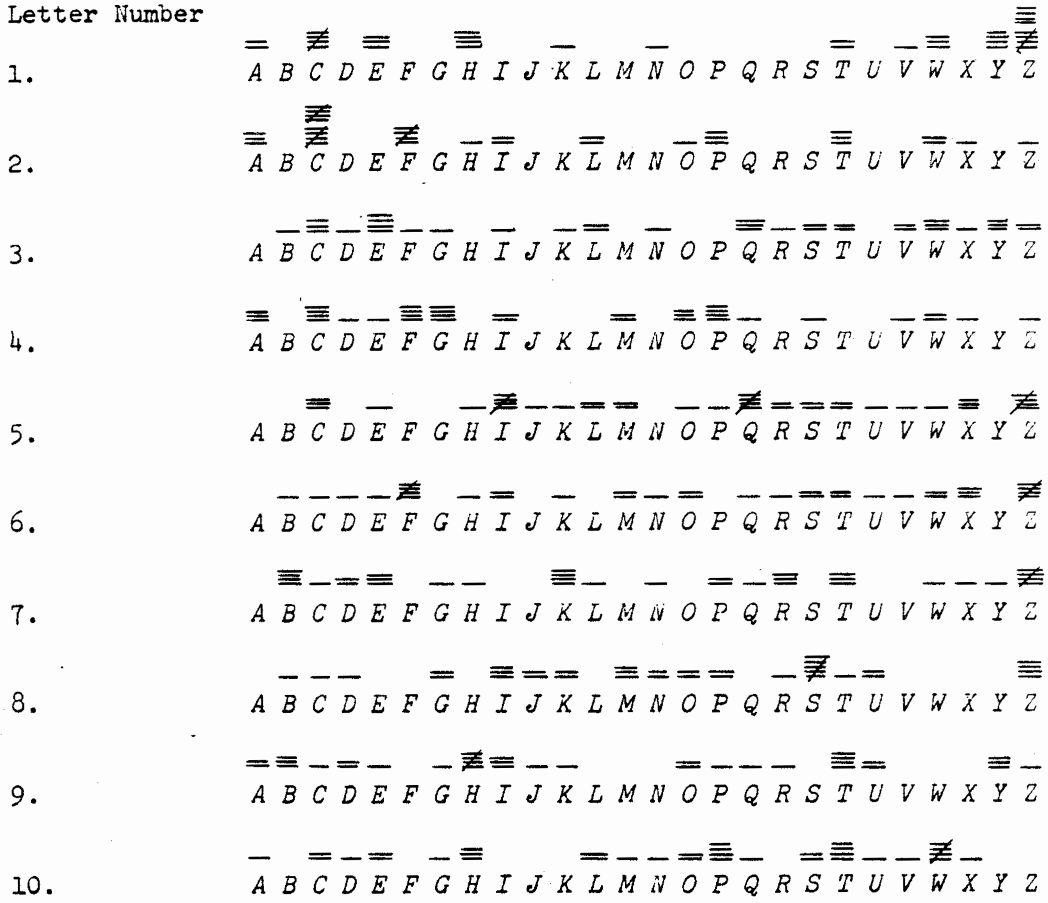


Figure 14–11 (~~C~~). Frequency distribution columns 1–10 (U).

(1) The first and second distributions are certainly monoalphabetic. The peaks and troughs are pronounced, and the number of blanks, considering the size of the samples, corresponds with that expected. But note that the same pattern is lost in the remaining alphabets. This may be explained by a change in the successive points of interruption.

(2) Assuming that the first, second, and possibly third columns are monoalphabetic, the possibility of an entry is provided, based upon the assumption of probable words. Recall that most military messages are prone to stereotypes, particularly in beginnings and endings. Thus words such as REFERENCE, REFER, REQUEST, ENEMY, IN, etc., are commonly found. High-frequency digraphs used in the initial portions of common words are observable in the first two or three columns. For example, in the first two columns above, the following digraphs can be found:

ZC-7	*WT*-3	*HC*-2
CI-2	*AF*-2	*CL*-2

14-7. (~~C~~) Interruptions

a. To this point, only the results of the keying-sequence interruption have been discussed. No mention has been made of that element which determines how the interruption takes place. For this purpose, either a letter of the ciphertext or of the plaintext may be used, the exact letter being agreed upon in advance. Since there is nothing fixed relative to the time of interruption, it will appear quite irregularly, exhibiting no distinctive pattern or cyclic periodicity. Whether the letter itself is a ciphertext or plaintext letter is of no importance. Interruption, in the case of a plaintext letter, takes place after that letter is enciphered. In the case of a ciphertext letter, the interruption occurs after the selected letter is produced by the enciphering process.

b. The source of the letter selected for use as an interrupter letter is significant in that it may have a direct bearing on the solution of a cryptogram. This may be seen in figure 14-12 where the interrupter is a plaintext letter.

```
Key------B U S I N E S S M A C H I|B U S|B U S I|B U S I N E|
Plain---A M M U N I T I O N F O Ⓡ|F I Ⓡ|S T A Ⓡ|T I L L E Ⓡ|
Cipher--B O L Y R P J D R O J K X|K J F|Y X S X|D J U P S Y|

Key------B U S I N E S S M A C H I N E S B U|B U S I N E S S M A C H I|
Plain---Y W I L L B E L O A D E D A F T E Ⓡ|A M M U N I T I O N F O Ⓡ|
Cipher--I Y D P Y F X U R A F A E N M J J V|B O L Y R P J D R O J K X|

Key------B U S I|B U S|B U S I N E|B U S I N
Plain---T H I Ⓡ|D A Ⓡ|T I L L E Ⓡ|Y . . . .
Cipher--D G D X|G U F|D J U P S Y|I . . . .
```

Cryptogram

```
B O L Y R   P J D R O   J K X K J   F Y X S X   D J U P S   Y I Y D P
Y F X U R   A F A E N   M J J V B   O L Y R P   J D R O J   K X D G D
X G U F D   J U P S Y   I X X X X
```

(Rp) Interruptor letter

P		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	1	*B*	*E*	*F*	*G*	*J*	*K*	*M*	*N*	*O*	*P*	*Q*	*S*	*T*	*V*	*W*	*X*	*Z*	*H*	*Y*	*D*	*R*	*A*	*U*	*L*	*I*	*C*
	2	*U*	*L*	*I*	*C*	*B*	*E*	*F*	*G*	*J*	*K*	*M*	*N*	*O*	*P*	*Q*	*S*	*T*	*V*	*W*	*X*	*Z*	*H*	*Y*	*D*	*R*	*A*
	3	*S*	*T*	*V*	*W*	*X*	*Z*	*H*	*Y*	*D*	*R*	*A*	*U*	*L*	*I*	*C*	*B*	*E*	*F*	*G*	*J*	*K*	*M*	*N*	*O*	*P*	*Q*
	4	*I*	*C*	*B*	*E*	*F*	*G*	*J*	*K*	*M*	*N*	*O*	*P*	*Q*	*S*	*T*	*V*	*W*	*X*	*Z*	*H*	*Y*	*D*	*R*	*A*	*U*	*L*
	5	*N*	*O*	*P*	*Q*	*S*	*T*	*V*	*W*	*X*	*Z*	*H*	*Y*	*D*	*R*	*A*	*U*	*L*	*I*	*C*	*B*	*E*	*F*	*G*	*J*	*K*	*M*
	6	*E*	*F*	*G*	*J*	*K*	*M*	*N*	*O*	*P*	*Q*	*S*	*T*	*V*	*W*	*X*	*Z*	*H*	*Y*	*D*	*R*	*A*	*U*	*L*	*I*	*C*	*B*
	7	*M*	*N*	*O*	*P*	*Q*	*S*	*T*	*V*	*W*	*X*	*Z*	*H*	*Y*	*D*	*R*	*A*	*U*	*L*	*I*	*C*	*B*	*E*	*F*	*G*	*J*	*K*
	8	*A*	*U*	*L*	*I*	*C*	*B*	*E*	*F*	*G*	*J*	*K*	*M*	*N*	*O*	*P*	*Q*	*S*	*T*	*V*	*W*	*X*	*Z*	*H*	*Y*	*D*	*R*
	9	*C*	*B*	*E*	*F*	*G*	*J*	*K*	*M*	*N*	*O*	*P*	*Q*	*S*	*T*	*V*	*W*	*X*	*Z*	*H*	*Y*	*D*	*R*	*A*	*U*	*L*	*I*
	10	*H*	*Y*	*D*	*R*	*A*	*U*	*L*	*I*	*C*	*B*	*E*	*F*	*G*	*J*	*K*	*M*	*N*	*O*	*P*	*Q*	*S*	*T*	*V*	*W*	*V*	*Z*

Figure 14-12 (~~C~~). Plaintext letter as interrupter (U).

(1) In this example, the plaintext letter R was selected as the interrupter letter. Each time Rp appears, the key is changed following its encipherment, then the key reverts to its initial starting point. As a consequence of using a high-frequency letter, repetitions will occur quite often. This is true because a high-frequency letter will be a part of many common words, because it will be followed quite often by the same letter, and also because the word in which it appears may be followed by words that are frequently repeated. Thus each time the word ARTILLERY appears in the plaintext, the cipher equivalents of TILLERY must be the same because the key sequence reverts to its initial position following the encipherment of the R. If a low-frequency letter was selected as a plaintext interrupter, then each cycle of key usage would be greatly extended, resulting in an approximation of periodic substitution with the probability of numerous repetitions.

(2) Although the length of the intervals between repetitions in any of the foregoing cases would be irregular, thus suppressing periodicity, the length of each interval is normally sufficient to permit solution by two general methods. First, if the cipher alphabets are known from the results of prior analysis, and the cryptogram to be deciphered merely represents a key change, solution would be possible through the probable-word method. Second, repetitions found in the text would be examined in the light of their presence being due to a stereotype word. A probable word, then selected, would be applied in successive juxtaposition to the ciphertext. Using the known sequences, a key letter for each letter of the probable word would be derived. The process would be continued until such time as an intelligible key sequence was found or the probable word disproved. In the latter case, a different probable word would be assumed and the same process repeated.

c. In the example above, a plaintext letter served as the interrupter letter. But suppose the correspondents had agreed upon a ciphertext letter instead. In this case the same message, using the same key and cipher sequences, would now appear as shown in figure 14–13.

```
Key--------B U S I N E S S M A C H I N E S B U S I N E S S M|
Plain------A M M U N I T I O N F O R F I R S T A R T I L L E|
Cipher-----B O L Y R P J D R O J K X T P F Y X S X B P U U Q|

Key--------B U S I N E S S M A C H I N|B U S I N E S S M A C H|B U|
Plain------R Y W I L L B E L O A D E D|A F T E R A M M U N I T|I O|
Cipher-----H R N M Y T T X H P C R F Q|B E J F I E L L B O N Q|O Q|

Key--------B U S I N E S S|M A C H|B U S I N E
Plain------N F O R T H I R|D A R T|I L L E R Y
Cipher-----V E C X B O D F|P A Z Q|O N U F I C

                          Cryptogram

B O L Y R   P J D R O   J K X T P   F Y X S X   B P U U Q   H R N M Y
T T X H P   C R F Q B   E J F I E   L L B O N   Q O Q V E   C X B O D
F P A Z Q   O N U F I   C X X X X

Qc = Interruptor letter
```

Figure 14–13 (~~C~~). Cipher letter as interrupter (U).

Note that in this example there are no significant repetitions. This is due only to the selection of *Qc* as the interrupter. Had another letter been chosen, repetitions might have been plentiful. For example, note the repetitions occurring in the message shown in figure 14–14 when *Sc* is used as an interrupter.

```
Key--------B A N D S B A N D S B A N D S B A N D S B A N|B A N D S B A N D S B
Plain------F R O M F O U R F I V E T O F O U R F I F T E|E N A M B A R R A G E
Cipher----K T A K Z W X I I D A C B N Z W X I I D K W S|J O N K T B T I D H J
```

Sc = Interruptor letter

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1	*B*	*E*	*F*	*G*	*J*	*K*	*M*	*N*	*O*	*P*	*Q*	*S*	*T*	*V*	*W*	*X*	*Z*	*H*	*Y*	*D*	*R*	*A*	*U*	*L*	*I*	*C*
C2	*A*	*U*	*L*	*I*	*C*	*B*	*E*	*F*	*G*	*J*	*K*	*M*	*N*	*O*	*P*	*Q*	*S*	*T*	*V*	*W*	*X*	*Z*	*H*	*Y*	*D*	*R*
C3	*N*	*O*	*P*	*Q*	*S*	*T*	*V*	*W*	*X*	*Z*	*H*	*Y*	*D*	*R*	*A*	*U*	*L*	*I*	*C*	*B*	*E*	*F*	*G*	*J*	*K*	*M*
C4	*D*	*R*	*A*	*U*	*L*	*I*	*C*	*B*	*E*	*F*	*G*	*J*	*K*	*M*	*N*	*O*	*P*	*Q*	*S*	*T*	*V*	*W*	*X*	*Z*	*H*	*Y*
C5	*S*	*T*	*V*	*W*	*X*	*Z*	*H*	*Y*	*D*	*R*	*A*	*U*	*L*	*I*	*C*	*B*	*E*	*F*	*G*	*J*	*K*	*M*	*N*	*O*	*P*	*Q*

Figure 14–14 (Ȼ). Repetitions as a result of interrupter letter encipherment (U).

(1) This last example provides a clue which may be used as an entry. Note that in this case the key is short, thus the key sequence is repeated several times before being interrupted. This of itself provides the possibility of repeated segments between periods of interruption. In such cases as above, where cipher repeats appear closely, the intervening letters between repeats may be eliminated from consideration as interrupter letters. Thus *Ac*, *Cc*, *Bc*, and *Nc* may be eliminated from consideration.

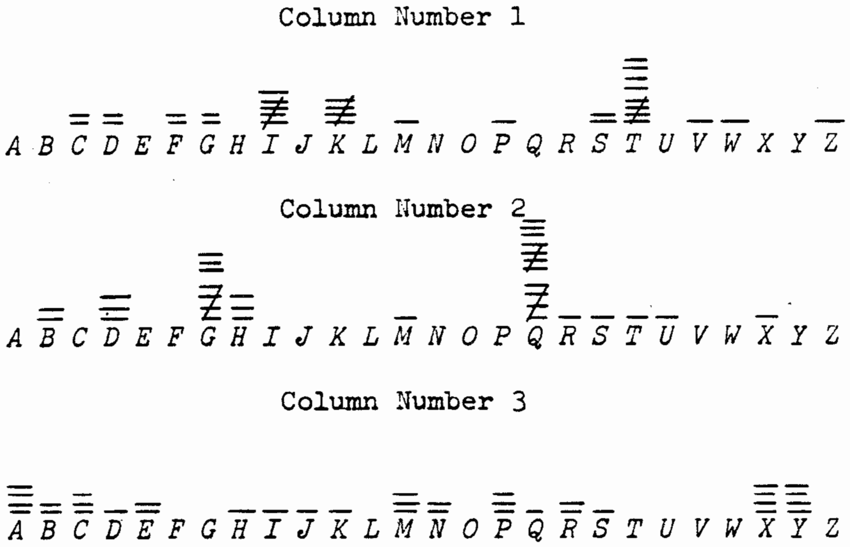
(2) Insofar as analysis is concerned, two possibilities are presented: superimposition or direct attack. In the first case, if the interrupter can be identified, the message may be divided into segments, each representing a key sequence run, and stacked as shown previously, the columns so formed being monoalphabetic. One difference in respect to the use of probable words should be noted. In cases similar to this, the analyst works from the inside of the message. That is, he attempts to find a given word in the body of the message. This is a much more difficult task than attacking the beginning of a message. This of course applies only to the case of stacking one message upon itself. Should depth of 30 to 40 messages of the same system and key be available, this system can be solved more readily by superimposition. In the second case, a direct attack upon an individual message is possible, but unless it contains some inconsistency in its text it can be a very difficult problem.

14–8. (Ȼ) Solution by Superimposition

a. As mentioned previously in the case of both numerically keyed and interrupter-letter encipherment, solution is best accomplished by superimposition which requires a depth of messages known to be from the same system. The solution will be made easier if the analyst has some preknowledge concerning the possible contents of the message. Here the knowledge of common stereotyped beginnings is invaluable. The general techniques used in this approach are demonstrated in the following paragraphs.

b. The first two or three groups constituting the beginning of the message are selected from messages produced by the same system, superimposed to form a column. A uniliteral frequency distribution is made of these columns. Normally only the first two or three columns are so treated, because it is assumed that beyond this point the use of an interrupter in some of the messages will destroy columnar monoalphabeticity. This process is demonstrated in figure 14–15.

1. T Q P F Y I N G C R F K E X C
2. I G X P J C T R F K E X G F W
3. S Q E Q X E T E T I R A X D X
4. M G Q D F P N Z Y M O R T Y T
5. T Q P P X C F N E T I N Q X P
6. F M A B M R H Z K T C G D T S
7. K B Y T D H C K H T M G J R Z
8. I U E R B G K Q D A P P Z Q A
9. I G Y I X G X P Y Z K Q X Q R
10. T Q C F T B R I U W Q E Z U Y
11. T Q B Z B Z F K F Z Z T I R A
12. P Q A L A T K Q D F P N Z Y M
13. D G S B J I B M K B Q A T S B
14. T Q M P O N L Q O G Z Q D F P
15. I G X B J G L N Y Z Z E L A G
16. G H N H H M K T S N B X L R Z
17. C H M F T I R A X D X D N N F
18. I G Y I R G C N H A E F U G I
19. W T R N C N M H E Y U A H H K
20. V D N E F A Y Z K Q X C M F T
21. T Q C P F Y A E Q D D T R N C
22. Z G I U Y L R X G F I T O O D
23. K R W T S P U Z E D M G I N J
24. T Q B Z X A U S P B F R M D X
25. T Q X C F O L Y G D J T B V F
26. I G X S N G M A Y Z O Z F T Q
27. K B Y P S Y Q E X S D Y I R G
28. G X C P C J F O O J N I A R A
29. F D D Y S D Y I R G C J L M E
30. D Q R Y H R H Z K T C G D T R
31. C H A P Q G A Z E M G Q D F P
32. K D A L K J L M S L P W Q D K
33. K S H G R O J N Q Z N H O Q A
34. S Q P F X R J G A R L Z B C W
35. T Q M P O A Q F M L Z Y W F P



TQP 2	*IGX* 3	*TQ* 9
TQC 2	*IGY* 2	*IG* 5
TQB 2		
TQM 2		
TQX 1		

Figure 14–15 (¢). *Frequency distribution and polygraphs of superimposed columns* (*U*).

c. The distribution derived from the first three columns exhibits several interesting characteristics. Note that the first distribution shows a pattern similar to that expected for a monoalphabetic distribution, but that the second has two peaks which seem abnormally high. These two peaks probably represent two vowels. The third distribution is somewhat flatter than the first. This may be the result of a key change occurring in several of the messages included in the distribution at this point. Considering these possibilities, the repeated trigraphs and digraphs observed may be examined for possible stereotype words.

(1) The repeated *TQc* digraph followed an equal number of times by *Pc*, *Cc*, *Dc*, and *Mc* is characteristic of the digraph REp in typical message beginnings, such as REQUEST, REFERENCE, REFER, RECEIPT, RECOMMEND, etc., and provides a ready point for initial assumptions. The only problem is associating the correct word with the correct digraph. In some instances the frequency of individual patterns compared to the

expected frequency of digraphs and trigraphs may provide a clue. In others such as this, where similar frequencies are involved, final resolution is merely a matter of trial and error. With this in mind and accepting that *TQc* is REp, the following associations are arbitrarily made.

P	REC	REP	REQ	REF
C	*TQP*	*TQC*	*TQB*	*TQM*

(2) Using the assumed equivalencies and assuming that the plain component is a direct standard alphabet, a matrix may now be set up as follows (fig. 14–16).

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1																		*T*								
C2					*Q*																					
C3			*P*			*M*										*C*	*B*									

Figure 14–16 (C). Initial placement of values (U).

(3) The assumed values for the third alphabet reveal two distinctive patterns that indicate the type alphabet involved. Note that *Rc*- -*Mc* and *CBc* are in reverse order, and also that the values involved are reciprocal, that is Cp=*Pc* and Pp=*Cc*. As the two patterns are characteristic of a reversed standard alphabet, this configuration is inserted in all three cipher sequences (fig. 14–17). The assumption being that, as in most cases, the secondary sequences are derived from the successive juxtaposition of two basic sequences.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1	*K*	*J*	*I*	*H*	*G*	*F*	*E*	*D*	*C*	*B*	*A*	*Z*	*Y*	*X*	*W*	*V*	*U*	*T*	*S*	*R*	*Q*	*P*	*O*	*N*	*M*	*L*
C2	*U*	*T*	*S*	*R*	*Q*	*P*	*O*	*N*	*M*	*L*	*K*	*J*	*I*	*H*	*G*	*F*	*E*	*D*	*C*	*B*	*A*	*Z*	*Y*	*X*	*W*	*V*
C3	*R*	*Q*	*P*	*O*	*N*	*M*	*L*	*K*	*J*	*I*	*H*	*G*	*F*	*E*	*D*	*C*	*B*	*A*	*Z*	*Y*	*X*	*W*	*V*	*U*	*T*	*S*

Figure 14–17 (C). Completion of assumed sequences (U).

(4) Using this matrix, the first three columns of each message beginning are now deciphered as shown in figure 14–18.

```
1.  C  T Q P F Y I N G C R F K E X C
    P  R E C
2.  C  I G X P J C T R F K E X G F W
    P  C O U
3.  C  S Q E Q X E T E T I R A X D X
    P  S E N
4.  C  M G Q D F P N Z Y M O R T Y T
    P  Y O B
5.  C  T Q P P X C F N E T I N Q X P
    P  R E C
6.  C  F M A B M R H Z K T C G D T S
    P  F I R         T
7.  C  K B Y T D H C K H T M G J R Z
    P  A T T
8.  C  I U E R B G K Q D A P P Z Q A
    P  C A N
9.  C  I G Y I X G X P Y Z K Q X Q R
    P  C O T
10. C  T Q C F T B R I U W Q E Z U Y
    P  R E P
11. C  T Q B Z B Z F K F Z Z T I R A
    P  R E Q
12. C  P Q A L A T K Q D F P N Z Y M
    P  V E R
13. C  D G S B J I B M K B Q A T S B
    P  H O Z
14. C  T Q M P O N L Q O G Z Q D F P
    P  R E F
15. C  I G X B J G L N Y Z Z E L A G
    P  C O U
16. C  G H N H H M K T S N B X L R Z
    P  E N E
17. C  C H M F T I R A X D X D N N F
    P  I N F
18. C  I G Y I R G C N H A E F U G I
    P  C O T
19. C  W T R N C N M H E Y U A H H K
    P  O B A
20. C  V D N E F A Y Z K Q X C M F T
    P  P R E
21. C  T Q C P F Y A E Q D D T R N C
    P  R E P
22. C  Z G I U Y L R X G F I T O O D
    P  L O J
23. C  K R W T S P U Z E D M G I N J
    P  A D V
24. C  T Q B Z X A U S P B F R M D X
    P  R E Q
25. C  T Q X C F O L Y G D J T B V F
    P  R E U
26. C  I G X S N G M A Y Z O Z F T Q
    P  C O U
27. C  K B Y P S Y Q E X S D Y I R G
    P  A T T
28. C  G X C P C J F O O J N I A R A
    P  E X P
29. C  F D D Y S D Y I R G C J L M E
    P  F R O
30. C  D Q R Y H R H Z K T C G D T R
    P  H E A
31. C  C H A P Q G A Z E M G Q D F P
    P  I N R
32. C  K D A L K J L M S L P W Q D K
    P  A R R
33. C  K S H G R O J N Q Z N H O Q A
    P  A C K
34. C  S Q P F X R J G A R L Z B C W
    P  S E C
35. C  T Q M P O A Q F M L Z Y W F P
    P  R E F
```

Figure 14–18 (~~C~~). Insertion of plaintext values (U).

(5) Several of the trigraphs so produced can easily be expanded to full words. Among these are:

REC	RECOMMEND or RECEIVE
FIR	FIRST
ATT	ATTACK or ATTENTION
CAN	CANCEL
REQ	REQUEST or REQUIRE
COU	COUNTER
ENE	ENEMY
INF	INFANTRY or INFORMATION

Other trigraphs seem to be impossible combinations of letters. Among these are:

YOB	OBA
COT	LOJ
HOZ	INR

This may be explained by a period of interruption occurring somewhere in the first two positions of these messages. In respect to this, note that, with the exception of INR, the letter "O" is common to all.

(6) To test the possibility of a key change being involved, a fourth cipher sequence for those seemingly good trigraphs can be constructed. The equivalencies thus established then can be tested against those which seem improbable. If the tetragraphs produced seem illogical, a key change may be assumed. Thus the following is produced:

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C4	*T*	*S*	*R*	*Q*	*P*	*O*	*N*	*M*	*L*	*K*	*J*	*I*	*H*	*G*	*F*	*E*	*D*	*C*	*B*	*A*	*Z*	*Y*	*X*	*W*	*V*	*U*

Using this sequence, the trigraphs assumed to be good may now be expanded to:

1.	C	*TQPF*	7.	C	*KBYT*
	P	RECO		P	ATTA
2.	C	*IGXP*	8.	C	*IUER*
	P	COUE		P	CANC
3.	C	*SQEQ*	16.	C	*GHNH*
	P	SEND		P	ENEN
6.	C	*FMAB*	17.	C	*CHMF*
	P	FIRS		P	INFO

(7) Each of the tetragraphs produced by this sequence conforms to the words assumed, with the exception of number 2. But note again that the O appears as plaintext. Moreover the same sequence applied to the improbable trigraphs now produces the following:

YOBQ	HOZS	LOJZ
COTL	OBAG	INRE

Thus a key change is indicated, and since O appears in all except INRE, which now appears to be two words (IN RE), it may be tentatively accepted as the interrupter letter. This being the case, the obvious step is to confirm this assumption by trying to decipher these groups that revert back to cipher sequence 1 each time the Op appears. Doing this, we find that the questionable groups now produce:

2.	C	*IGXP*	19.	C	*WTRN*
	P	CONF		P	ORDE
		*			*
4.	C	*MGQD*	22.	C	*ZGIU*
	P	YOUR		P	LOCA
		*			*
9.	C	*IGYJ*	31.	C	*CHAP*
	P	COMM		P	INRE

(8) The appearance of valid plaintext confirms the assumption of Op as the interrupter letter. The final solution is now quite simple. Knowing the sequence of the cipher and plain components, and having identified the interrupter letter, all that remains to reconstruct the system is to determine the number of alphabets involved and their respective juxtapositions. This can be done by selecting one or more messages in which the probably word or words contain no O and juxtaposing the sequences to produce the known ciphertext. When the points of juxtaposition repeat, the full key length is reproduced. Thus, the matrix size is determined. For example:

6. *F M A B M R H Z K T C G D T S*
F I R S T A R T I L L E R Y

7. *K B Y T D H C*
A T T A C K

8. *I U E R B G K*
C A N C E L L

14. *T Q M P O N L Q O*
R E F E R E N C E

Key K U R T F R Y S S E N | K U R

The matrix may now be reconstructed as shown in figure 14–19, and each message deciphered.

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C1	*K*	*J*	*I*	*H*	*G*	*F*	*E*	*D*	*C*	*B*	*A*	*Z*	*Y*	*X*	*W*	*V*	*U*	*T*	*S*	*R*	*Q*	*P*	*O*	*N*	*M*	*L*
C2	*U*	*T*	*S*	*R*	*Q*	*P*	*O*	*N*	*M*	*L*	*K*	*J*	*I*	*H*	*G*	*F*	*E*	*D*	*C*	*B*	*A*	*Z*	*Y*	*X*	*W*	*V*
C3	*R*	*Q*	*P*	*O*	*N*	*M*	*L*	*K*	*J*	*I*	*H*	*G*	*F*	*E*	*D*	*C*	*B*	*A*	*Z*	*Y*	*X*	*W*	*V*	*U*	*T*	*S*
C4	*T*	*S*	*R*	*Q*	*P*	*O*	*N*	*M*	*L*	*K*	*J*	*I*	*H*	*G*	*F*	*E*	*D*	*C*	*B*	*A*	*Z*	*Y*	*X*	*W*	*V*	*U*
C5	*F*	*E*	*D*	*C*	*B*	*A*	*Z*	*Y*	*X*	*W*	*V*	*U*	*T*	*S*	*R*	*Q*	*P*	*O*	*N*	*M*	*L*	*K*	*J*	*I*	*H*	*G*
C6	*R*	*Q*	*P*	*O*	*N*	*M*	*L*	*K*	*J*	*I*	*H*	*G*	*F*	*E*	*D*	*C*	*B*	*A*	*Z*	*Y*	*X*	*W*	*V*	*U*	*T*	*S*
C7	*Y*	*X*	*W*	*V*	*U*	*T*	*S*	*R*	*Q*	*P*	*O*	*N*	*M*	*L*	*K*	*J*	*I*	*H*	*G*	*F*	*E*	*D*	*C*	*B*	*A*	*Z*
C8	*S*	*R*	*Q*	*P*	*O*	*N*	*M*	*L*	*K*	*J*	*I*	*H*	*G*	*F*	*E*	*D*	*C*	*B*	*A*	*Z*	*Y*	*X*	*W*	*V*	*U*	*T*
C9	*S*	*R*	*Q*	*P*	*O*	*N*	*M*	*L*	*K*	*J*	*I*	*H*	*G*	*F*	*E*	*D*	*C*	*B*	*A*	*Z*	*Y*	*X*	*W*	*V*	*U*	*T*
C10	*E*	*D*	*C*	*B*	*A*	*Z*	*Y*	*X*	*W*	*V*	*U*	*T*	*S*	*R*	*Q*	*P*	*O*	*N*	*M*	*L*	*K*	*J*	*I*	*H*	*G*	*F*
C11	*N*	*M*	*L*	*K*	*J*	*I*	*H*	*G*	*F*	*E*	*D*	*C*	*B*	*A*	*Z*	*Y*	*X*	*W*	*V*	*U*	*T*	*S*	*R*	*Q*	*P*	*O*

Figure 14–19 (~~C~~). Completion of matrix (U).

PART SIX (¢)

INTRODUCTORY CODE SYSTEMS

CHAPTER 15 (¢)

CODE SYSTEMS

Section I. (¢) INTRODUCTION

15-1. (¢) Classification of Code Systems

Codes differ from ciphers in two respects. First, a group of symbols (letters, numbers, or a mixture of both) is used to represent a letter, syllable, word, phrase, or sentence of plaintext. Second, as they are not generated by an enciphering process, they do not bear the same relationship to the structure of the underlying plaintext as does a cipher. As code systems are arbitrary in nature, each group having its own assigned value, they require the use of books, lists, charts, etc., to tabulate the codes and their meanings. Codes may be classified by the number and type of documents used.

a. Open codes are systems of disguised secret writing in which units of normal plaintext are used as the code equivalent for letters, numbers, words, etc., of the plaintext message. They can be, and often are, combined to form an intelligible text of an apparently innocent message. An example of such an open code message is the poem passed by BBC on 1 June 1944 warning the French underground that the invasion of France was to be launched in less than 2 weeks:

LES SANGLOTS LONGS
DES VIOLONS
DE L'AUTOMNE

Another example is the following message passed to Secretary of War Stimson at the Potsdam Conference to advise him of the success of the explosion of the first atomic bomb at Alamogordo, New Mexico.

DOCTOR HAS JUST RETURNED MOST ENTHUSIASTIC AND CONFIDENT THAT THE LITTLE BOY IS AS HUSKY AS HIS BIG BROTHER. THE LIGHT IN HIS EYES DISCERNIBLE FROM HERE TO HIGHHOLD AND COULD HAVE HEARD HIS SCREAMS FROM HERE TO MY FARM.

The BIG BROTHER referred to in the preceding message is the atomic bomb dropped on Hiroshima on 6 August 1945.

b. Book codes are code systems in which the code groups are contained in bound documents, arranged in some systematic order. They may be classified as either one- or two-part codes.

(1) A one-part code is a code in which the plaintext element and its corresponding code group are contained in one document, arranged in alphabetic, numeric, or other systematic order. This is an example of a one-part code:

165	GAS ALERT OFF
166	GAS ALERT ON
167	GAS ATTACK READY
168	GAS HAS BEEN RELEASED
169	GAS HAS BLOWN BACK
170	GAS HAS CEASED TO BE RELEASED
171	GAS WILL BE RELEASED AT (TIME)

(2) A two-part code is a randomized code system consisting of an encoding book and a decoding book, or sections of either. In the encoding book or section, the plaintext equivalents are arranged in alphabetical or numerical order, the code groups being assigned at random. In the decoding section or book, the code groups are arranged in a systematic order, alphabetical or numerical, and are accompanied by their meanings as given in the encoding section. The significant difference between two-part codes and one-part codes is that, in the former, the sequential relationship between code groups and plaintext does not exist. For example, compare the two-part code shown in figure 15-1 with the one-part code above.

ENCODING SECTION

W E I P	2583	Intercept ing ion or s	F I P I	0514	Key s
X I G L	2756	- station	C U F Z	0255	Ki
K A X P	1072	Intercepted	K A K B	1059	Kill ing s
R O T B	2043	Interdict ing ion s	F Y V M	0595	Killed
W O G L	2631	Interdicted	C I Q M	0215	Kilocycle s
Q O P Y	1889	Interfere ing nce s (in)	H O D U	0828	Kilometer s
G A V Q	0620	Interfered (in) (with)	V Y R U	2541	Kind s (of)
X A X D	2722	Intermediate	G Y K Z	0734	Kitchen s
H I Z R	0824	Intermittent ly	N O P A	1589	Knew
B O G C	0081	Interpreter s	Q A G T	1806	Knot s
Z E I N	2883	Interrogate ing ion s	Q Y X E	1947	Know ing s
L A V M	1220	Interrupt ing ion s	K Y T F	1193	Knowledge (of)
M Y E P	1479	Interrupted	L Y X I	1347	Known
H A M F	0761	Intersect ing ion s	F I K D	0509	Ko
Z U S T	2967	Interval s (of)	M O K W	1434	Ku

DECODING SECTION

H A L E	0760	Few	H I G H	0815	Meteorological
M F	61	Intersect ing ion s	R I	16	Allowance s (for)
N G	62	Short ly	S K	17	Demoralize ation ing s
O H	63	Circular s	T L	18	Presence (of)
P I	64	U	U M	19	Altogether
H A Q K	0765	Centimeter s	H I V N	0820	USS
R L	66	Repulse ing s	W O	21	Release ing s
S M	67	Your message (No.)	X P	22	Fi
T N	68	Assembly point s	Y Q	23	Well
U O	69	Runner s	Z R	24	Intermittent ly
H A V P	0770	Air base s	H O A R	0825	Strengthened
W Q	71	River s	B S	26	Often
X R	72	Mask ing s	C T	27	Void
Y S	73	Built	D U	28	Kilometer s
Z T	74	Gain ing s	E V	29	Favorable y

Figure 15-1 (~~C~~). Two-part code (U).

15-2. (~~C~~) Matrix Codes

a. Matrix codes as a class represent a transition between cipher and code systems. They may range from simple syllabary squares correctly classed as ciphers to code charts which include a small vocabulary of words and phrases. Generally, matrix codes follow closely the cryptographic principles of multiliteral systems treated previously. They differ from cipher systems primarily in their construction. In cipher systems, excepting the monome-dinome and monome-dinome-trinome systems, the ratio between plain and cipher elements is nearly constant. Matrix codes, however, have no definite ratio. Substitution of values may involve constant-length code groups for variable-length plaintext units composed of a mixture of letters, syllables, words, phrases, or sentences. An example of a typical matrix code is shown in figure 15-2.

	38	39	40	41	42	43	44	45	46
25	A	ADVANCE	AMMO	AN	AND	ATTACK	B	BE	C
26	CA	CALIBER	CO	D	DE	DIVISION	E	EAST	EN
27	ENEMY	ER	F	FLANK	FOR	FROM	G	H	HAS
28	HAVE	HQ	I	IN	INFO	ING	IT	J	K
29	L	LE	M	MACH GUN	MENT	MSG	N	NE	NO
30	NORTH	O	OF	ON	ORDER	P	POSI TION	Q	R
31	RE	REGT	REPORT	REQUEST	S	SE	SECTOR	SEND	SOUTH
32	STOP	SUPPORT	T	TANK	BEGIN SPELL	THAT	TION	U	END SPELL
33	V	W	WEST	WILL	X	Y	Z	ZERO	1
34	2	3	4	5	6	7	8	9	0

Sample Message:

REPORT	BEGIN SPELL	NE	W	END SPELL	POSITION	OF	REGT	STOP
3140	3242	2945	3339	3246	3044	3040	3139	3238

Figure 15–2 (C). Matrix code (U).

b. The cryptographic operation of the system is quite simple, following the same methods as given for multiliteral systems. For example, the plaintext message:

REPORT NEW POSITION OF REGIMENT

is enciphered as:

3140 3242 2945 3339 3246 3044 3040 3139 3238

Note that each plaintext value is represented by the row and column indicator which intersected at the position of the desired plaintext value. Thus *3140* equates to REPORT. Note also that words which do not appear in the chart are spelled out, as in the case of NEW which is represented by two code groups, *2945*=NE and W=*3339*. This characteristic, in conjunction with specific groups which indicates when to begin spell (*3242*) and when to end spell (*3246*) is a means of entry into the system.

c. A variant form of the matrix code illustrated in figure 15–3 is the so-called "upper and lower case" matrix code. Essentially it is similar to the normal matrix code, only so structured as to contain two plaintext values in each cell. Thus the capacity of the matrix is doubled and variant plaintext values for the equivalent code group are introduced. The cryptographic operation of this system is similar to that of the foregoing with one exception. That is, in this system at least two groups which normally have but one plain value are set aside to indicate whether the groups following are upper or lower case. An example of this system and the method of its operation are shown in figure 15–3.

	1	2	3	4	5
ØØ	A AMMO	1 ARTY	AND ATTACK	AT BARRAGE	AN BATTALION
13	B BATTERY	2 BEGIN	BE BRIDGE	BY CAPTURE	 LOWER CASE
25	C CASUALTY	3 COMMAND	CA COMMUNI-CATION	CE COMPANY	CO CROSSROADS
37	D DAILY	4 DASH	DA DISPOSI-TION	DE DIVISION	 UPPER CASE
49	DO EAST	DR EMPLACE-MENT	E ENEMY	5 EQUIP-MENT	ED EVERY

Sample message:

```
BEGIN ATTACK AT 1245 HOURS AND CAPTURE BRIDGE 321.

BEGIN  ATTACK  UPPER CASE  AT   1    2    4    5
132    ØØ3     375         ØØ4  ØØ2  132  372  494

AND  LOWER CASE  CAPTURE  BRIDGE  UPPER CASE
ØØ3  135         134      133     375

3    2    1
252  132  ØØ2
```

Figure 15–3 (~~C~~). Upper case, lower case, matrix code (U).

Although a system of this type introduces variant values, i.e. the code group *252* may indicate either the number 3 or the word COMMAND, it does not provide a great deal more security than the normal matrix code. Its chief advantage lies in the inclusion of a long vocabulary.

d. Syllabary codes are used either to supplement a book code by adding a means of expanding its vocabulary, or to provide a flexible means of secret communications. As in all matrix codes, it appears in the form of a matrix. However, the contents of the matrix are normally limited to letters, numbers, and syllables. Cryptographically, it is also similar to multiliteral systems, having row and column coordinates for the purpose of designating the plaintext element within the cells of the matrix. A sample of a syllabary square is shown in figure 15–4.

	1	2	3	4	5	6	7	8	9	0
1	A	1	AL	AN	AND	AR	ARE	AS	AT	ATE
2	ATI	B	2	BE	C	3	CA	CE	CO	COM
3	D	4	DA	DE	E	5	EA	ED	EN	ENT
4	ER	ERE	ERS	ES	EST	F	6	G	7	H
5	8	HAS	HE	I	9	IN	ING	ION	IS	IT
6	IVE	J	Ø	K	L	LA	LE	M	ME	N
7	ND	NE	NT	O	OF	ON	OR	OW	P	Q
8	R	RA	RE	RED	RES	RI	RO	S	SE	SH
9	ST	STO	T	TE	TED	TER	TH	THE	THI	THR
0	TI	TO	U	V	VE	W	WE	X	Y	Z

Figure 15–4 (~~C~~). Syllabary square (U).

The system provides for all the letters of the alphabet, the cardinal numbers, and the more common polygraphs. Also, the placement of the plaintext elements are such that the finding of any value is easy for the cryptographer. In effect, the system above provides variant values by the inclusion of both letters and polygraphs, without variant row and column coordinates. For example, the word reconnaissance could appear in ciphertext as:

```
 R   E   C   O   N   N   A   I   S   S  AN  CE  or
 81  35  25  74  60  60  11  54  88  88  14  28
RE  CO   N   N   A  IS   S  AN  CE  or
 83  29  60  60  11  59  88  14  28
 R   E  CO   N   N   A  IS   S   A   N   C   E  or
 81  35  29  60  60  11  59  88  11  60  25  35
RE   C  ON   N   A  IS   S  AN   C   E  etc.
 83  25  76  60  11  59  88  14  25  35
```

e. Code charts are similar to the syllabary square in that they are of like dimensions and operate on the same cryptographic principles. A significant difference between the two is that the code chart containing words and phrases is normally designed to serve a specific function, while the syllabary square has more general application. Further, the code chart, being limited in intent, normally contains less internal variants. An example of these facets of a code chart may be seen in one of its more common applications: an operator's code. A code chart of this type contains those common words, phrases, operating signals, and words that relate directly to the establishment and maintenance of communications between two points. Provision is made for the cardinal numbers and occasionally the letters of the alphabet. Although security of interoperator communications may be important in these cases, the chief object is to be the provision of a concise and rapid means of communications. Figure 15–5 depicts a type of operator code.

	0	1		3	4	5	6	7	8	9
1	1	QAP	QRA	QRM	QRN	QRO	QRP	QSA	QSU	10
2	A	Z	Read Numbers					Read Signals	20	QSP
3	B	1	3					30	QSL	GTA
4	C	J	0	4	QRK	QRL	40	W	Routine	
5	D	K	P	S	5	50	U	X	Priority	
6	E	L	Q	T	60	6	V	Y	Immediate	
7	F	M	R	70	QTR	QSY	7	Z	Flash	
8	G	N	80	QRX	QRX	QRZ	QRV	8	QTC	
9	H	90	Refer your Message						9	QRW
0		Read Phrases	Number	Precedence					Read Letters	0

Figure 15–5 (~~C~~). *Operator's code* (*U*).

15–3. (~~C~~) Enciphered Codes

Occasionally the code groups of coded messages undergo a further process of encipherment; the resulting cryptogram constitutes an enciphered code message. Enciphered code is used to enhance the security of a widely held code. It can be used as a means of securing messages encoded in common commercial and telegraphic codes, and it can be used when increased security is required for highly classified communications normally passed in a less secure system.

a. Both of the two general classes of cipher methods, transposition and substitution, can be used to encipher code. Encipherment by transposition is used less as it is subject to error and requires highly skilled personnel for its practical use. The bulkiness of code materials and elements makes transposition encipherment of codes unwieldy for practical military use.

b. All of the methods of substitution from the simple monoalphabetic methods to the most complex polyalphabetic systems can be used for the encipherment of code groups. Substitution tables of various sorts are often used. Tables may be used to convert 5-letter code groups to pronounceable groups of 5 letters, to convert 5-letter code groups to 5-figure code groups, or simply to convert combinations of letters into other combinations. The most important method, however, is the arithmetical method which is favored because of its simplicity and relative speed of operation as compared to that of the alphabetical methods.

c. Two basic arithmetic techniques are used. They are addition and subtraction. In both, an arbitrarily selected sequence of numbers, normally corresponding in length to the code group, is added to or subtracted from the code group using noncarrying methods. The resulting sum or quotient becomes the ciphertext for transmission. The recipient of the message has only to reverse the operation, using the same key to uncover the plain code groups. Both processes are shown in figure 15–6.

Additive:			Enciphering			
Message	ENEMY	FORCES	DEPLOYED	ALONG	RIVER	LINE
Code	*2514*	*2337*	*1233*	*0864*	*0771*	*2970*
Additive	2701	2701	2701	2701	2701	2701
Text	4215	4038	3934	2565	2472	4671
			Deciphering			
Text	4215	4038	3934	2565	2472	4671
Subtractive	2701	2701	2701	2701	2701	2701
Code	*2514*	*2337*	*1233*	*0864*	*0771*	*2970*
Message	ENEMY	FORCES	DEPLOYED	ALONG	RIVER	LINE

Subtractive:			Enciphering			
Message	ENEMY	FORCES	DEPLOYED	ALONG	RIVER	LINE
Code	*2514*	*2337*	*1233*	*0864*	*0771*	*2970*
Subtractive	0891	8709	9579	8426	7268	3984
Text	2723	4638	2764	2448	3513	9096
			Deciphering			
Text	2723	4638	2764	2448	3513	9096
Additive	0891	0709	9579	8426	7268	3984
Code	*2514*	*2337*	*1233*	*0864*	*0771*	*2970*
Message	ENEMY	FORCES	DEPLOYED	ALONG	RIVER	LINE

Figure 15–6 (¢). Arithmetic enciphered codes (U).

The additive or subtractive may be fixed or variable. Fixed additives and subtractives, i.e. a series of numbers, the same or repeating, used to encipher each code group, are particularly weak cryptographically if the basic code system contains any inherent limitations in size or sequential arrangement. If, however, a variable additive or subtractive, i.e. nonrepeating groups, is used, a much more secure system may be provided. Variable additives or subtractives are normally obtained from special tables or lists which contain a series of heterogeneous elements, none of which is used more than once. Using this method, a high degree of security may be imparted to the enciphered message, even if the basic code book is possessed by the enemy.

15–4. (¢) Disadvantages and Advantages of Code Systems

a. One great disadvantage of code systems is the sheer bulk of material required to provide a comprehensive vocabulary and the attendant problems of distribution and operation. However, code systems offer certain advantages which in some cases may outweigh the disadvantages. The advantages are:

(1) Code systems offer a more secure means of communications than most other hand systems, particularly in the case of small two-part codes which are superseded rapidly.

(2) Economy in transmission is made possible by the nature of code systems. That is, it is possible to express an entire word or thought and convey it by a single group, whereas in cipher systems the same word or thought requires a great deal more in the way of ciphertext to accomplish the same thing.

(3) Code systems are particularly adaptable to languages which are based on idiographs as are Chinese and Japanese. In Chinese for example, to allow for the transmission of idiographs, the "Chinese telegraphic code" was compiled. This code contains 10,000 characters, each represented by one code group and arranged similar to a two-part code.

b. In terms of military usage, code finds its greatest application both in brevity codes and in field codes. A brevity code has for its sole purpose the shortening of messages and is not necessarily a secret code. An example of this type code may be observed in the Q and Z signals common to telecommunications. A field code, on the other hand, is a secret code and is designed primarily for low-echelon units. Code systems which are often used for this purpose are the matrix codes given above and occasionally two-part codes with limited vocabularies. An example of this type code may be seen in the current US Army KAC–P operation codes.

Section II. (¢) ANALYSIS OF CODES

15–5. (¢) Introduction

The analysis of any code beyond the most simple form is dependent upon the availability of a volume of messages derived from the same system. The volume of messages required for successful analysis is in direct proportion to the complexity of the system. The analysis of complex systems generally presupposes the use of data processing equipment to sort, collate, and list significant repeats and characteristics observed in the raw traffic in preparation for analysis. The use of this material enables the analyst to enter the system through some identifiable characteristic. Through a preliminary study of associated communications data (callsigns, frequencies, operator chatter, etc.), characteristics of the code system (indicators, syllabary spelling, special indicators, etc.), and collateral information concerning the units and their operations, the analyst may isolate specific messages and identify certain plaintext values, such as placenames, personnel, and stereotypes which may be used to break into the code's values. In short the analysis of code systems involves the study of large volumes of material. For this reason, and since in military usage code systems find their greatest application as field codes, this section will treat only the analysis of matrix codes.

15–6. ~~(C)~~ Principles of Analysis

a. Since the cryptographic principles underlying the operation of matrix codes are similar to those of multiliteral systems, the same general techniques are used with some slight modification to fit each situation. Additionally, the characteristics themselves provide a basis for analysis of the matrix code. These characteristics are given below, and their significance in terms of analytic attack is noted. However, they are not listed in order of importance, as the applicability of each is determined by the system itself, which is subject to variation.

b. The plaintext values in a code matrix are usually arranged in some systematic order, usually alphabetically, to ease the encoding process. However, this is not always the case, for some systems may have plaintext values inserted in the cells of the matrix in random order. The significance of the former case lies in the possibility of assuming additional plaintext values and of placing questionable values. For example, in the matrix code shown in figure 15–2, note that the sequence of plaintext values in the first row of cells is "A, ADVANCE, AMMO, AN, AND, ATTACK, B, BE, and C" respectively. If the values "AMMO and AND" had been previously placed, one could obviously assume that the intervening cell would contain a plaintext value beginning with A and having either an M or N as its second letter. Of course where the plaintext values are inserted randomly, this technique is inappropriate.

c. The row and column coordinates are usually one or two digits each, forming groups of two, three, or four digits. The coordinates where numbers are used may be in numerical order, some systematic disarranged order, or randomly ordered. The same situation may apply in cases where letters are used. However, since the amount of letters available is greater than the amount of numbers possible, variations are increased. Insofar as analysis is concerned, the significance of two points, their identity and the method of their order, lies in the possibility of their use as a means of entry into the system. Usually, in all forms of matrix codes, the coordinates are changed regularly to provide a degree of security to offset the limitation imposed by the usual small size of the matrix, where interior values are generally fixed. Thus, once the initial recovery of a matrix is accomplished in part or in whole, analysis thereafter is concerned with the recovery of the row and column coordinates. If a systematic method of generation and assignment is involved, it is possible that the analyst may be able to predict their use in advance. If this does occur, then cryptanalysis is replaced by cryptography. The patterned use of row and column indicators is also of significance in the initial analysis of a matrix system as it often permits the placement of possible values within the matrix and the prior location of all coordinates during the initial stage of analysis.

d. Also of importance to the cryptanalyst is the use of special code groups within a matrix to indicate: begin spell, end spell, read number, read letter, upper case, and lower case. Note that the variant values provided by matrix systems for special meanings are usually somewhat limited. Therefore their use introduces a limitation into the resultant code which provides a sure entry into the system. The initial break into most matrix code systems and book codes, where syllabary spelling is a part, is through the recovery of syllabary spelling or numbers. The principle of analysis is quite simple where spelling is the basis of attack. The analyst searches the intercepted traffic for one or more groups which are repeated quite frequently, assuming that these groups represent the special indicators. If these are found, the code groups lying between are extracted and studied as either possible spelled words or sequences of numbers. These in turn are searched for recognizable patterns and compared to a list of suspect words or numbers which, through the analysis of collateral information, have been determined to be words likely to appear in the underlying plaintext. From this comparison, possible plaintext values are assigned to the code groups, the values being used to assume additional words.

e. The complete solution of a given system normally involves the use of one or more of the techniques outlined above, and when several are used, analysis is usually approached on a simultaneous basis. That is, after the system is first identified and its messages are isolated, all techniques are employed to reconstruct the original encoding matrix and derive the plaintext equivalencies of the code text. The methodology involved herein is discussed in other paragraphs.

15–7. (~~C~~) Identification

a. Identification of matrix codes rests on their similarity to multiliteral systems. That is, the code groups will appear almost exactly like the cipher groups produced by long multiliteral tables. Factors which might serve to distinguish the two are: the repeated appearance of a few groups equating to the special indicators mentioned previously, and perhaps a slight variation between observed and expected digraphic frequency distribution. However, these means of initial identification are extremely tenuous. Normally, identification comes through either a process of elimination (that is, a solution is first attempted as a multiliteral, then when failing, the system is assumed to be a matrix code) or from preknowledge of the system in use by the correspondents.

b. Code groups, when they are three to five digits in length, are normally transmitted in their original length. Smaller groups of two or three digits may be combined in some instances for transmission. The study of these groups often permits the identification of the code system. For example, code groups produced by a matrix often show positional limitations in their structure, again similar to the limitations produced by multiliteral cipher systems. This may be seen in the groups below.

1344 7344 6322 7300 2311 3388 7344 1366
5355 8322 6300 4333 2388 4377 0366 3366
3300 6399 1333 2388 6322 7333 9311 7344
1366 2388

A glance suffices to show that only a few combinations of dinomes are involved in each group. The limitations in the case are:

Row coordinates	*03, 13, 23, 33, 43, 53, 63, 73, 83, 93*
Column coordinates	*00, 01, 22, 33, 44, 55, 66, 77, 88, 99*

With such obvious values as coordinates, the analyst could assume with certainty that the system is based upon a 10 x 10 matrix. Moreover, the progression of the numbers themselves is possibly indicative of the order of their assignment to the rows and columns.

c. As a general rule, positional limitations will always be present in matrix codes, although not as apparent. Exceptions to this rule occur when the number of rows or columns match the number of different values used. For example, in the case of a 10 x 10 matrix where single numbers are used, all possible combinations are exhausted, thus no limitation will exist. This may be observed in figure 15-7.

	1	2	3	4	5	6	7	8	9	0
1										
2										
3										
4										
5										
6										
7										
8										
9										
0										

Code groups possible 00 through 99

Figure 15-7 (U). 10 x 10 matrix, single digit coordinates (U).

If on the other hand the number of possible combinations exceeds the total number of cells, a definite limitation exists. This may be observed in figure 15-8.

	09	19	29	39	49	59	69	79	89	99
10										
20										
30										
40										
50										
60										
70										
80										
90										
00										

Possible code groups 0009 - 9099

Groups used 100

Figure 15-8 (U). 10 x 10 matrix, dinome coordinates (U).

15-8. (~~C~~) Matrix Reconstruction

a. Matrix reconstruction in the case of initial analysis involves the study of characteristics, if any, of both coordinate generation and assignment, and the sequence of the plaintext values inserted in the cells of the matrix. If some systematic method is involved and is recognizable early in the analytic attack, the whole process of cryptanalysis can be greatly simplified.

b. In the case of coordinates, the analyst first determines if a limitation exists in the code groups. If this occurs, he uses these limitations to determine the total size of the matrix and the dimensions in terms of numbers of rows and columns. Using this information, he constructs a skeleton matrix. If some pattern exists in the digits used as coordinate indicators, he may attempt to place them correctly prior to the analysis of the internal plaintext values. The correct sequence of randomly generated coordinates cannot, of course, be determined without the prior recovery of the internal values. Where generation is involved, prior or concurrent placement is always possible. In those cases where the coordinates are rapidly superseded and where all or part of the internal values are known, this becomes doubly important. Some examples of systematic generation are:

Numerical order
20 21 22 23 24 25 26 27 28 29
Constant additive (+9)
86 95 04 13 22 31 40 49 58 67
Progressive additives (+1, 2, 3, 4, 5, 6, 7, 8, 9)
10 11 13 16 20 25 31 38 46 55

c. When analysis has progressed to the point where plaintext values are assumed for specific code groups, the order in which they are inscribed in the matrix should be carefully checked. Often, but not always, inscription of plaintext values follows a specific route. If this route can be identified, assumption of plaintext values is greatly simplified as identification of each given group can be limited to a restricted number of choices. This limitation is expecially important where a pattern in the order of row and column coordinates has been predetermined. In this case the placement of plaintext values is not subject to distortion by errors of location.

Section III. (¢) ANALYSIS OF MATRIX CODES

15–9. (¢) Analysis of Code Charts

a. The analysis of procedure tables or operator code charts is usually a rather simple task. This is due in part to the internal limitations of the code chart and also to the circumstances in which the code chart would be used. For example, the code charts, as shown in the preceding example, are generally limited on content, subject matter, and occasion of use, and usually refer to the operations of a communications system only. Given the knowledge of the circumstances surrounding the transmission of a particular message, the analyst can usually infer its contents. Hence, it is but a short step to the recovery of the plaintext value.

b. An additional factor that usually aids in solving these systems is that charts of this type are infrequently changed. Thus the analyst over a period of time is able to recover all interior plain values. Once this has been accomplished, further analysis of the system becomes a case of key recovery.

c. The periods of key usage will vary from case to case usually depending upon the usage of the chart. In some cases, they can be changed daily; in others, weeks may elapse before they are changed. In either case, key recovery is based on applying a procedure in reverse to that used heretofore, i.e. the analyst will find himself determining the correct cipher elements for one or more known values. For example, if the analyst knew that the digraphs *01 92 22 10 54* related to a message "QSY 5965," he would have little difficulty in placing the row and column indicators in their respective correct positions. Further recovery and development of the chart is merely a matter of time.

15–10. (¢) Analysis of Syllabary Squares

a. Essentially, the only difference between the method and technique of solving for plaintext of codes produced by a syllabary code and the previously covered multiliteral system lies in the volume of material required. For a given code sequence of assumed plaintext value, a larger number of plaintext elements may have to be considered. The code text for the word RECONNAISSANCE shown in paragraph 15–2 illustrates this point. Four possible forms of encoding were given. Assume then that the analyst knows that the sequence *81 35 29 60 60 11 59 88 11 60 25 35* equates to that word. Even with this knowledge, he still has to determine the correct way in which the word is divided, i.e. does *81c*=Rp or does it equal REp. In cases such as these, the analyst must modify his interpretation of frequency characteristics and idiomorphic patterns.

b. As a general rule, solution of this system is quite difficult in those cases where a volume of messages produced by a given system is lacking or where the cryptographer has made full use of the variants available within the system. Fortunately, cryptographers often develop patterns of usage which are beneficial to the cryptanalyst. On occasion some will tend to reuse certain code values consistently, thus producing an easily identifiable word pattern. Moreover, this consistent use of one code value for one letter or polygraph establishes that one-to-one relationship which quickly leads to the determination of a plaintext value.

c. Another method in which it is possible to establish plaintext values for a number of variants is the analysis of a number of messages which have repeated elements, words, or stereotyped phrases. The significance of this can be observed in the codings given for RECONNAISSANCE above. The similarity in the structure of the cipher sequences, representing different possibilities of encoding, would lead the analyst to valid assumptions concerning the structure of the underlying word. For example, consider the code group repeated in figure 15–9.

```
(1)  81  35  25  74  60  60  11  54  88  88  14  28
(2)  83  29  60  60  11  59  88  14  28
(3)  81  35  29  60  60  11  59  88  11  60  25  35
(4)  83  25  76  60  11  59  88  14  25  35
```

Figure 15–9 (Ȼ). Idiomorphism in code sequences (U).

(1) Examination of the first three code sequences reveals the repeated dinome *60* preceded by four, three, and two dinomes respectively. Since *60* is repeated, it is probably a single letter rather than a digraph or trigraph. If in the first code sequence the groups *81 35 25 74* represent 4 letters preceding the repeated letters indicated by *60,* then the groups *83 29* of the second sequence must represent the same letters as digraphs. Further, since the first and third sequences start with the same two dinomes, *81* and *35,* but differ in that the groups *25 74* of the first is replaced by *29* in the third, then *83* of the fourth equals a combination of the values for *81* and *35,* and *29* for *25* and *74.* This can be shown as:

```
81  35  25  74  60  60
  83      29    60  60
```

Following the same logic, the following equivalencies are discovered:

$$81+35=83$$
$$25+74=29$$
$$74+60=76$$
$$54+88=59$$
$$11+60=14$$
$$25+35=28$$

(2) With equivalencies established, it becomes possible to break the code sequence into uniliteral terms, thus forming the basis for drawing up word patterns. For example, the code sequences above could be reduced to the following code digraphs and one-word patterns established as shown:

A	B	C	D	D	E	F	G	G	E	D	B	A
81	*35*	*25*	*74*	*60*	*60*	*11*	*54*	*88*	*88*	*11*	*60*	*25*	*35*
R	E	C	O	N	N	A	I	S	S	A	N	C	E

d. Another method of entry into a syllabary square which does not require the depth of text that the above implies is the study and classification of repetition characters. This classification is based upon a general knowledge of the behavior of general classes of plaintext elements. For example, code units representing digits may appear in clusters representing time, map coordinates, etc. Further, particular digits in certain usages have positional limitations. The first digit of the 24-hour time system, for example, is limited to 0, 1, or 2; the second digit will use all numbers 1 through 0, the third from 0 to 5, and the last 1 through 0. Further, the 0, one of the three numbers appearing in the first position, may also appear double in the last two positions with any noteworthy frequency.

e. In either case, once sufficient equivalencies can be established, it becomes possible to reduce the greater part of the text to uniliteral terms and solve accordingly. The way is also opened for the recovery of the matrix. If the analyst has either a wholly—or a partially-recovered matrix available, the solution is thereby greatly simplified, as values can be assumed with a great degree of certainty.

f. An important point in respect to reducing a matrix code to uniliteral terms is that this is possible only under the circumstances where the encoding process proceeds along a nearly one-for-one basis. That is, a given code group equates to a given letter more often than it equates to a polygraph. Such a situation most often occurs in syllabary squares or in matrices which made them susceptible to this particular method of attack.

15–11. (Ȼ) Analysis of Matrix Codes

a. The analysis of matrix codes follows the same general approach as that used for syllabary squares. That is, the code groups are studied to determine their inherent positional limitations. From their limitations the dimensions of the matrix are assumed and, using the row and column values, a reconstruction matrix is set up. Where possible, the initial entry into the system is made through sequences of syllabary spelling. Then, equivalencies for the code groups are established and the plaintext values are inserted into the body of the matrix. Once segments of spelling can be identified and the plaintext determined, it then becomes possible to attack the remaining code groups on the basis of possible plaintext values which can be associated with the spelled sequences.

b. Note that this proposition depends entirely on the use of syllabary spelling in the code under analysis and the ability of the analyst to identify these sequences. Normally, identification is predicated on the basis of isolating repeated sequences in the code text of a number of messages. For this purpose an index listing prepared by data processing facilities may be used. An index listing is nothing more than a systematic listing of the groups that appear in a series of messages believed to have been produced by the same code system. There is no fixed type of index, its specific form being determined by the structure of the code system under analysis and the requirements of the analyst. Two common types are: an index of repeated groups, and an index of repeated sequences.

(1) An index of repeated groups is made up of a listing of all repeated groups appearing in a number of messages. Additionally, the repeated groups are keyed to a specific message and location within that message. This type of listing is convenient to use where great numbers of codes are processed and where a complete listing of all the groups would be too bulky. It is also useful for the initial identification of the special indicators discussed previously.

(2) The second general type is an index of repeated sequences. This can be based on the previous type index where specific groups have been isolated as spelling indicators or, if such are not used in a particular code system, simply a list of repeated sequences. This particular index form is especially suitable for the location and subsequent analysis of syllabary spelling sequences that occur in the body of a code as differentiated from stereotyped beginnings or endings.

c. In the case where no indication is given that a sequence represents a spelled word or phrase, the possibility always exists that it might represent a sequence of words rather than letters. In such cases, differentiation can sometimes be made on the frequency and position of the repeated groups. For example, if a repeated sequence of code groups appeared consistently at the beginning or ending of a message, one could assume that it represented a stereotype address and, in this case, might represent words. On the other hand, if a given sequence appeared in different positions in several messages, one might assume that it represented a commonly used spelled word. In either case, note that identification of this sort is merely an assumption which has to be either proved or disproved in subsequent analysis.

d. Assuming that a number of given sequences have been isolated as spell-sequences, the problem then is to determine what words are actually being spelled. The general approach is to attempt to fit the sequence to a stereotype common to the communications under study. These stereotypes may be military terms, titles, ranks, geographic place names, etc. In actual practice, the analyst's familiarity with the communications system, the correspondents, and the area of operations is an invaluable aid. The actual recovery of plaintext equivalencies for code groups can make use of idiomophic patterns of the words. Note that these patterns may represent single letters as well as polygraphs, though usually digraphs are not common.

APPENDIX A (~~C~~)
FREQUENCY DISTRIBUTIONS OF ENGLISH DIGRAPHS

Frequency distributions of English digraphs appearing in 50,000 letters of governmental plaintext telegrams, reduced to 5,000 digraphs.

Table A-1 (~~C~~). Frequency distribution digraphs (U).

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	TOTAL	BLANKS
A	3	6	14	27	1	4	6	2	17	1	2	32	14	64	2	12		44	41	47	13	7	3		12		374	3
B	4				18				2	1		6	1		4			2	1	1	2				7		49	14
C	20		3	1	32	1		14	7		4	5	1	1	41			4	1	14	4		1		1		155	8
D	32	4	4	8	33	8	2	2	27	1		3	5	4	16	5	2	12	13	15	5	3	4		1		209	3
E	35	4	32	60	42	18	4	7	27	1		29	14	111	12	20	12	87	54	37	3	20	7	7	4	1	648	1
F	5		2	1	10	11	1		39			2	1		40	1		9	3	11	3		1		1		141	9
G	7		2	1	14	2	1	20	5	1		2	1	3	6	2		5	3	4	2		1				82	7
H	20	1	3	2	20	5			33			1	2	3	20	1	1	17	4	28	8		1		1		171	7
I	8	2	22	6	13	10	19				2	23	9	75	41	7		27	35	27		25		15		2	368	7
J	1				2										2						2						7	22
K	1		1		6				2			1		1					1								13	19
L	8	3	3	9	37	3	1	1	20			27		1	13	3		2	6	8	2	2	2		10		183	5
M	36	6	3	1	26	1		1	9				13		10	8		2	4	2	2				2		126	10
N	26	3	19	52	57	9	27	4	30	1	2	5	5	8	18	3	1	4	24	82	7	3	3		5		397	2
O	7	4	8	12	3	25	2	3	5	1	2	19	25	77	6	25		64	14	19	37	7	8	1	2		376	2
P	14	1	1	1	23	2		3	6			13	4	1	17	11		18	6	8	3	1	1		1		135	6
Q													1					1			15						17	23
R	39	2	9	17	98	6	7	3	30	1	1	5	9	7	28	13		11	31	42	5	5	4		9		382	3
S	24	3	13	5	49	12	2	26	34		1	2	3	4	15	10		5	19	63	11	1	4		1		307	4
T	28	3	6	6	71	7	1	78	45			5	6	7	50	2	1	17	19	19	5		36		41	1	454	4
U	5	3	3	3	11	1	8		5			6	5	21	1			31	12	12		1					130	9
V	6				57				12						1					1							77	21
W	12				22			4	13			1		2	19			1	1						1		76	16
X	2		2	1	1	1		1	2					1	1	2		1	1	7							23	13
Y	6	2	4	4	9	11	1	1	3			2	2	6	10	3		4	11	15	1		1				96	7
Z	1				2				1																		4	23
TOTAL	370	46	154	217	657	137	82	170	374	8	14	189	123	397	373	130	17	368	304	462	130	75	77	23	99	4	5000	
BLANKS	1	11	6	7	1	7	12	10	3	18	19	6	6	7	3	8	21	4	4	5	7	15	11	3	10	23		248

Table A–2 ~~(C)~~. The 428 digraphs of Table A–1, arranged according to their absolute frequencies, accompanied by the logarithms of their assigned probabilities (U).

	F	L_{10} (F)	L_{224} (2F)
EN	111	2.05	.99
RE	98	1.99	.96
ER	87	1.94	.94
NT	82	1.91	.93
TH	78	1.89	.92
ON	77	1.89	.92
IN	75	1.88	.92
TE	71	1.85	.91
AN	64	1.81	.89
OR	64	1.81	.89
ST	63	1.80	.88
ED	60	1.78	.88
NE	57	1.76	.87
VE	57	1.76	.87
ES	54	1.73	.86
ND	52	1.72	.85
TO	50	1.70	.84
SE	49	1.69	.84
	[1]1,249		
AT	47	1.67	.83
TI	45	1.65	.82
AR	44	1.64	.82
EE	42	1.62	.81
RT	42	1.62	.81
AS	41	1.61	.80
CO	41	1.61	.80
IO	41	1.61	.80
TY	41	1.61	.80
FO	40	1.60	.80
FI	39	1.59	.80
RA	39	1.59	.80
ET	37	1.57	.79
LE	37	1.57	.79
OU	37	1.57	.79
MA	36	1.56	.78
TW	36	1.56	.78
EA	35	1.54	.78
IS	35	1.54	.78
SI	34	1.53	.77
DE	33	1.52	.77
HI	33	1.52	.77
AL	32	1.51	.76
CE	32	1.51	.76
DA	32	1.51	.76
EC	32	1.51	.76
RS	31	1.49	.75
UR	31	1.49	.75
NI	30	1.48	.75
RI	30	1.48	75
EL	29	1.46	.74
HT	28	1.45	.74
LA	28	1.45	.74
RO	28	1.45	.74
TA	28	1.45	.74
	[2]2,495		
AD	27	1.43	.73
DI	27	1.43	.73
EI	27	1.43	.73
IR	27	1.43	.73
IT	27	1.43	.73
LL	27	1.43	.73
NG	27	1.43	.73
ME	26	1.41	.72
NA	26	1.41	.72
SH	26	1.41	.72
IV	25	1.40	.72
OF	25	1.40	.72
OM	25	1.40	.72
OP	25	1.40	.72
NS	24	1.38	.71
SA	24	1.38	.71
IL	23	1.36	.70
PE	23	1.36	.70
IC	22	1.34	.69
WE	22	1.34	.69
UN	21	1.32	.68
CA	20	1.30	.67
EP	20	1.30	.67
EV	20	1.30	.67
GH	20	1.30	.67
HA	20	1.30	.67
HE	20	1.30	.67
HO	20	1.30	.67
LI	20	1.30	.67
IG	19	1.28	.67
NC	19	1.28	.67
OL	19	1.28	.67
OT	19	1.28	.67
SS	19	1.28	.67
TS	19	1.28	.67
TT	19	1.28	.67
WO	19	1.28	67
BE	18	1.26	.66
EF	18	1.26	.66
NO	18	1.26	.66
PR	18	1.26	.66
AI	17	1.23	.64
HR	17	1.23	.64
PO	17	1.23	.64
RD	17	1.23	.64
TR	17	1.23	.64
DO	16	1.20	.63
DT	15	1.18	.62
IX	15	1.18	.62
QO	15	1.18	.62
SO	15	1.18	.62
YT	15	1.18	.62
AC	14	1.15	.61
AM	14	1.15	.61
CH	14	1.15	.61
CT	14	1.15	.61
EM	14	1.15	.61
GE	14	1.15	.61
OS	14	1.15	.61
PA	14	1.15	.61
AU	13	1.11	.59
DS	13	1.11	.59
IE	13	1.11	.59
LO	13	1.11	.59
MM	13	1.11	.59
PL	13	1.11	.59
RP	13	1.11	.59
SC	13	1.11	.59
WI	13	1.11	.59
	[3]3,745		
AP	12	1.08	.58
AY	12	1.08	.58
DR	12	1.08	.58
EO	12	1.08	.58
EQ	12	1.08	.58
OD	12	1.08	.58
SF	12	1.08	.58
US	12	1.08	.58
UT	12	1.08	.58
VI	12	1.08	.58
WA	12	1.08	.58
FF	11	1.04	.56
FT	11	1.04	.56
PP	11	1.04	.56
RR	11	1.04	.56
SU	11	1.04	.56
UE	11	1.04	.56
YF	11	1.04	.56
YS	11	1.04	.56
FE	10	1.00	.55
IF	10	1.00	.55
LY	10	1.00	.55
MO	10	1.00	.55
SP	10	1.00	.55
YO	10	1.00	.55
FR	9	0.95	.53
IM	9	0.95	.53
LD	9	0.95	.53
MI	9	0.95	.53
NF	9	0.95	.53
RC	9	0.95	.53
RM	9	0.95	.53
RY	9	0.95	.53
YE	9	0.95	.53
DD	8	0.90	.51
DF	8	0.90	.51
HU	8	0.90	.51
IA	8	0.90	.51
LT	8	0.90	.51
MP	8	0.90	.51
NN	8	0.90	.51
OC	8	0.90	.51
OW	8	0.90	.51
PT	8	0.90	.51
UG	8	0.90	.51
AV	7	0.85	.48
BY	7	0.85	.48
CI	7	0.85	.48

[1] The 18 digraphs above this line compose 25% of the total.
[2] The 53 digraphs above this line compose 50% of the total.
[3] The 122 digraphs above this line compose 75% of the total.

Table A–2 (~~C~~). The 428 digraphs of Table A–1, arranged according to their absolute frequencies, accompanied by the logarithms of their assigned probabilities (U) – Continued

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
EH	7	0.85	.48	RU ...	5	0.70	.42	GS	3	0.48	.33	JE	2	0.30	.25
EW ...	7	0.85	.48	RV ...	5	0.70	.42	HC	3	0.48	.33	JO	2	0.30	.25
EX	7	0.85	.48	SD	5	0.70	.42	HN ...	3	0.48	.33	JU	2	0.30	.25
GA ...	7	0.85	.48	SR	5	0.70	.42	LB	3	0.48	.33	KI	2	0.30	.25
IP	7	0.85	.48	TL	5	0.70	.42	LC	3	0.48	.33	LM ...	2	0.30	.25
NU ...	7	0.85	.48	TU	5	0.70	.42	LF	3	0.48	.33	LR	2	0.30	.25
OA ...	7	0.85	.48	UA ...	5	0.70	.42	LP	3	0.48	.33	LU	2	0.30	.25
OV ...	7	0.85	.48	UI	5	0.70	.42	MC ...	3	0.48	.33	LV	2	0.30	.25
RG ...	7	0.85	.48	UM ...	5	0.70	.42	NP	3	0.48	.33	LW ...	2	0.30	.25
RN ...	7	0.85	.48	AF	4	0.60	.38	NV ...	3	0.48	.33	MR ...	2	0.30	.25
TF	7	0.85	.48	BA	4	0.60	.38	NW ...	3	0.48	.33	MT ...	2	0.30	.25
TN	7	0.85	.48	BO	4	0.60	.38	OE	3	0.48	.33	MU ...	2	0.30	.25
XT	7	0.85	.48	CK	4	0.60	.38	OH ...	3	0.48	.33	MY ...	2	0.30	.25
AB	6	0.78	.45	CR	4	0.60	.38	PH	3	0.48	.33	NB	2	0.30	.25
AG	6	0.78	.45	CU	4	0.60	.38	PU	3	0.48	.33	NK ...	2	0.30	.25
BL	6	0.78	.45	DB	4	0.60	.38	RH ...	3	0.48	.33	OG ...	2	0.30	.25
GO	6	0.78	.45	DC	4	0.60	.38	SB	3	0.48	.33	OK ...	2	0.30	.25
ID	6	0.78	.45	DN	4	0.60	.38	SM	3	0.48	.33	OY ...	2	0.30	.25
KE	6	0.78	.45	DW ...	4	0.60	.38	TB	3	0.48	.33	PF	2	0.30	.25
LS	6	0.78	.45	EB	4	0.60	.38	UB	3	0.48	.33	RB	2	0.30	.25
MB ...	6	0.78	.45	EG	4	0.60	.38	UC	3	0.48	.33	SG	2	0.30	.25
OO ...	6	0.78	.45	EY	4	0.60	.38	UD ...	3	0.48	.33	SL	2	0.30	.25
PI	6	0.78	.45	GT	4	0.60	.38	YI	3	0.48	.33	TP	2	0.30	.25
PS	6	0.78	.45	HS	4	0.60	.38	YP	3	0.48	.33	UP	2	0.30	.25
RF	6	0.78	.45	MS	4	0.60	.38	AH ...	2	0.30	.25	WN ...	2	0.30	.25
TC	6	0.78	.45	NH ...	4	0.60	.38	AK ...	2	0.30	.25	XA ...	2	0.30	.25
TD	6	0.78	.45	NR ...	4	0.60	.38	AO ...	2	0.30	.25	XC	2	0.30	.25
TM ...	6	0.78	.45	OB	4	0.60	.38	BI	2	0.30	.25	XI	2	0.30	.25
UL	6	0.78	.45	PM	4	0.60	.38	BR	2	0.30	.25	XP	2	0.30	.25
VA ...	6	0.78	.45	RW ...	4	0.60	.38	BU	2	0.30	.25	YB	2	0.30	.25
YA ...	6	0.78	.45	SN	4	0.60	.38	DG ...	2	0.30	.25	YL	2	0.30	.25
YN ...	6	0.78	.45	SW	4	0.60	.38	DH ...	2	0.30	.25	YM ...	2	0.30	.25
CL	5	0.70	.42	WH ...	4	0.60	.38	DQ ...	2	0.30	.25	ZE	2	0.30	.25
DM ...	5	0.70	.42	YC	4	0.60	.38	FC	2	0.30	.25	AE	1	0.00	.13
DP	5	0.70	.42	YD ...	4	0.60	.38	FL	2	0.30	.25	AJ	1	0.00	.13
DU ...	5	0.70	.42	YR ...	4	0.60	.38	GC	2	0.30	.25	BJ	1	0.00	.13
FA	5	0.70	.42	AA ...	3	0.48	.33	GF	2	0.30	.25	BM ...	1	0.00	.13
GI	5	0.70	.42	AW ...	3	0.48	.33	GL	2	0.30	.25	BS	1	0.00	.13
GR ...	5	0.70	.42	CC	3	0.48	.33	GP	2	0.30	.25	BT	1	0.00	.13
HF	5	0.70	.42	DL	3	0.48	.33	GU ...	2	0.30	.25	CD	1	0.00	.13
NL	5	0.70	.42	DV ...	3	0.48	.33	HD ...	2	0.30	.25	CF	1	0.00	.13
NM ...	5	0.70	.42	EU	3	0.48	.33	HM ...	2	0.30	.25	CM ...	1	0.00	.13
NY ...	5	0.70	.42	FS	3	0.48	.33	IB	2	0.30	.25	CN	1	0.00	.13
OI	5	0.70	.42	FU	3	0.48	.33	IK	2	0.30	.25	CS	1	0.00	.13
RL	5	0.70	.42	GN ...	3	0.48	.33	IZ	2	0.30	.25	CW ...	1	0.00	.13

Table A–2 (~~C~~). The 428 digraphs of Table A–1, arranged according to their absolute frequencies, accompanied by the logarithms of their assigned probabilities (U) – Continued

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
CY	1	0.00	.13	HW	1	0.00	.13	PD	1	0.00	.13	WL	1	0.00	.13
DJ	1	0.00	.13	HY	1	0.00	.13	PN	1	0.00	.13	WR	1	0.00	.13
DY	1	0.00	.13	JA	1	0.00	.13	PV	1	0.00	.13	WS	1	0.00	.13
EJ	1	0.00	.13	KA	1	0.00	.13	PW	1	0.00	.13	WY	1	0.00	.13
EZ	1	0.00	.13	KC	1	0.00	.13	PY	1	0.00	.13	XD	1	0.00	.13
FD	1	0.00	.13	KL	1	0.00	.13	QM	1	0.00	.13	XE	1	0.00	.13
FG	1	0.00	.13	KN	1	0.00	.13	QR	1	0.00	.13	XF	1	0.00	.13
FM	1	0.00	.13	KS	1	0.00	.13	RJ	1	0.00	.13	XH	1	0.00	.13
FP	1	0.00	.13	LG	1	0.00	.13	RK	1	0.00	.13	XN	1	0.00	.13
FW	1	0.00	.13	LH	1	0.00	.13	SK	1	0.00	.13	XO	1	0.00	.13
FY	1	0.00	.13	LN	1	0.00	.13	SV	1	0.00	.13	XR	1	0.00	.13
GD	1	0.00	.13	MD	1	0.00	.13	SY	1	0.00	.13	XS	1	0.00	.13
GG	1	0.00	.13	MF	1	0.00	.13	TG	1	0.00	.13	YG	1	0.00	.13
GJ	1	0.00	.13	MH	1	0.00	.13	TQ	1	0.00	.13	YH	1	0.00	.13
GM	1	0.00	.13	NJ	1	0.00	.13	TZ	1	0.00	.13	YU	1	0.00	.13
GW	1	0.00	.13	NQ	1	0.00	.13	UF	1	0.00	.13	YW	1	0.00	.13
HB	1	0.00	.13	OJ	1	0.00	.13	UO	1	0.00	.13	ZA	1	0.00	.13
HL	1	0.00	.13	OX	1	0.00	.13	UV	1	0.00	.13	ZI	1	0.00	.13
HP	1	0.00	.13	PB	1	0.00	.13	VO	1	0.00	.13		5,000		
HQ	1	0.00	.13	PC	1	0.00	.13	VT	1	0.00	.13				

Table A–3 (~~C~~). The 18 digraphs composing 25% of the digraphs in Table A–1, accompanied by the logarithms of their assigned probabilities, arranged alphabetically according to their initial letters (U)

(1) AND ACCORDING TO THEIR FINAL LETTERS

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
AN	64	1.81	.89	ON	77	1.89	.92
				OR	64	1.81	.89
ED	60	1.78	.88	RE	98	1.99	.96
EN	111	2.05	.99				
ER	87	1.94	.94	SE	49	1.69	.84
ES	54	1.73	.86	ST	63	1.80	.88
				TE	71	1.85	.91
IN	75	1.88	.92	TH	78	1.89	.92
				TO	50	1.70	.84
ND	52	1.72	.85	VE	57	1.76	.87
NE	57	1.76	.87		1,249		
NT	82	1.91	.93				

(2) AND ACCORDING TO THEIR ABSOLUTE FREQUENCIES

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
AN	64	1.81	.89	ON	77	1.89	.92
				OR	64	1.81	.89
EN	111	2.05	.99	RE	98	1.99	.96
ER	87	1.94	.94				
ED	60	1.78	.88	ST	63	1.80	.88
ES	54	1.73	.86	SE	49	1.69	.84
				TH	78	1.89	.92
IN	75	1.88	.92	TE	71	1.85	.91
				TO	50	1.70	.84
NT	82	1.91	.93	VE	57	1.76	.87
NE	57	1.76	.87		1,249		
ND	52	1.72	.85				

Table A–4 (~~C~~). The 53 digraphs composing 50% of the digraphs of Table A–1, accompanied by the logarithms of their assigned probabilities, arranged alphabetically according to their initial letters (U)

(1) AND ACCORDING TO THEIR FINAL LETTERS

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
AL	32	1.51	.76	MA ...	36	1.56	.78
AN ...	64	1.81	.89				
AR ...	44	1.64	.82	ND ...	52	1.72	.85
AS	41	1.61	.80	NE	57	1.76	.87
AT	47	1.67	.83	NI	30	1.48	.75
				NT	82	1.91	.93
CE	32	1.51	.76				
CO	41	1.61	.80	ON ...	77	1.89	.92
				OR ...	64	1.81	.89
DA ...	32	1.51	.76	OU ...	37	1.57	.79
DE	33	1.52	.77				
				RA ...	39	1.59	.80
EA	35	1.54	.78	RE	98	1.99	.96
EC	32	1.51	.76	RI	30	1.48	.75
ED	60	1.78	.88	RO ...	28	1.45	.74
EE	42	1.62	.81	RS	31	1.49	.75
EL	29	1.46	.74	RT	42	1.62	.81
EN	111	2.05	.99				
ER	87	1.94	.94	SE	49	1.69	.84
ES	54	1.73	.86	SI	34	1.53	.77
ET	37	1.57	.79	ST	63	1.80	.88
FI	39	1.59	.80	TA	28	1.45	.74
FO	40	1.60	.80	TE	71	1.85	.91
				TH	78	1.89	.92
HI	33	1.52	.77	TI	45	1.65	.82
HT	28	1.45	.74	TO	50	1.70	.84
				TW ...	36	1.56	.78
IN	75	1.88	.92	TY	41	1.61	.80
IO	41	1.61	.80				
IS	35	1.54	.78	UR ...	31	1.49	.75
LA	28	1.45	.74	VE	57	1.76	.87
					2,495		
LE	37	1.57	.79				

(2) AND ACCORDING TO THEIR ABSOLUTE FREQUENCIES

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
AN ...	64	1.81	.89	MA ...	36	1.56	.78
AT	47	1.67	.83				
AR ...	44	1.64	.82	NT	82	1.91	.93
AS	41	1.61	.80	NE	57	1.76	.87
AL	32	1.51	.76	ND ...	52	1.72	.85
				NI	30	1.48	.75
CO	41	1.61	.80				
CE	32	1.51	.76	ON ...	77	1.89	.92
				OR ...	64	1.81	.89
DE	33	1.52	.77	OU ...	37	1.57	.79
DA ...	32	1.51	.76				
				RE	98	1.99	.96
EN	111	2.05	.99	RT	42	1.62	.81
ER	87	1.94	.94	RA ...	39	1.59	.80
ED	60	1.78	.88	RS	31	1.49	.75
ES	54	1.73	.86	RI	30	1.48	.75
EE	42	1.62	.81	RO ...	28	1.45	.74
ET	37	1.57	.79				
EA	35	1.54	.78	ST	63	1.80	.88
EC	32	1.51	.76	SE	49	1.69	.84
EL	29	1.46	.74	SI	34	1.53	.77
FO	40	1.60	.80	TH	78	1.89	.92
FI	39	1.59	.80	TE	71	1.85	.91
				TO	50	1.70	.84
HI	33	1.52	.77	TI	45	1.65	.82
HT	28	1.45	.74	TY	41	1.61	.80
				TW ...	36	1.56	.78
IN	75	1.88	.92	TA	28	1.45	.74
IO	41	1.61	.80				
IS	35	1.54	.78	UR ...	31	1.49	.75
LE	37	1.57	.79	VE	57	1.76	.87
					2,495		
LA	28	1.45	.74				

Table A–5 ~~(C)~~. The 122 digraphs composing 75% of the digraphs of Table A–1, accompanied by the logarithms of their assigned probabilities, arranged alphabetically according to their initial letters (U)

(1) AND ACCORDING TO THEIR FINAL LETTERS

	F	L_{10}	L_{224}		F	L_{10}	L_{224}		F	L_{10}	L_{224}		F	L_{10}	L_{224}
		(F)	(2F)			(F)	(2F)			(F)	(2F)			(F)	(2F)
AC	14	1.15	.61	ER	87	1.94	.94	MA ...	36	1.56	.78	RS	31	1.49	.75
AD ...	27	1.43	.73	ES	54	1.73	.86	ME ...	26	1.41	.72	RT	42	1.62	.81
AI	17	1.23	.64	ET	37	1.57	.79								
AL	32	1.51	.76	EV	20	1.30	.67	NA ...	26	1.41	.72	SA	24	1.38	.71
AM ...	14	1.15	.61					NC	19	1.28	.67	SE	49	1.69	.84
AN ...	64	1.81	.89	FI	39	1.59	.80	ND ...	52	1.72	.85	SH	26	1.41	.72
AR ...	44	1.64	.82	FO	40	1.60	.80	NE	57	1.76	.87	SI	34	1.53	.77
AS	41	1.61	.80					NG	27	1.43	.73	SO	15	1.18	.62
AT	47	1.67	.83	GE	14	1.15	.61	NI	30	1.48	.75	SS	19	1.28	.67
AU ...	13	1.11	.59	GH ...	20	1.30	.67	NO ...	18	1.26	.66	ST	63	1.80	.88
								NS	24	1.38	.71				
BE	18	1.26	.66	HA ...	20	1.30	.67	NT ...	82	1.91	.93	TA	28	1.45	.74
				HE	20	1.30	.67					TE	71	1.85	.91
CA	20	1.30	.67	HI	33	1.52	.77	OF	25	1.40	.72	TH	78	1.89	.92
CE	32	1.51	.76	HO ...	20	1.30	.67	OL	19	1.28	.67	TI	45	1.65	.82
CH	14	1.15	.61	HR ...	17	1.23	.64	OM ...	25	1.40	.72	TO	50	1.70	.84
CO	41	1.61	.80	HT	28	1.45	.74	ON ...	77	1.89	.92	TR	17	1.23	.64
CT	14	1.15	.61					OP	25	1.40	.72	TS	19	1.28	.67
DA ...	32	1.51	.76	IC	22	1.34	.69	OR ...	64	1.81	.89	TT	19	1.28	.67
DE	33	1.52	.77	IE	13	1.11	.59	OS	14	1.15	.61	TW ...	36	1.56	.78
DI	27	1.43	.73	IG	19	1.28	.67	OT	19	1.28	.67	TY	41	1.61	.80
DO ...	16	1.20	.63	IL	23	1.36	.70	OU ...	37	1.57	.79				
DS	13	1.11	.59	IN	75	1.88	.92					UN ...	21	1.32	.68
DT	15	1.18	.62	IO	41	1.61	.80	PA	14	1.15	.61	UR ...	31	1.49	.75
				IR	27	1.43	.73	PE	23	1.36	.70				
EA	35	1.54	.78	IS	35	1.54	.78	PO	17	1.23	.64	VE	57	1.76	.87
EC	32	1.51	.76	IT	27	1.43	.73	PR	18	1.26	.66				
ED	60	1.78	.88	IV	25	1.40	.72					WE ...	22	1.34	.69
EE	42	1.62	.81	IX	15	1.18	.62	QU ...	15	1.18	.62	WO ...	19	1.28	.67
EF	18	1.26	.66												
EI	27	1.43	.73	LA	28	1.45	.74	RA ...	39	1.59	.80	YT	15	1.18	.62
EL	29	1.46	.74	LE	37	1.57	.79	RD ...	17	1.23	.64		3,745		
EM ...	14	1.15	.61	LI	20	1.30	.67	RE	98	1.99	.96				
EN	111	2.05	.99	LL	27	1.43	.73	RI	30	1.48	.75				
EP	20	1.30	.67	LO	13	1.11	.59	RO ...	28	1.45	.74				

Table A–5 (U). The 122 digraphs composing 75% of the digraphs of Table A–1, accompanied by the logarithms of their assigned probabilities, arranged alphabetically according to their initial letters (U) – Continued

(2) AND ACCORDING TO THEIR ABSOLUTE FREQUENCIES

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
AN	64	1.81	.89	EI	27	1.43	.73	MA	36	1.56	.78	RI	30	1.48	.75
AT	47	1.67	.83	EP	20	1.30	.67	ME	26	1.41	.72	RO	28	1.45	.74
AR	44	1.64	.82	EV	20	1.30	.67					RD	17	1.23	.64
AS	41	1.61	.80	EF	18	1.26	.66	NT	82	1.91	.93				
AL	32	1.51	.76	EM	14	1.15	.61	NE	57	1.76	.87				
AD	27	1.43	.73					ND	52	1.72	.85	ST	63	1.80	.88
AI	17	1.23	.64	FO	40	1.60	.80	NI	30	1.48	.75	SE	49	1.69	.84
AC	14	1.15	.61	FI	39	1.59	.80	NG	27	1.43	.73	SI	34	1.53	.77
AM	14	1.15	.61					NA	26	1.41	.72	SH	26	1.41	.72
AU	13	1.11	.59	GH	20	1.30	.67	NS	24	1.38	.71	SA	24	1.38	.71
				GE	14	1.15	.61	NC	19	1.28	.67	SS	19	1.28	.67
BE	18	1.26	.66					NO	18	1.26	.66	SO	15	1.18	.62
				HI	33	1.52	.77								
CO	41	1.61	.80	HT	28	1.45	.74					TH	78	1.89	.92
CE	32	1.51	.76	HA	20	1.30	.67	ON	77	1.89	.92	TE	71	1.85	.91
CA	20	1.30	.67	HE	20	1.30	.67	OR	64	1.81	.89	TO	50	1.70	.84
CH	14	1.15	.61	HO	20	1.30	.67	OU	37	1.57	.79	TI	45	1.65	.82
CT	14	1.15	.61	HR	17	1.23	.64	OF	25	1.40	.72	TY	41	1.61	.80
								OM	25	1.40	.72	TW	36	1.56	.78
				IN	75	1.88	.92	OP	25	1.40	.72	TA	28	1.45	.74
DE	33	1.52	.77	IO	41	1.61	.80	OL	19	1.28	.67	TS	19	1.28	.67
DA	32	1.51	.76	IS	35	1.54	.78	OT	19	1.28	.67	TT	19	1.28	.67
DI	27	1.43	.73	IR	27	1.43	.73	OS	14	1.15	.61	TR	17	1.23	.64
DO	16	1.20	.63	IT	27	1.43	.73								
DT	15	1.18	.62	IV	25	1.40	.72	PE	23	1.36	.70				
DS	13	1.11	.59	IL	23	1.36	.70	PR	18	1.26	.66	UR	31	1.49	.75
				IC	22	1.34	.69	PO	17	1.23	.64	UN	21	1.32	.68
EN	111	2.05	.99	IG	19	1.28	.67	PA	14	1.15	.61				
ER	87	1.94	.94	IX	15	1.18	.62					VE	57	1.76	.87
ED	60	1.78	.88	IE	13	1.11	.59								
ES	54	1.73	.86					QU	15	1.18	.62	WE	22	1.34	.69
EE	42	1.62	.81	LE	37	1.57	.79					WO	19	1.28	.67
ET	37	1.57	.79	LA	28	1.45	.74	RE	98	1.99	.96				
EA	35	1.54	.78	LL	27	1.43	.73	RT	42	1.62	.81	YT	15	1.18	.62
EC	32	1.51	.76	LI	20	1.30	.67	RA	39	1.59	.80		3,745		
EL	29	1.46	.74	LO	13	1.11	.59	RS	31	1.49	.75				

Table A–6 (C). The 428 digraphs of Table A–1, arranged in alphabetic order by initial letters, then by absolute frequencies accompanied by the logarithms of their assigned probabilities (U)

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
AN ...	64	1.81	.89	CT	14	1.15	.61	ED	60	1.78	.88	GH ...	20	1.30	.67
AT	47	1.67	.83	CI	7	0.85	.48	ES	54	1.73	.86	GE	14	1.15	.61
AR ...	44	1.64	.82	CL	5	0.70	.42	EE	42	1.62	.81	GA ...	7	0.85	.48
AS	41	1.61	.80	CK	4	0.60	.38	ET	37	1.57	.79	GO ...	6	0.78	.45
AL	32	1.51	.76	CR	4	0.60	.38	EA	35	1.54	.78	GI	5	0.70	.42
AD ...	27	1.43	.73	CU	4	0.60	.38	EC	32	1.51	.76	GR ...	5	0.70	.42
AI	17	1.23	.64	CC	3	0.48	.33	EL	29	1.46	.74	GT	4	0.60	.38
AC	14	1.15	.61	CD	1	0.00	.13	EI	27	1.43	.73	GN ...	3	0.48	.33
AM ...	14	1.15	.61	CF	1	0.00	.13	EP	20	1.30	.67	GS	3	0.48	.33
AU ...	13	1.11	.59	CM ...	1	0.00	.13	EV	20	1.30	.67	GC	2	0.30	.25
AP	12	1.08	.58	CN	1	0.00	.13	EF	18	1.26	.66	GF	2	0.30	.25
AY ...	12	1.08	.58	CS	1	0.00	.13	EM ...	14	1.15	.61	GL	2	0.30	.25
AV ...	7	0.85	.48	CW ...	1	0.00	.13	EO	12	1.08	.58	GP	2	0.30	.25
AB	6	0.78	.45	CY	1	0.00	.13	EQ	12	1.08	.58	GU ...	2	0.30	.25
AG ...	6	0.78	.45					EH	7	0.85	.48	GD ...	1	0.00	.13
AF	4	0.60	.38	DE	33	1.52	.77	EW ...	7	0.85	.48	GG ...	1	0.00	.13
AA ...	3	0.48	.33	DA ...	32	1.51	.76	EX	7	0.85	.48	GJ	1	0.00	.13
AW ...	3	0.48	.33	DI ...	27	1.43	.73	EB	4	0.60	.38	GM ...	1	0.00	.13
AH ...	2	0.30	.25	DO ...	16	1.20	.63	EG	4	0.60	.38	GW ...	1	0.00	.13
AK ...	2	0.30	.25	DT	15	1.18	.62	EY	4	0.60	.38				
AO ...	2	0.30	.25	DS	13	1.11	.59	EU	3	0.48	.33				
AE	1	0.00	.13	DR ...	12	1.08	.58	EJ	1	0.00	.13				
AJ	1	0.00	.13	DD ...	8	0.90	.51	EZ	1	0.00	.13	HI	33	1.52	.77
				DF	8	0.90	.51					HT	28	1.45	.74
BE	18	1.26	.66	DM ...	5	0.70	.42	FO	40	1.60	.80	HA ...	20	1.30	.67
BY	7	0.85	.48	DP	5	0.70	.42	FI	39	1.59	.80	HE	20	1.30	.67
BL	6	0.78	.45	DU ...	5	0.70	.42	FF	11	1.04	.56	HO ...	20	1.30	.67
BA	4	0.60	.38	DB	4	0.60	.38	FT	11	1.04	.56	HR ...	17	1.23	.64
BO	4	0.60	.38	DC	4	0.60	.38	FE	10	1.00	.55	HU ...	8	0.90	.51
BI	2	0.30	.25	DN ...	4	0.60	.38	FR	9	0.95	.53	HF	5	0.70	.42
BR	2	0.30	.25	DW ...	4	0.60	.38	FA	5	0.70	.42	HS	4	0.60	.38
BU	2	0.30	.25	DL	3	0.48	.33	FS	3	0.48	.33	HC	3	0.48	.33
BJ	1	0.00	.13	DV ...	3	0.48	.33	FU	3	0.48	.33	HN ...	3	0.48	.33
BM ...	1	0.00	.13	DG ...	2	0.30	.25	FC	2	0.30	.25	HD ...	2	0.30	.25
BS	1	0.00	.13	DH ...	2	0.30	.25	FL	2	0.30	.25	HM ...	2	0.30	.25
BT	1	0.00	.13	DQ ...	2	0.30	.25	FD	1	0.00	.13	HB	1	0.00	.13
				DJ	1	0.00	.13	FG	1	0.00	.13	HL	1	0.00	.13
CO	41	1.61	80	DY ...	1	0.00	.13	FM ...	1	0.00	.13	HP	1	0.00	.13
CE	32	1.51	.76					FP	1	0.00	.13	HQ ...	1	0.00	.13
CA	20	1.30	.67	EN	111	2.05	.99	FW ...	1	0.00	.13	HW ...	1	0.00	.13
CH	14	1.15	.61	ER	87	1.94	.94	FY	1	0.00	.13	HY ...	1	0.00	.13

Table A–6 (U). The 428 digraphs of Table A–1, arranged in alphabetic order by initial letters, then by absolute frequencies, accompanied by the logarithms of their assigned probabilities (U) – Continued

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
IN	75	1.88	.92	LO	13	1.11	.59	ND	52	1.72	.85	OV	7	0.85	.48
IO	41	1.61	.80	LY	10	1.00	.55	NI	30	1.48	.75	OO	6	0.78	.45
IS	35	1.54	.78	LD	9	0.95	.53	NG	27	1.43	.73	OI	5	0.70	.42
IR	27	1.43	.73	LT	8	0.90	.51	NA	26	1.41	.72	OB	4	0.60	.38
IT	27	1.43	.73	LS	6	0.78	.45	NS	24	1.38	.71	OE	3	0.48	.33
IV	25	1.40	.72	LB	3	0.48	.33	NC	19	1.28	.67	OH	3	0.48	.33
IL	23	1.36	.70	LC	3	0.48	.33	NO	18	1.26	.66	OG	2	0.30	.25
IC	22	1.34	.69	LF	3	0.48	.33	NF	9	0.95	.53	OK	2	0.30	.25
IG	19	1.28	.67	LP	3	0.48	.33	NN	8	0.90	.51	OY	2	0.30	.25
IX	15	1.18	.62	LM	2	0.30	.25	NU	7	0.85	.48	OJ	1	0.00	.13
IE	13	1.11	.59	LR	2	0.30	.25	NL	5	0.70	.42	OX	1	0.00	.13
IF	10	1.00	.55	LU	2	0.30	.25	NM	5	0.70	.42				
IM	9	0.95	.53	LV	2	0.30	.25	NY	5	0.70	.42	PE	23	1.36	.70
IA	8	0.90	.51	LW	2	0.30	.25	NH	4	0.60	.38	PR	18	1.26	.66
IP	7	0.85	.48	LG	1	0.00	.13	NR	4	0.60	.38	PO	17	1.23	.64
ID	6	0.78	.45	LH	1	0.00	.13	NP	3	0.48	.33	PA	14	1.15	.61
IB	2	0.30	.25	LN	1	0.00	.13	NV	3	0.48	.33	PL	13	1.11	.59
IK	2	0.30	.25					NW	3	0.48	.33	PP	11	1.04	.56
IZ	2	0.30	.25	MA	36	1.56	.78	NB	2	0.30	.25	PT	8	0.90	.51
				ME	26	1.41	.72	NK	2	0.30	.25	PI	6	0.78	.45
JE	2	0.30	.25	MM	13	1.11	.59	NJ	1	0.00	.13	PS	6	0.78	.45
JO	2	0.30	.25	MO	10	1.00	.55	NQ	1	0.00	.13	PM	4	0.60	.38
JU	2	0.30	.25	MI	9	0.95	.53					PH	3	0.48	.33
JA	1	0.00	.13	MP	8	0.90	.51					PU	3	0.48	.33
				MB	6	0.78	.45	ON	77	1.89	.92	PF	2	0.30	.25
KE	6	0.78	.45	MS	4	0.60	.38	OR	64	1.81	.89	PB	1	0.00	.13
KI	2	0.30	.25	MC	3	0.48	.33	OU	37	1.57	.79	PC	1	0.00	.13
KA	1	0.00	.13	MR	2	0.30	.25	OF	25	1.40	.72	PD	1	0.00	.13
KC	1	0.00	.13	MT	2	0.30	.25	OM	25	1.40	.72	PN	1	0.00	.13
KL	1	0.00	.13	MU	2	0.30	.25	OP	25	1.40	.72	PV	1	0.00	.13
KN	1	0.00	.13	MY	2	0.30	.25	OL	19	1.28	.67	PW	1	0.00	.13
KS	1	0.00	.13	MD	1	0.00	.13	OT	19	1.28	.67	PY	1	0.00	.13
				MF	1	0.00	.13	OS	14	1.15	.61				
LE	37	1.57	.79	MH	1	0.00	.13	OD	12	1.08	.58				
LA	28	1.45	.74					OC	8	0.90	.51	QU	15	1.18	.62
LL	27	1.43	.73	NT	82	1.91	.93	OW	8	0.90	.51	QM	1	0.00	.13
LI	20	1.30	.67	NE	57	1.76	.87	OA	7	0.85	.48	QR	1	0.00	.13

Table A–6 (~~C~~). The 428 digraphs of Table A–1, arranged in alphabetic order by initial letters, then by absolute frequencies accompanied by the logarithms of their assigned probabilities (U) – Continued

	F	L_{10} (F)	L_{224} (2F)
RE	98	1.99	.96
RT	42	1.62	.81
RA	39	1.59	.80
RS	31	1.49	.75
RI	30	1.48	.75
RO	28	1.45	.74
RD	17	1.23	.64
RP	13	1.11	.59
RR	11	1.04	.56
RC	9	0.95	.53
RM	9	0.95	.53
RY	9	0.95	.53
RG	7	0.85	.48
RN	7	0.85	.48
RF	6	0.78	.45
RL	5	0.70	.42
RU	5	0.70	.42
RV	5	0.70	.42
RW	4	0.60	.38
RH	3	0.48	.33
RB	2	0.30	.25
RJ	1	0.00	.13
RK	1	0.00	.13
ST	63	1.80	.88
SE	49	1.69	.84
SI	34	1.53	.77
SH	26	1.41	.72
SA	24	1.38	.71
SS	19	1.28	.67
SO	15	1.18	.62
SC	13	1.11	.59
SF	12	1.08	.58
SU	11	1.04	.56
SP	10	1.00	.55
SD	5	0.70	.42
SR	5	0.70	.42
SN	4	0.60	.38
SW	4	0.60	.38
SB	3	0.48	.33
SM	3	0.48	.33
SG	2	0.30	.25
SL	2	0.30	.25
SK	1	0.00	.13
SV	1	0.00	.13
SY	1	0.00	.13
TH	78	1.89	.92
TE	71	1.85	.91
TO	50	1.70	.84
TI	45	1.65	.82
TY	41	1.61	.80
TW	36	1.56	.78
TA	28	1.45	.74
TS	19	1.28	.67
TT	19	1.28	.67
TR	17	1.23	.64
TF	7	0.85	.48
TN	7	0.85	.48
TC	6	0.78	.45
TD	6	0.78	.45
TM	6	0.78	.45
TL	5	0.70	.42
TU	5	0.70	.42
TB	3	0.48	.33
TP	2	0.30	.25
TG	1	0.00	.13
TQ	1	0.00	.13
TZ	1	0.00	.13
UR	31	1.49	.75
UN	21	1.32	.68
US	12	1.08	.58
UT	12	1.08	.58
UE	11	1.04	.56
UG	8	0.90	.51
UL	6	0.78	.45
UA	5	0.70	.42
UI	5	0.70	.42
UM	5	0.70	.42
UB	3	0.48	.33
UC	3	0.48	.33
UD	3	0.48	.33
UP	2	0.30	.25
UF	1	0.00	.13
UO	1	0.00	.13
UV	1	0.00	.13
VE	57	1.76	.87
VI	12	1.08	.58
VA	6	0.78	.45
VO	1	0.00	.13
VT	1	0.00	.13
WE	22	1.34	.69
WO	19	1.28	.67
WI	13	1.11	.59
WA	12	1.08	.58
WH	4	0.60	.38
WN	2	0.30	.25
WL	1	0.00	.13
WR	1	0.00	.13
WS	1	0.00	.13
WY	1	0.00	.13
XT	7	0.85	.48
XA	2	0.30	.25
XC	2	0.30	.25
XI	2	0.30	.25
XP	2	0.30	.25
XD	1	0.00	.13
XE	1	0.00	.13
XF	1	0.00	.13
XH	1	0.00	.13
XN	1	0.00	.13
XO	1	0.00	.13
XR	1	0.00	.13
XS	1	0.00	.13
YT	15	1.18	.62
YF	11	1.04	.56
YS	11	1.04	.56
YO	10	1.00	.55
YE	9	0.95	.53
YA	6	0.78	.45
YN	6	0.78	.45
YC	4	0.60	.38
YD	4	0.60	.38
YR	4	0.60	.38
YI	3	0.48	.33
YP	3	0.48	.33
YB	2	0.30	.25
YL	2	0.30	.25
YM	2	0.30	.25
YG	1	0.00	.13
YH	1	0.00	.13
YU	1	0.00	.13
YW	1	0.00	.13
ZE	2	0.30	.25
ZA	1	0.00	.13
ZI	1	0.00	.13
	5,000		

Table A–7 (~~C~~). The 428 digraphs of Table A–1, arranged in alphabetic order by final letters, then by absolute frequency, accompanied by the logarithms of their assigned probabilities (U)

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
RA	39	1.59	.80	EC	32	1.51	.76	RE	98	1.99	.96	GF	2	0.30	.25
MA	36	1.56	.78	IC	22	1.34	.69	TE	71	1.85	.91	PF	2	0.30	.25
EA	35	1.54	.78	NC	19	1.28	.67	NE	57	1.76	.87	CF	1	0.00	.13
DA	32	1.51	.76	AC	14	1.15	.61	VE	57	1.76	.87	MF	1	0.00	.13
LA	28	1.45	.74	SC	13	1.11	.59	SE	49	1.69	.84	UF	1	0.00	.13
TA	28	1.45	.74	RC	9	0.95	.53	EE	42	1.62	.81	XF	1	0.00	.13
NA	26	1.41	.72	OC	8	0.90	.51	LE	37	1.57	.79				
SA	24	1.38	.71	TC	6	0.78	.45	DE	33	1.52	.77				
CA	20	1.30	.67	DC	4	0.60	.38	CE	32	1.51	.76	NG	27	1.43	.73
HA	20	1.30	.67	YC	4	0.60	.38	ME	26	1.41	.72	IG	19	1.28	.67
PA	14	1.15	.61	CC	3	0.48	.33	PE	23	1.36	.70	UG	8	0.90	.51
WA	12	1.08	.58	HC	3	0.48	.33	WE	22	1.34	.69	RG	7	0.85	.48
IA	8	0.90	.51	LC	3	0.48	.33	HE	20	1.30	.67	AG	6	0.78	.45
GA	7	0.85	.48	MC	3	0.48	.33	BE	18	1.26	.66	EG	4	0.60	.38
OA	7	0.85	.48	UC	3	0.48	.33	GE	14	1.15	.61	DG	2	0.30	.25
VA	6	0.78	.45	FC	2	0.30	.25	IE	13	1.11	.59	OG	2	0.30	.25
YA	6	0.78	.45	GC	2	0.30	.25	UE	11	1.04	.56	SG	2	0.30	.25
FA	5	0.70	.42	XC	2	0.30	.25	FE	10	1.00	.55	FG	1	0.00	.13
UA	5	0.70	.42	KC	1	0.00	.13	YE	9	0.95	.53	GG	1	0.00	.13
BA	4	0.60	.38	PC	1	0.00	.13	KE	6	0.78	.45	LG	1	0.00	.13
AA	3	0.48	.33					OE	3	0.48	.33	TG	1	0.00	.13
XA	2	0.30	.25					JE	2	0.30	.25	YG	1	0.00	.13
JA	1	0.00	.13	ED	60	1.78	.88	ZE	2	0.30	.25				
KA	1	0.00	.13	ND	52	1.72	.85	AE	1	0.00	.13				
ZA	1	0.00	.13	AD	27	1.43	.73	XE	1	0.00	.13				
				RD	17	1.23	.64					TH	78	1.89	.92
AB	6	0.78	.45	OD	12	1.08	.58					SH	26	1.41	.72
MB	6	0.78	.45	LD	9	0.95	.53					GH	20	1.30	.67
DB	4	0.60	.38	DD	8	0.90	.51	OF	25	1.40	.72	CH	14	1.15	.61
EB	4	0.60	.38	ID	6	0.78	.45	EF	18	1.26	.66	EH	7	0.85	.48
OB	4	0.60	.38	TD	6	0.78	.45	SF	12	1.08	.58	NH	4	0.60	.38
LB	3	0.48	.33	SD	5	0.70	.42	FF	11	1.04	.56	WH	4	0.60	.38
SB	3	0.48	.33	YD	4	0.60	.38	YF	11	1.04	.56	OH	3	0.48	.33
TB	3	0.48	.33	UD	3	0.48	.33	IF	10	1.00	.55	PH	3	0.48	.33
UB	3	0.48	.33	HD	2	0.30	.25	NF	9	0.95	.53	RH	3	0.48	.33
IB	2	0.30	.25	CD	1	0.00	.13	DF	8	0.90	.51	AH	2	0.30	.25
NB	2	0.30	.25	FD	1	0.00	.13	TF	7	0.85	.48	DH	2	0.30	.25
RB	2	0.30	.25	GD	1	0.00	.13	RF	6	0.78	.45	LH	1	0.00	.13
YB	2	0.30	.25	MD	1	0.00	.13	HF	5	0.70	.42	MH	1	0.00	.13
HB	1	0.00	.13	PD	1	0.00	.13	AF	4	0.60	.38	XH	1	0.00	.13
PB	1	0.00	.13	XD	1	0.00	.13	LF	3	0.48	.33	YH	1	0.00	.13

Table A–7 (~~C~~). The 428 digraphs of Table A–1, arranged in alphabetic order by final letters then by absolute frequency, accompanied by the logarithms of their assigned probabilities (U) – Continued

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
TI	45	1.65	.82	LL	27	1.43	.73	AN	64	1.81	.89	RP	13	1.11	.59
FI	39	1.59	.80	IL	23	1.36	.70	UN	21	1.32	.68	AP	12	1.08	.58
SI	34	1.53	.77	OL	19	1.28	.67	NN	8	0.90	.51	PP	11	1.04	.56
HI	33	1.52	.77	PL	13	1.11	.59	RN	7	0.85	.48	SP	10	1.00	.55
NI	30	1.48	.75	BL	6	0.78	.45	TN	7	0.85	.48	MP	8	0.90	.51
RI	30	1.48	.75	UL	6	0.78	.45	YN	6	0.78	.45	IP	7	0.85	.48
DI	27	1.43	.73	CL	5	0.70	.42	DN	4	0.60	.38	DP	5	0.70	.42
EI	27	1.43	.73	NL	5	0.70	.42	SN	4	0.60	.38	LP	3	0.48	.33
LI	20	1.30	.67	RL	5	0.70	.42	GN	3	0.48	.33	NP	3	0.48	.33
AI	17	1.23	.64	TL	5	0.70	.42	HN	3	0.48	.33	YP	3	0.48	.33
WI	13	1.11	.59	DL	3	0.48	.33	WN	2	0.30	.25	GP	2	0.30	.25
VI	12	1.08	.58	FL	2	0.30	.25	CN	1	0.00	.13	TP	2	0.30	.25
MI	9	0.95	.53	GL	2	0.30	.25	KN	1	0.00	.13	UP	2	0.30	.25
CI	7	0.85	.48	SL	2	0.30	.25	LN	1	0.00	.13	XP	2	0.30	.25
PI	6	0.78	.45	YL	2	0.30	.25	PN	1	0.00	.13	FP	1	0.00	.13
GI	5	0.70	.42	HL	1	0.00	.13	XN	1	0.00	.13	HP	1	0.00	.13
OI	5	0.70	.42	KL	1	0.00	.13								
UI	5	0.70	.42	WL	1	0.00	.13					EQ	12	1.08	.58
YI	3	0.48	.33					TO	50	1.70	.84	DQ	2	0.30	.25
BI	2	0.30	.25					CO	41	1.61	.80	HQ	1	0.00	.13
KI	2	0.30	.25	OM	25	1.40	.72	IO	41	1.61	.80	NQ	1	0.00	.13
XI	2	0.30	.25	AM	14	1.15	.61	FO	40	1.60	.80	TQ	1	0.00	.13
ZI	1	0.00	.13	EM	14	1.15	.61	RO	28	1.45	.74				
				MM	13	1.11	.59	HO	20	1.30	.67	ER	87	1.94	.94
				IM	9	0.95	.53	WO	19	1.28	.67	OR	64	1.81	.89
AJ	1	0.00	.13	RM	9	0.95	.53	NO	18	1.26	.66	AR	44	1.64	.82
BJ	1	0.00	.13	TM	6	0.78	.45	PO	17	1.23	.64	UR	31	1.49	.75
DJ	1	0.00	.13	DM	5	0.70	.42	DO	16	1.20	.63	IR	27	1.43	.73
EJ	1	0.00	.13	NM	5	0.70	.42	SO	15	1.18	.62	PR	18	1.26	.66
GJ	1	0.00	.13	UM	5	0.70	.42	LO	13	1.11	.59	HR	17	1.23	.64
NJ	1	0.00	.13	PM	4	0.60	.38	EO	12	1.08	.58	TR	17	1.23	.64
OJ	1	0.00	.13	SM	3	0.48	.33	MO	10	1.00	.55	DR	12	1.08	.58
RJ	1	0.00	.13	HM	2	0.30	.25	YO	10	1.00	.55	RR	11	1.04	.56
				LM	2	0.30	.25	GO	6	0.78	.45	FR	9	0.95	.53
CK	4	0.60	.38	YM	2	0.30	.25	OO	6	0.78	.45	GR	5	0.70	.42
AK	2	0.30	.25	BM	1	0.00	.13	BO	4	0.60	.38	SR	5	0.70	.42
IK	2	0.30	.25	CM	1	0.00	.13	AO	2	0.30	.25	CR	4	0.60	.38
NK	2	0.30	.25	FM	1	0.00	.13	JO	2	0.30	.25	NR	4	0.60	.38
OK	2	0.30	.25	GM	1	0.00	.13	UO	1	0.00	.13	YR	4	0.60	.38
RK	1	0.00	.13	QM	1	0.00	.13	VO	1	0.00	.13	BR	2	0.30	.25
SK	1	0.00	.13					XO	1	0.00	.13	LR	2	0.30	.25
												MR	2	0.30	.25
				EN	111	2.05	.99					QR	1	0.00	.13
AL	32	1.51	.76	ON	77	1.89	.92	OP	25	1.40	.72	WR	1	0.00	.13
EL	29	1.46	.74	IN	75	1.88	.92	EP	20	1.30	.67	XR	1	0.00	.13

Table A–7 ~~(C)~~. The 428 digraphs of Table A–1, arranged in alphabetic order by final letters, then according to their absolute frequency, accompanied by the logarithms of their assigned probabilities (U) – Continued

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
ES	54	1.73	.86	OT	19	1.28	.67	JU	2	0.30	.25	PW	1	0.00	.13
AS	41	1.61	.80	TT	19	1.28	.67	LU	2	0.30	.25	YW ...	1	0.00	.13
IS	35	1.54	.78	DT	15	1.18	.62	MU ...	2	0.30	.25				
RS	31	1.49	.75	YT	15	1.18	.62	YU ...	1	0.00	.13	IX	15	1.18	.62
NS	24	1.38	.71	CT	14	1.15	.61					EX	7	0.85	.48
SS	19	1.28	.67	UT	12	1.08	.58	IV	25	1.40	.72	OX ...	1	0.00	.13
TS	19	1.28	.67	FT	11	1.04	.56	EV	20	1.30	.67				
OS	14	1.15	.61	LT	8	0.90	.51	AV ...	7	0.85	.48	TY	41	1.61	.80
DS	13	1.11	.59	PT	8	0.90	.51	OV ...	7	0.85	.48	AY ...	12	1.08	.58
US	12	1.08	.58	XT	7	0.85	.48	RV ...	5	0.70	.42	LY	10	1.00	.55
YS	11	1.04	.56	GT	4	0.60	.38	DV ...	3	0.48	.33	RY ...	9	0.95	.53
LS	6	0.78	.45	MT ...	2	0.30	.25	NV ...	3	0.48	.33	BY	7	0.85	.48
PS	6	0.78	.45	BT	1	0.00	.13	LV	2	0.30	.25	NY ...	5	0.70	.42
HS	4	0.60	.38	VT	1	0.00	.13	PV	1	0.00	.13	EY	4	0.60	.38
MS	4	0.60	.38					SV	1	0.00	.13	MY ...	2	0.30	.25
FS	3	0.48	.33	OU ...	37	1.57	.79	UV ...	1	0.00	.13	OY ...	2	0.30	.25
GS	3	0.48	.33	QU ...	15	1.18	.62					CY	1	0.00	.13
BS	1	0.00	.13	AU ...	13	1.11	.59	TW ...	36	1.56	.78	DY ...	1	0.00	.13
CS	1	0.00	.13	SU	11	1.04	.56	OW ...	8	0.90	.51	FY	1	0.00	.13
KS	1	0.00	.13	HU ...	8	0.90	.51	EW ...	7	0.85	.48	HY ...	1	0.00	.13
WS	1	0.00	.13	NU ...	7	0.85	.48	DW ...	4	0.60	.38	PY	1	0.00	.13
XS	1	0.00	.13	DU ...	5	0.70	.42	RW ...	4	0.60	.38	SY	1	0.00	.13
				RU ...	5	0.70	.42	SW	4	0.60	.38	WY ...	1	0.00	.13
NT	82	1.91	.93	TU	5	0.70	.42	AW ...	3	0.48	.33				
ST	63	1.80	.88	CU	4	0.60	.38	NW ...	3	0.48	.33	IZ	2	0.30	.25
AT	47	1.67	.83	EU	3	0.48	.33	LW ...	2	0.30	.25	EZ	1	0.00	.13
RT	42	1.62	.81	FU	3	0.48	.33	CW ...	1	0.00	.13	TZ	1	0.00	.13
ET	37	1.57	.79	PU	3	0.48	.33	FW ...	1	0.00	.13		5,000		
HT	28	1.45	.74	BU	2	0.30	.25	GW ...	1	0.00	.13				
IT	27	1.43	.73	GU ...	2	0.30	.25	HW ...	1	0.00	.13				

Table A–8 (~~C~~). The 18 digraphs composing 25% of the digraphs of Table A–1, accompanied by the logarithms of their assigned probabilities, arranged alphabetically by final letters (U)

(1) AND ACCORDING TO THEIR INITIAL LETTERS

(2) AND ACCORDING TO THEIR ABSOLUTE FREQUENCIES

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
ED	60	1.78	.88	IN	75	1.88	.92	ED	60	1.78	.88	IN	75	1.88	.92
ND ...	52	1.72	.85	ON ...	77	1.89	.92	ND ...	52	1.72	.85	AN ...	64	1.81	.89
NE	57	1.76	.87	TO	50	1.70	.84	RE	98	1.99	.96	TO	50	1.70	.84
RE	98	1.99	.96					TE	71	1.85	.91				
SE	49	1.69	.84	ER	87	1.94	.94	NE	57	1.76	.87	ER	87	1.94	.94
TE	71	1.85	.91	OR ...	64	1.81	.89	VE	57	1.76	.87	OR ...	64	1.81	.89
VE	57	1.76	.87					SE	49	1.69	.84				
				ES	54	1.73	.86					ES	54	1.73	.86
TH	78	1.89	.92					TH	78	1.89	.92				
				NT	82	1.91	.93					NT	82	1.91	.93
AN ...	64	1.81	.89	ST	63	1.80	.88	EN	111	2.05	.99	ST	63	1.80	.88
EN	111	2.05	.99		1,249			ON ...	77	1.89	.92		1,249		

Table A–9 (~~C~~). The 53 digraphs composing 50% of the digraphs of Table A–1, accompanied by the logarithms of their assigned probabilities, arranged alphabetically by final letters (U)

(1) AND ACCORDING TO THEIR INITIAL LETTERS

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
DA ...	32	1.51	.76	NE	57	1.76	.87	AN ...	64	1.81	.89	AS	41	1.61	.80
EA	35	1.54	.78	RE	98	1.99	.96	EN	111	2.05	.99	ES	54	1.73	.86
LA	28	1.45	.74	SE	49	1.69	.84	IN	75	1.88	.92	IS	35	1.54	.78
MA ...	36	1.56	.78	TE	71	1.85	.91	ON ...	77	1.89	.92	RS	31	1.49	.75
RA ...	39	1.59	.80	VE	57	1.76	.87								
TA	28	1.45	.74									AT	47	1.67	.83
				TH	78	1.89	.92	CO	41	1.61	.80	ET	37	1.57	.79
EC	32	1.51	.76					FO	40	1.60	.80	HT	28	1.45	.74
				FI	39	1.59	.80	IO	41	1.61	.80	NT	82	1.91	.93
				HI	33	1.52	.77	RO ...	28	1.45	.74	RT	42	1.62	.81
ED	60	1.78	.88	NI	30	1.48	.75	TO	50	1.70	.84	ST	63	1.80	.88
ND ...	52	1.72	.85	RI	30	1.48	.75								
				SI	34	1.53	.77					OU ...	37	1.57	.79
				TI	45	1.65	.82								
CE	32	1.51	.76					AR ...	44	1.64	.82	TW ...	36	1.56	.78
DE	33	1.52	.77					ER	87	1.94	.94				
EE	42	1.62	.81	AL	32	1.51	.76	OR ...	64	1.81	.89	TY	41	1.61	.80
LE	37	1.57	.79	EL	29	1.46	.74	UR ...	31	1.49	.75		2,495		

Table A–9 (~~C~~). The 53 digraphs composing 50% of the digraphs of Table A–1, accompanied by the logarithms of their assigned probabilities, arranged alphabetically by final letters (U) – Continued

(2) AND ACCORDING TO THEIR ABSOLUTE FREQUENCIES

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
RA ...	39	1.59	.80	EE	42	1.62	.81	EN	111	2.05	.99	ES	54	1.73	.86
MA ...	36	1.56	.78	LE	37	1.57	.79	ON ...	77	1.89	.92	AS	41	1.61	.80
EA	35	1.54	.78	DE	33	1.52	.77	IN	75	1.88	.92	IS	35	1.54	.78
DA ...	32	1.51	.76	CE	32	1.51	.76	AN ...	64	1.81	.89	RS	31	1.49	.75
LA	28	1.45	.74												
TA	28	1.45	.74									NT	82	1.91	.93
				TH	78	1.89	.92	TO	50	1.70	.84	ST	63	1.80	.88
EC	32	1.51	.76					CO	41	1.61	.80	AT	47	1.67	.83
								IO	41	1.61	,80	RT	42	1.62	.81
				TI	45	1.65	.82	FO	40	1.60	.80	ET	37	1.57	.79
ED	60	1.78	.88	FI	39	1.59	.80	RO ...	28	1.45	.74	HT	28	1.45	.74
ND ...	52	1.72	.85	SI	34	1.53	.77								
				HI	33	1.52	.77					OU ...	37	1.57	.79
RE	98	1.99	.96	NI	30	1.48	.75								
TE	71	1.85	.91	RI	30	1.48	.75	ER	87	1.94	.94	TW ...	36	1.56	.78
NE	57	1.76	.87					OR ...	64	1.81	.89				
VE	57	1.76	.87	AL	32	1.51	.76	AR ...	44	1.64	.82	TY	41	1.61	.80
SE	49	1.69	.84	EL	29	1.46	.74	UR ...	31	1.49	.75		2,495		

Table A–10 (~~C~~). The 122 digraphs composing 75% of the digraphs of Table A–1, accompanied by the logarithms of their assigned probabilities, arranged alphabetically by final letters (U)

(1) AND ACCORDING TO THEIR INITIAL LETTERS

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
CA	20	1.30	.67	ND ...	52	1.72	.85	EF	18	1.26	.66	SI	34	1.53	.77
DA ...	32	1.51	.76	RD ...	17	1.23	.64	OF	25	1.40	.72	TI	45	1.65	.82
EA	35	1.54	.78												
HA ...	20	1.30	.67	BE	18	1.26	.66	IG	19	1.28	.67	AL	32	1.51	.76
LA	28	1.45	.74	CE	32	1.51	.76	NG ...	27	1.43	.73	EL	29	1.46	.74
MA ...	36	1.56	.78	DE	33	1.52	.77					IL	23	1.36	.70
NA ...	26	1.41	.72	EE	42	1.62	.81	CH	14	1.15	.61	LL	27	1.43	.73
PA	14	1.15	.61	GE	14	1.15	.61	GH ...	20	1.30	.67	OL	19	1.28	.67
RA ...	39	1.59	.80	HE	20	1.30	.67	SH	26	1.41	.72				
SA	24	1.38	.71	IE	13	1.11	.59	TH	78	1.89	.92				
TA	28	1.45	.74	LE	37	1.57	.79					AM ...	14	1.15	.61
				ME ...	26	1.41	.72	AI	17	1.23	.64	EM ...	14	1.15	.61
AC	14	1.15	.61	NE	57	1.76	.87	DI	27	1.43	.73	OM ...	25	1.40	.72
EC	32	1.51	.76	PE	23	1.36	.70	EI	27	1.43	.73				
IC	22	1.34	.69	RE	98	1.99	.96	FI	39	1.59	.80	AN ...	64	1.81	.89
NC	19	1.28	.67	SE	49	1.69	.84	HI	33	1.52	.77	EN	111	2.05	.99
				TE	71	1.85	.91	LI	20	1.30	.67	IN	75	1.88	.92
AD ...	27	1.43	.73	VE	57	1.76	.87	NI	30	1.48	.75	ON ...	77	1.89	.92
ED	60	1.78	.88	WE ...	22	1.34	.69	RI	30	1.48	.75	UN ...	21	1.32	.68

Table A–10 (~~C~~). The 122 digraphs composing 75% of the digraphs of Table A–1, accompanied by the logarithms of their assigned probabilities, arranged alphabetically by final letters (U) – Continued

(1) AND ACCORDING TO THEIR INITIAL LETTERS– Continued

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
CO	41	1.61	.80	AR ...	44	1.64	.82	RS	31	1.49	.75	TT	·19	1.28	.67
DO ...	16	1.20	.63	ER	87	1.94	.94	SS	19	1.28	.67	YT	15	1.18	.62
FO	40	1.60	.80	HR ...	17	1.23	.64	TS	19	1.28	.67				
HO ...	20	1.30	.67	IR	27	1.43	.73					AU ...	13	1.11	.59
IO	41	1.61	.80	OR ...	64	1.81	.89					OU ...	37	1.57	.79
LO	13	1.11	.59	PR	18	1.26	.66					QU ...	15	1.18	.62
NO ...	18	1.26	.66	TR	17	1.23	.64	AT	47	1.67	.83				
PO	17	1.23	.64	UR ...	31	1.49	.75	CT	14	1.15	.61	EV	20	1.30	.67
RO ...	28	1.45	.74					DT	15	1.18	.62	IV	25	1.40	.72
SO	15	1.18	.62					ET	37	1.57	.79				
TO	50	1.70	.84	AS	41	1.61	.80	HT	28	1.45	.74	TW ...	36	1.56	.78
WO ...	19	1.28	.67	DS	13	1.11	.59	IT	27	1.43	.73				
				ES	54	1.73	.86	NT	82	1.91	.93	IX	15	1.18	.62
				IS	35	1.54	.78	OT	19	1.28	.67				
EP	20	1.30	.67	NS	24	1.38	.71	RT	42	1.62	.81	TY	41	1.61	.80
OP	25	1.40	.72	OS	14	1.15	.61	ST	63	1.80	.88		3,745		

(2) AND ACCORDING TO THEIR ABSOLUTE FREQUENCIES

	F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)		F	L_{10} (F)	L_{224} (2F)
RA ...	39	1.59	.80	RE	98	1.99	.96	TH	78	1.89	.92	OM ...	25	1.40	.72
MA ...	36	1.56	.78	TE	71	1.85	.91	SH	26	1.41	.72	AM ...	14	1.15	.61
EA	35	1.54	.78	NE	57	1.76	.87	GH ...	20	1.30	.67	EM ...	14	1.15	.61
DA ...	32	1.51	.76	VE	57	1.76	.87	CH	14	1.15	.61				
LA	28	1.45	.74	SE	49	1.69	.84					EN	111	2.05	.99
TA	28	1.45	.74	EE	42	1.62	.81					ON ...	77	1.89	.92
NA ...	26	1.41	.72	LE	37	1.57	.79	TI	45	1.65	.82	IN	75	1.88	.92
SA	24	1.38	.71	DE	33	1.52	.77	FI	39	1.59	.80	AN ...	64	1.81	.89
CA	20	1.30	.67	CE	32	1.51	.76	SI	34	1.53	.77	UN ...	21	1.32	.68
HA ...	20	1.30	.67	ME ...	26	1.41	.72	HI	33	1.52	.77				
PA	14	1.15	.61	PE	23	1.36	.70	NI	30	1.48	.75	TO	50	1.70	.84
				WE ...	22	1.34	.69	RI	30	1.48	.75	CO	41	1.61	.80
EC	32	1.51	.76	HE	20	1.30	.67	DI	27	1.43	.73	IO	41	1.61	.80
IC	22	1.34	.69	BE	18	1.26	.66	EI	27	1.43	.73	FO	40	1.60	.80
NC	19	1.28	.67	GE	14	1.15	.61	LI	20	1.30	.67	RO ...	28	1.45	.74
AC	14	1.15	.61	IE	13	1.11	.59	AI	17	1.23	.64	HO ...	20	1.30	.67
												WO ...	19	1.28	.67
				OF	25	1.40	.72	AL	32	1.51	.76	NO ...	18	1.26	.66
ED	60	1.78	.88	EF	18	1.26	.66	EL	29	1.46	.74	PO	17	1.23	.64
ND ...	52	1.72	.85					LL	27	1.43	.73	DO ...	16	1.20	.63
AD ...	27	1.43	.73	NG ...	27	1.43	.73	IL	23	1.36	.70	SO	15	1.18	.62
RD ...	17	1.23	.64	IG	19	1.28	.67	OL	19	1.28	.67	LO	13	1.11	.59

Table A–10 ~~(C)~~. The 122 digraphs composing 75% of the digraphs of Table A–1, accompanied by the logarithms of their assigned probabilities, arranged alphabetically by final letters (U) – Continued

(2) AND ACCORDING TO THEIR ABSOLUTE FREQUENCIES–Continued

	F	L_{10}	L_{224}		F	L_{10}	L_{224}		F	L_{10}	L_{224}		F	L_{10}	L_{224}
		(F)	(2F)			(F)	(2F)			(F)	(2F)			(F)	(2F)
OP	25	1.40	.72	ES	54	1.73	.86	NT	82	1.91	.93	OU ...	37	1.57	.79
EP	20	1.30	.67	AS	41	1.61	.80	ST	63	1.80	.88	QU ...	15	1.18	.62
				IS	35	1.54	.78	AT	47	1.67	.83	AU ...	13	1.11	.59
				RS	31	1.49	.75	RT	42	1.62	.81				
				NS	24	1.38	.71	ET	37	1.57	.79	IV	25	1.40	.72
ER	87	1.94	.94	SS	19	1.28	.67	HT	28	1.45	.74	EV	20	1.30	.67
OR ...	64	1.81	.89	TS	19	1.28	.67	IT	27	1 43	.73				
AR ...	44	1.64	.82	OS	14	1.15	.61	OT	19	1.28	.67	TW ...	36	1.56	.78
UR ...	31	1.49	.75	DS	13	1.11	.59	TT	19	1.28	.67				
IR	27	1.43	.73					DT	15	1.18	.62	IX	15	1.18	.62
PR	18	1.26	.66					YT	15	1.18	.62				
HR ...	17	1.23	.64					CT	14	1.15	.61	TY	41	1.61	.80
TR	17	1.23	.64										3,745		

APPENDIX B (~~C~~)
FREQUENCY DISTRIBUTIONS OF ENGLISH TRIGRAPHS

Frequency distributions of English trigraphs appearing in 50,000 letters of governmental plaintext telegrams.

Table B–1 (~~C~~). The 56 trigraphs appearing 100 or more times, arranged according to their absolute frequencies, accompanied by the logarithms of their assigned probabilities (U)

	F	L_{10} (F)	L_{586} (F)		F	L_{10} (F)	L_{586} (F)		F	L_{10} (F)	L_{586} (F)
ENT	569	2.76	.99	TOP	174	2.24	.82	EIG	135	2.13	.79
ION	260	2.41	.88	NTH	171	2.23	.82	FIV	135	2.13	.79
AND	228	2.36	.86	TWE	170	2.23	.82	MEN	131	2.12	.78
ING	226	2.35	.86	TWO	163	2.21	.81	SEV	131	2.12	.78
IVE	225	2.35	.86	ATI	160	2.20	.81	ERS	126	2.10	.78
TIO	221	2.34	.85	THR	158	2.20	.81	UND	125	2.10	.78
FOR	218	2.34	.85	NTY	157	2.20	.81	NET	118	2.07	.77
OUR	211	2.32	.85	HRE	153	2.18	.80	PER	115	2.06	.76
THI	211	2.32	.85	WEN	153	2.18	.80	STA	115	2.06	.76
ONE	210	2.32	.85	FOU	152	2.18	.80	TER	115	2.06	.76
NIN	207	2.32	.85	ORT	146	2.16	.80	EQU	114	2.06	.76
STO	202	2.31	.84	REE	146	2.16	.80	RED	113	2.05	.76
EEN	196	2.29	.84	SIX	146	2.16	.80	TED	112	2.05	.76
GHT	196	2.29	.84	ASH	143	2.16	.80	ERI	109	2.04	.76
INE	192	2.28	.83	DAS	140	2.15	.79	HIR	106	2.03	.75
VEN	190	2.28	.83	IGH	140	2.15	.79	IRT	105	2.02	.75
EVE	177	2.25	.82	ERE	138	2.14	.79	DER	101	2.00	.74
EST	176	2.25	.82	COM	136	2.13	.79	DRE	100	2.00	.74
TEE	174	2.24	.82	ATE	135	2.13	.79				

Table B–2 (~~C~~). The 56 trigraphs appearing 100 or more times, arranged in alphabetic order by initial letters, then by absolute frequencies, accompanied by the logarithms of their assigned probabilities (U)

	F	L_{10} (F)	L_{586} (F)		F	L_{10} (F)	L_{586} (F)		F	L_{10} (F)	L_{586} (F)
AND	228	2.36	.86	GHT	196	2.29	.84	REE	146	2.16	.80
ATI	160	2.20	.81					RED	113	2.05	.76
ASH	143	2.16	.80	HRE	153	2.18	.80				
ATE	135	2.13	.79	HIR	106	2.03	.75	STO	202	2.31	.84
								SIX	146	2.16	.80
COM	136	2.13	.79	ION	260	2.41	.88	SEV	131	2.12	.78
				ING	226	2.35	.86	STA	115	2.06	.76
DAS	140	2.15	.79	IVE	225	2.35	.86				
DER	101	2.00	.74	INE	192	2.28	.83				
DRE	100	2.00	.74	IGH	140	2.15	.79	TIO	221	2.34	.85
				IRT	105	2.02	.75	THI	211	2.32	.85
ENT	569	2.76	.99					TEE	174	2.24	.82
EEN	196	2.29	.84	MEN	131	2.12	.78	TOP	174	2.24	.82
EVE	177	2.25	.82					TWE	170	2.23	.82
EST	176	2.25	.82	NIN	207	2.32	.85	TWO	163	2.21	.81
ERE	138	2.14	.79	NTH	171	2.23	.82	THR	158	2.20	.81
EIG	135	2.13	.79	NTY	157	2.20	.81	TER	115	2.06	.76
ERS	126	2.10	.78	NET	118	2.07	.77	TED	112	2.05	.76
EQU	114	2.06	.76								
ERI	109	2.04	.76	OUR	211	2.32	.85	UND	125	2.10	.78
				ONE	210	2.32	.85				
FOR	218	2.34	.85	ORT	146	2.16	.80	VEN	190	2.28	.83
FOU	152	2.18	.80								
FIV	135	2.13	.79	PER	115	2.06	.76	WEN	153	2.18	.80

Table B–3 (~~C~~). The 56 trigraphs appearing 100 or more times, arranged in alphabetic order by central letters, then by absolute frequencies, accompanied by the logarithms of their assigned probabilities (U)

	F	L_{10} (F)	L_{586} (F)		F	L_{10} (F)	L_{586} (F)		F	L_{10} (F)	L_{586} (F)
DAS	140	2.15	.79	TIO	221	2.34	.85	HRE	153	2.18	.80
				NIN	207	2.32	.85	ORT	146	2.16	.80
				SIX	146	2.16	.80	ERE	138	2.14	.79
				EIG	135	2.13	.79	ERS	126	2.10	.78
EEN	196	2.29	.84	FIV	135	2.13	.79	ERI	109	2.04	.76
VEN	190	2.28	.83	HIR	106	2.03	.75	IRT	105	2.02	.75
TEE	174	2.24	.82					DRE	100	2.00	.74
WEN	153	2.18	.80								
REE	146	2.16	.80	ENT	569	2.76	.99	EST	176	2.25	.82
MEN	131	2.12	.78	AND	228	2.36	.86	ASH	143	2.16	.80
SEV	131	2.12	.78	ING	226	2.35	.86				
NET	118	2.07	.77	ONE	210	2.32	.85	STO	202	2.31	.84
PER	115	2.06	.76	INE	192	2.28	.83	NTH	171	2.23	.82
TER	115	2.06	.76	UND	125	2.10	.78	ATI	160	2.20	.81
RED	113	2.05	.76					NTY	157	2.20	.81
TED	112	2.05	.76					ATE	135	2.13	.79
DER	101	2.00	.74	ION	260	2.41	.88	STA	115	2.06	.76
				FOR	218	2.34	.85				
				TOP	174	2.24	.82	OUR	211	2.32	.85
IGH	140	2.15	.79	FOU	152	2.18	.80				
				COM	136	2.13	.79	IVE	225	2.35	.86
								EVE	177	2.25	.82
THI	211	2.32	.85								
GHT	196	2.29	.84					TWE	170	2.23	.82
THR	158	2.20	.81	EQU	114	2.06	.76	TWO	163	2.21	.81

Table B–4 (~~C~~). The 56 trigraphs appearing 100 or more times, arranged in alphabetic order by final letters, then by absolute frequencies, accompanied by the logarithms of their assigned probabilities (U)

	F	L_{10} (F)	L_{586} (F)		F	L_{10} (F)	L_{586} (F)		F	L_{10} (F)	L_{586} (F)
STA	115	2.06	.76	THI	211	2.32	.85	TER	115	2.06	.76
				ATI	160	2.20	.81	HIR	106	2.03	.75
AND	228	2.36	.86	ERI	109	2.04	.76	DER	101	2.00	.74
UND	125	2.10	.78								
RED	113	2.05	.76	COM	136	2.13	.79	DAS	140	2.15	.79
TED	112	2.05	.76					ERS	126	2.10	.78
				ION	260	2.41	.88				
IVE	225	2.35	.86	NIN	207	2.32	.85	ENT	569	2.76	.99
ONE	210	2.32	.85	EEN	196	2.29	.84	GHT	196	2.29	.84
INE	192	2.28	.83	VEN	190	2.28	.83	EST	176	2.25	.82
EVE	177	2.25	.82	WEN	153	2.18	.80	ORT	146	2.16	.80
TEE	174	2.24	.82	MEN	131	2.12	.78	NET	118	2.07	.77
TWE	170	2.23	.82					IRT	105	2.02	.75
HRE	153	2.18	.80	TIO	221	2.34	.85				
REE	146	2.16	.80	STO	202	2.31	.84	FOU	152	2.18	.80
ERE	138	2.14	.79	TWO	163	2.21	.81	EQU	114	2.06	.76
ATE	135	2.13	.79								
DRE	100	2.00	.74					FIV	135	2.13	.79
				TOP	174	2.24	.82	SEV	131	2.12	.78
ING	226	2.35	.86								
EIG	135	2.13	.79								
				FOR	218	2.34	.85	SIX	146	2.16	.80
NTH	171	2.23	.82	OUR	211	2.32	.85				
ASH	143	2.16	.80	THR	158	2.20	.81				
IGH	140	2.15	.79	PER	115	2.06	.76	NTY	157	2.20	.81

APPENDIX C (~~C~~)
FREQUENCY DISTRIBUTION OF ENGLISH TETRAGRAPHS

Frequency distributions of English tetragraphs appearing in 50,000 letters of governmental plaintext telegrams.

Table C–1 ~~(C)~~. The 54 tetragraphs appearing 50 or more times, arranged by absolute frequencies, accompanied by the logarithms of assigned probabilities (U)

	F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)
TION	218	2.34	.99	THIR	104	2.02	.87	ASHT	64	1.81	.79
EVEN	168	2.23	.95	EENT	102	2.01	.87	HUND	64	1.81	.79
TEEN	163	2.21	.94	REQU	98	1.99	.86	DRED	63	1.80	.79
ENTY	161	2.21	.94	HIRT	97	1.99	.86	RIOD	63	1.80	.79
STOP	154	2.19	.93	COMM	93	1.97	.85	IVED	62	1.79	.78
WENT	153	2.18	.93	QUES	87	1.94	.84	ENTS	62	1.79	.78
NINE	153	2.18	.93	UEST	87	1.94	.84	FFIC	62	1.79	.78
TWEN	152	2.18	.93	EQUE	86	1.93	.84	FROM	59	1.77	.78
THRE	149	2.17	.93	NDRE	77	1.89	.82	IRTY	59	1.77	.78
FOUR	144	2.16	.92	OMMA	71	1.85	.81	RTEE	59	1.77	.78
IGHT	140	2.15	.92	LLAR	71	1.85	.81	UNDR	59	1.77	.78
FIVE	135	2.13	.91	OLLA	70	1.85	.81	NAUG	56	1.75	.77
HREE	134	2.13	.91	VENT	70	1.85	.81	OURT	56	1.75	.77
DASH	132	2.12	.91	DOLL	68	1.83	.80	UGHT	56	1.75	.77
EIGH	132	2.12	.91	LARS	68	1.83	.80	STAT	54	1.73	.76
SEVE	121	2.08	.89	THIS	68	1.83	.80	AUGH	52	1.72	.76
ENTH	114	2.06	.89	PERI	67	1.83	.80	CENT	52	1.72	.76
MENT	111	2.05	.88	ERIO	66	1.82	.80	FICE	50	1.70	.75

Table C–2 ~~(C)~~. The 54 tetragraphs appearing 50 or more times, arranged in alphabetic order by initial letters, then by absolute frequencies, accompanied by the logarithms of assigned probabilities (U)

	F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)
ASHT	64	1.81	.79	HREE	134	2.13	.91	REQU	98	1.99	.86
AUGH	52	1.72	.76	HIRT	97	1.99	.86	RIOD	63	1.80	.79
				HUND	64	1.81	.79	RTEE	59	1.77	.78
COMM	93	1.97	.85								
CENT	52	1.72	.76	IGHT	140	2.15	.92	STOP	154	2.19	.93
				IVED	62	1.79	.78	SEVE	121	2.08	.89
DASH	132	2.12	.91	IRTY	59	1.77	.78	STAT	54	1.73	.76
DOLL	68	1.83	.80								
DRED	63	1.80	.79	LLAR	71	1.85	.81	TION	218	2.34	.99
				LARS	68	1.83	.80	TEEN	163	2.21	.94
EVEN	168	2.23	.95					TWEN	152	2.18	.93
ENTY	161	2.21	.94	MENT	111	2.05	.88	THRE	149	2.17	.93
EIGH	132	2.12	.91					THIR	104	2.02	.87
ENTH	114	2.06	.89	NINE	153	2.18	.93	THIS	68	1.83	.80
EENT	102	2.01	.87	NDRE	77	1.89	.82				
EQUE	86	1.93	.84	NAUG	56	1.75	.77	UEST	87	1.94	.84
ERIO	66	1.82	.80					UNDR	59	1.77	.78
ENTS	62	1.79	.78	OMMA	71	1.85	.81	UGHT	56	1.75	.77
				OLLA	70	1.85	.81				
FOUR	144	2.16	.92	OURT	56	1.75	.77				
FIVE	135	2.13	.91					VENT	70	1.85	.81
FFIC	62	1.79	.78	PERI	67	1.83	.80				
FROM	59	1.77	.78								
FICE	50	1.70	.75	QUES	87	1.94	.84	WENT	153	2.18	.93

Table C–3 (~~C~~). The 54 tetragraphs appearing 50 or more times, arranged in alphabetic order by their second letters, and then according to their absolute frequencies, accompanied by the logarithms of their assigned probabilities (U)

	F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)
DASH	132	2.12	.91	TION	218	2.34	.99	HREE	134	2.13	.91
LARS	68	1.83	.80	NINE	153	2.18	.93	ERIO	66	1.82	.80
NAUG	56	1.75	.77	FIVE	135	2.13	.91	DRED	63	1.80	.79
				EIGH	132	2.12	.91	FROM	59	1.77	.78
NDRE	77	1.89	.82	HIRT	97	1.99	.86	IRTY	59	1.77	.78
				RIOD	63	1.80	.79				
TEEN	163	2.21	.94	FICE	50	1.70	.75				
WENT	153	2.18	.93					ASHT	64	1.81	.79
SEVE	121	2.08	.89	LLAR	71	1.85	.81				
MENT	111	2.05	.88	OLLA	70	1.85	.81				
EENT	102	2.01	.87					STOP	154	2.19	.93
REQU	98	1.99	.86					RTEE	59	1.77	.78
UEST	87	1.94	.84	OMMA	71	1.85	.81	STAT	54	1.73	.76
VENT	70	1.85	.81								
PERI	67	1.83	.80	ENTY	161	2.21	.94	QUES	87	1.94	.84
CENT	52	1.72	.76	ENTH	114	2.06	.89	HUND	64	1.81	.79
				ENTS	62	1.79	.78	OURT	56	1.75	.77
FFIC	62	1.79	.78	UNDR	59	1.77	.78	AUGH	52	1.72	.76
IGHT	140	2.15	.92	FOUR	144	2.16	.92	EVEN	168	2.23	.95
UGHT	56	1.75	.77	COMM	93	1.97	.85	IVED	62	1.79	.78
				DOLL	68	1.83	.80				
THRE	149	2.17	.93					TWEN	152	2.18	.93
THIR	104	2.02	.87								
THIS	68	1.83	.80	EQUE	86	1.93	.84				

Table C–4 (~~C~~). The 54 tetragraphs appearing 50 or more times, arranged in alphabetic order by their their letters, then by absolute frequencies, accompanied by the logarithms of their assigned probabilities (U)

	F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)
LLAR	71	1.85	.81	EIGH	132	2.12	.91	COMM	93	1.97	.85
STAT	54	1.73	.76	AUGH	52	1.72	.76	OMMA	71	1.85	.81
FICE	50	1.70	.75	IGHT	140	2.15	.92	WENT	153	2.18	.93
				ASHT	64	1.81	.79	NINE	153	2.18	.93
UNDR	59	1.77	.78	UGHT	56	1.75	.77	MENT	111	2.05	.88
								EENT	102	2.01	.87
EVEN	168	2.23	.95					VENT	70	1.85	.81
TEEN	163	2.21	.94	THIR	104	2.02	.87	HUNT	64	1.81	.79
TWEN	152	2.18	.93	THIS	68	1.83	.80	CENT	52	1.72	.76
HREE	134	2.13	.91	ERIO	66	1.82	.80				
QUES	87	1.94	.84	FFIC	62	1.79	.78	TION	218	2.34	.99
DRED	63	1.80	.79					STOP	154	2.19	.93
IVED	62	1.79	.78	OLLA	70	1.85	.81	RIOD	63	1.80	.79
RTEE	59	1.77	.78	DOLL	68	1.83	.80	FROM	59	1.77	.78

Table C–4 (~~C~~). The 54 tetragraphs appearing 50 or more times, arranged in alphabetic order by their third letters, then by absolute frequencies, accompanied by the logarithms of their assigned probabilities (U) – Continued

	F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)
REQU	98	1.99	.86	DASH	132	2.12	.91	FOUR	144	2.16	.92
				UEST	87	1.94	.84	EQUE	86	1.93	.84
THRE	149	2.17	.93					NAUG	56	1.75	.77
HIRT	97	1.99	.86								
NDRE	77	1.89	.82	ENTY	161	2.21	.94				
LARS	68	1.83	.80	ENTH	114	2.06	.89				
PERI	67	1.83	.80	ENTS	62	1.79	.78	FIVE	135	2.13	.91
OURT	56	1.75	.77	IRTY	59	1.77	.78	SEVE	121	2.08	.89

Table C–5 (~~C~~). The 54 tetragraphs appearing 50 or more times, arranged in alphabetic order by their final letters, then by absolute frequencies, accompanied by the logarithms of their assigned probabilities (U)

	F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)		F	L_{10} (F)	L_{244} (F)
OMMA	71	1.85	.81	DASH	132	2.12	.91	QUES	87	1.94	.84
OLLA	70	1.85	.81	EIGH	132	2.12	.91	THIS	68	1.83	.80
				ENTH	114	2.06	.89	LARS	68	1.83	.80
				AUGH	52	1.72	.76	ENTS	62	1.79	.78
FFIC	62	1.79	.78								
				PERI	67	1.83	.80				
								WENT	153	2.18	.93
HUND	64	1.81	.79	DOLL	68	1.83	.80	IGHT	140	2.15	.92
DRED	63	1.80	.79					MENT	111	2.05	.88
RIOD	63	1.80	.79	COMM	93	1.97	.85	EENT	102	2.01	.87
IVED	62	1.79	.78	FROM	59	1.77	.78	HIRT	97	1.99	.86
								UEST	87	1.94	.84
				TION	218	2.34	.99	VENT	70	1.85	.81
NINE	153	2.18	.93	EVEN	168	2.23	.95	ASHT	64	1.81	.79
THRE	149	2.17	.93	TEEN	163	2.21	.94	OURT	56	1.75	.77
FIVE	135	2.13	.91	TWEN	152	2.18	.93	UGHT	56	1.75	.77
HREE	134	2.13	.91					STAT	54	1.73	.76
SEVE	121	2.08	.89	ERIO	66	1.82	.80	CENT	52	1.72	.76
EQUE	86	1.93	.84								
NDRE	77	1.89	.82	STOP	154	2.19	.93				
RTEE	59	1.77	.78					REQU	98	1.99	.86
FICE	50	1.70	.75	FOUR	144	2.16	.92				
				THIR	104	2.02	.87				
				LLAR	71	1.85	.81	ENTY	161	2.21	.94
NAUG	56	1.75	.77	UNDR	59	1.77	.78	IRTY	59	1.77	.78

APPENDIX D (~~C~~)
WORD AND PATTERN LISTS

Table D–1 (~~C~~). List of words used in military text arranged alphabetically according to word length (U)

TWO LETTER WORDS

AM
AN
AS
AT
BE
BN
BY
CO
CP
CQ
DO
EM
GO
HE
HQ
IF
IN
IS
IT
MC
ME
MM
MP
MY
NO
OF
OK
ON
OR
QM
SO
TO
US
WD
WE
WO

THREE LETTER WORDS

ACT
ADD
ADJ
AGE
AGO
AID
AIM
AIR
ALL
AND
ANY
APT
ARC
ARE
ARM
ASK
BAD
BAG
BAR
BID
BIG
BOX
BUT
BUY
CAM
CAN
CAR
CAV
COL
CPL
CUT
CWT
DAY
DID
DIE
DOG
DRY
DUE
DUN
EAT
END
EYE
FAR
FEW
FIT
FIX
FOR
FOX
GAL
GAS
GEN
GET
GHQ
GOT
GUN
HAD
HAM
HAS
HER
HIM
HIS
HOW
ILL
ITS
JIG
JOB
KEG
LAW
LAY
LET
LOT
LOW
MAJ
MAN
MAT
MAY
MEN
MIX
NAN
NET
NEW
NOT
NOW
OFF
OLD
ONE
OUR
OUT
OWE
OWN
PAR
PAY
PEN
PER
PIN
PUT
PVT
QMC
RED
RID
ROB
RUN
SAW
SAY
SEA
SEE
SET
SGT
SHE
SIX
SPY
SUM
SUN
TAN
TAX
TEN
THE
TIN
TON
TOO
TOP
TRY
TUB
TWO
USE
VAT
WAR
WAS
WAY
WET
WGT
WON
YET
YOU

FOUR LETTER WORDS

ABLE
AIDE
ALLY
ALSO
AREA
ARMY
ASIA
AWAY
AXIS
BACK
BASE
BEEN
BLUE
BODY
BOMB
BOOK
BOTH
BULB
BULK
CALL
CELL
CITY
CODE
COOK
DARK
DASH
DATE
DAYS
DIRT
DOWN
DRAW
DUMP
EACH
EAST
EASY
EDGE
EYES
FALL
FARM
FAST
FEEL
FEET
FELL
FILE
FIRE
FIRM
FIVE
FLAG
FLEE
FORM
FOUR
FROM
FULL
FUSE
FUZE
GUNS
HALF
HALT
HAND
HARD
HAVE
HEAD
HERD
HERE
HIGH
HILL
HITS
HOLD
HOOK
INTO
ITEM
JOIN
JULY
JUNE
JUST
KEEP
KIND
KING
LAND
LAST
LATE
LEAD
LEAK
LEFT
LESS
LIEU
LINE
LIST
LOAD
LONG
LOOK
LOSS
LOST
LOVE
MADE
MAIM
MAIN
MANY
MASK
MASS
MEAT
MEET
MESS
MIKE
MILE
MINE
MORE
MOVE
MTCL
MULE
NAVY
NEAR

Table D-1 ~~(C)~~. List of words used in military text arranged alphabetically according to word length (U)--Continued

FOUR LETTER WORDS– Continued

NEXT
NINE
NOON
NOTE
OBOE
OMIT
ONCE
ONLY
OPEN
ORAL
OVER
PARK
PASS
PIPE
PLAN
POST
PUMP
PUSH
RAID
RAIL
RAIN
RANK
REAR
RIOT
ROAD
ROUT
RULE
RUSH
SAID
SAME
SANK
SEEN
SHIP
SHOT
SIDE
SOME
SOON
STOP
SUNK
TAKE
TALK
TANK
TARE
TASK
TEAM
TENT
TEXT
THAN
THAT
THEM
THEN
THEY
THIS
TIME
TONS
TOOK
TOOL
TOWN
TYPE
UNIT
VARY
VERY
WEAK
WEEK
WELL
WERE
WEST
WHAT
WHEN
WILL
WIRE
WITH
XRAY
YOKE
YOUR
ZERO
ZONE

FIVE LETTER WORDS

ABOUT
AFTER
AGAIN
AGENT
ALARM
ALERT
ALIGN
ALINE
ALLOW
ALONG
AMONG
ANNEX
APPLY
APRIL
AREAS
ARMOR
ASSET
AWAIT
AWARD
BAKER
BANKS
BARGE
BEACH
BEGIN
BEING
BLACK
BLIND
BOATS
BOMBS
BOOTH
BREAK
BRIBE
BROKE
BURST
CANAL
CASES
CAUSE
CEASE
CHECK
CHIEF
CLEAR
CLERK
CLOSE
COAST
COLON
COMMA
CORPS
COUNT
COVER
CREEK
CREST
CROSS
CURVE
DAILY
DECKS
DEFER
DELAY
DEPOT
DEPTH
DOCKS
DRAWN
DRESS
DRILL
DRIVE
EAGER
EARLY
EIGHT
ENEMY
ENTER
EQUAL
EQUIP
ERASE
ERROR
EITHER
EVERY
FATAL
FEARS
FERRY
FIELD
FIFTH
FIFTY
FLIGHT
FIRES
FIRST
FLANK
FLARE
FLATS
FLEET
FOGGY
FORCE
FORTY
FRESH
FRONT
GATES
GAUGE
GIVEN
GOING
GROUP
GUARD
GUEST
HEAVY
HONOR
HORSE
HOURS
HOUSE
ISSUE
JAPAN
LARGE
LATER
LEAST
LEAVE
LEVEL
LIGHT
LIMIT
LOCAL
MAJOR
MARCH
METER
MILES
MOTOR
NAVAL
NIGHT
NINTH
NORTH
ORDER
OTHER
PACKS
PAIRS
PARTY
PETER
PLACE
PLAIN
PLANS
POINT
PRESS
PRIOR
PROOF
PROVE
QUEEN
QUICK
QUIET
RADIO
RAFTS
RAIDS
RALLY
RANGE
RAPID
REACH
READY
REFER
REPEL
RIDGE
RIGHT
RIGID
RIVER
ROGER
ROUTE
SCALE
SEIZE
SEVEN
SHELL
SHIFT
SHIPS
SHORE
SIEGE
SIGHT
SIXTH
SIXTY
SLOPE
SMALL
SMOKE
SOUTH
SPEED
SPELL
SPLIT
SQUAD
STAFF
STAKE
START
STEEL
SUGAR
TAKEN
TANKS
TENTH
THEIR
THERE
THESE
THIRD
THREE
TITLE
TODAY
TOTAL
TRACT
TRAIN
TROOP
TRUCE
TRUCK
UNDER
UNION
UNITS
USUAL
VALOR
VISIT
VITAL
VOCAL
VOICE
WAGON
WEIGH
WHEEL
WHERE
WHICH
WIDTH
WIPED
WOODS
YARDS
ZEBRA

Table D-1 (~~C~~). List of words used in military text arranged alphabetically according to word length (U)--Continued

SIX LETTER WORDS

ACCEPT
ACCESS
ACROSS
ACTION
ACTIVE
ADJUST
ADVICE
ADVISE
AFFAIR
ALASKA
ALLEGE
ALLIED
ALLIES
ALWAYS
ANIMAL
ANNUAL
ANYWAY
APPEAR
ARABIA
ARMIES
ARMORY
ARREST
ARRIVE
ASSETS
ASSIST
ASSURE
ATTACH
ATTACK
ATTAIN
AUGUST
BANNER
BARBED
BARGES
BATTEN
BATTLE
BEETLE
BEFORE
BETTER
BEYOND
BILLET
BITTER
BODIES
BOMBED
BOMBER
BOTTOM
BRANCH
BREACH
BREEZE
BRIDGE
BROKEN
BUREAU
CANADA
CANCEL
CANNOT
CANVAS
CASUAL
CAUSED
CENTER
CHANGE
CHARGE
CHEESE
CHURCH
CIPHER
CIRCLE
COFFEE
COLORS
COLUMN
COMBAT
COMMIT
COMMON
CONVEY
CONVOY
COURSE
CREDIT
CRISIS
CRITIC
DAMAGE
DEBARK
DECIDE
DECODE
DECREE
DEFEAT
DEFECT
DEFEND
DEGREE
DEPART
DEPEND
DEPLOY
DESERT
DETACH
DETAIL
DEVICE
DEVISE
DIRECT
DIVERT
DIVIDE
DOCTOR
DOLLAR
DOWNED
DRYRUN
DUGOUT
DURING
EFFECT
EFFORT
EIGHTH
EIGHTY
EITHER
ELEVEN
EMBARK
EMPLOY
ENCODE
ENGAGE
ENGINE
ENROLL
ENTIRE
ERASER
ESCORT
EUROPE
EXCEPT
EXCESS
EXCITE
EXPECT
EXPELS
EXPEND
EXTEND
EXTENT
FIERCE
FILING
FINISH
FIRING
FLIGHT
FLYING
FOLLOW
FORCES
FORMAL
FORMED
FOUGHT
FOURTH
FRIDAY
FUTURE
GARAGE
GEORGE
GREASE
GROUND
GUNNER
HALTED
HAMMER
HAPPEN
HARBOR
HELPER
HIGHER
HOURLY
INDEED
INFORM
INLAND
INTEND
INTENT
INVENT
ISLAND
ISSUES
KEEPER
KILLED
LADDER
LANDED
LAUNCH
LEADER
LEAGUE
LESSON
LETTER
LINING
LIQUID
LITTER
LITTLE
LOCATE
LOSSES
MANAGE
MANNER
MANUAL
MEAGER
MEDIUM
MEMBER
METHOD
METRIC
MINING
MINUTE
MIRROR
MOBILE
MONDAY
MORALE
MORTAR
MOVING
MURDER
MUZZLE
NAUGHT
NEARER
NINETY
NORMAL
NOTING
NOUGHT
NOVICE
NOZZLE
NUMBER
OCCUPY
OFFEND
OFFICE
OPPOSE
ORDERS
ORIENT
OTHERS
OUTPUT
PANAMA
PARADE
PARLEY
PASSED
PASSES
PATROL
PERIOD
PICKET
PINCER
PISTOL
PLACES
PLANES
POINTS
POISON
POLICE
PONTON
POSTAL
PREFER
PROMPT
PROPER
PURSUE
RADIAL
RAIDED
RATION
RAVINE
RECORD
REDUCE
REFILL
REFUGE
REFUSE
REJECT
RELIEF
REMAIN
REMEDY
REPAIR
REPORT
RESCUE
RESIST
RESULT
RESUME
RETIRE
RETURN
REVIEW
RIDING
ROCKET
ROUTED
ROUTES
RUBBER
RUNNER
SALARY
SCHEME
SCHOOL
SCORED
SCREEN
SEAMAN
SEAMEN
SEARCH
SECOND
SECTOR
SECURE
SELECT
SERIAL
SETTLE
SEVERE
SHELLS
SIGCOM
SIGNAL
SINGLE
SLIGHT
SPHERE
SPOOLS
SPOONS
STATES
STATUS
STRAFE
STREET
STRESS
STRIPS
SUBMIT
SUDDEN
SUFFER
SUMMER
SUMMIT
SUMMON
SUNDAY
SUNKEN
SUNSET
SUPPLY
SURVEY
SWITCH
SYSTEM
TABLES
TANKER
TARGET
TATTOO
TERROR
THIRTY
THOUGH
THREAT
TRAINS
TRENCH
TROOPS
TURRET
TWELVE
TWENTY
UNABLE
UNITED
UNLESS
VALLEY
VERBAL
VERIFY
VESSEL
VICTIM
VICTOR
VISITS
VISUAL
WEIGHT
WIRING
WITHIN
WOODED
ZIGZAG

SEVEN LETTER WORDS

ABANDON
ABSENCE
ADDRESS
ADVANCE
AGAINST
ALMANAC
AMMETER
ANALYZE
ANOTHER
ANTENNA
APPOINT
APPROVE
ARMORED
ARRANGE
ARRIVAL
ASIATIC
ASSAULT
ATTACKS
ATTEMPT
AVERAGE
AVIATOR
AWKWARD
BAGGAGE
BALLOON
BARRAGE
BATTERY
BATTLES
BEARING
BECAUSE
BEDDING
BETWEEN
BICYCLE
BINDING
BIVOUAC
BOMBARD

Table D-1 (~~C~~). List of words used in military text arranged alphabetically according to word length (U)--Continued

SEVEN LETTER WORDS–Continued

BOMBERS
BOMBING
BOYCOTT
BRIBERY
BRIGADE
CALIBER
CALIBRE
CAPTAIN
CAPTIVE
CARRIER
CAVALRY
CENTRAL
CHANGES
CHANNEL
CHARLIE
CHASSIS
CIRCUIT
CLIPPER
COASTAL
COLLECT
COLLEGE
COLONEL
COMMAND
COMMEND
COMMENT
COMMUTE
COMPANY
COMPASS
CONCEAL
CONDEMN
CONDUCT
CONFINE
CONTACT
CONTAIN
CONTROL
CORRECT
COUNCIL
COURIER
COVERED
CROSSED
CRUISER
CURRENT
CYCLONE
DAMAGED
DEBOUCH
DECIDED
DECLARE
DECODED
DEFENSE
DELAYED
DELIVER
DERRICK
DESTROY
DETRAIN
DETRUCK
DEVELOP
DIAGRAM
DISCUSS
DISEASE
DISMISS
DISTILL
DROPPED
EASTERN
ECHELON
ELEMENT
ELEVATE
EMBASSY
ENCODED
ENEMIES
ENFORCE
ENGAGED
ENTENTE
ENTRAIN
ENTRUCK
ENVELOP
EVENING
EXCLUDE
EXPLAIN
EXPRESS
EXTRACT
EXTREME
FALLING
FARTHER
FEDERAL
FIFTEEN
FIGHTER
FILLING
FINDING
FISHING
FITTING
FOGHORN
FORCING
FORGING
FORWARD
FOXHOLE
FUELOIL
FURNISH
FURTHER
GASSING
GENERAL
GETTING
GLASSES
GRADUAL
GRENADE
GUARDED
HALTING
HASBEEN
HEADING
HEAVIER
HIGHEST
HOLDING
HORIZON
HOSTILE
HUNDRED
ICEBERG
ILLEGAL
ILLNESS
INCLUDE
INFLICT
INITIAL
INQUIRE
INQUIRY
INSPIRE
INSTALL
INSTANT
INVADED
ISLANDS
ISSUING
JANUARY
JUMPOFF
KITCHEN
KILLING
LANDING
LEADING
LECTURE
LIAISON
LIBRARY
LICENSE
LIFTING
LOADING
LOGICAL
LOOKOUT
MACHINE
MANDATE
MANNING
MAPPING
MARCHED
MARSHAL
MARTIAL
MAXIMUM
MEDICAL
MESSAGE
MESSING
MILITIA
MINIMUM
MISFIRE
MISSING
MISSION
MORNING
NATURAL
NEAREST
NIGHTLY
NOTHING
NUMBERS
OBSERVE
OCTOBER
OFFENSE
OFFICER
OMITTED
OPERATE
OPINION
ORDERED
OUTPOST
OUTSIDE
PACIFIC
PACKAGE
PASSAGE
PASSIVE
PATROLS
PAYROLL
PLACING
PLATOON
POUNDER
PRAIRIE
PRECEDE
PREPARE
PRESENT
PRESSED
PRIMARY
PROCEED
PROGRAM
PROMOTE
PROPOSE
PROTECT
PROTEST
PROVOST
PURPOSE
PURSUIT
PUSHING
QUARTER
QUICKLY
RADIATE
RAIDING
RAILWAY
RAINING
RAPIDLY
REACHED
RECEIPT
RECEIVE
RECOVER
RECRUIT
REDUCED
REFUGEE
REGULAR
RELEASE
RELIEVE
REPAIRS
REPLACE
REQUEST
REQUIRE
RESERVE
RESPECT
RESPOND
RETIRED
RETREAT
REVENUE
REVERSE
REVOLVE
ROUTINE
RUNNING
SAILORS
SATISFY
SECRECY
SECTION
SECTORS
SERVICE
SESSION
SETBACK
SEVENTH
SEVENTY
SEVERAL
SHELLED
SHORTLY
SIGNIFY
SIMILAR
SIMPLEX
SINKING
SIXTEEN
SLOPING
SMOKING
SOLDIER
STARTER
STATION
STEAMER
STOPPED
STORAGE
SUCCESS
SUGGEST
SUMMARY
SUNRISE
SUPPORT
SUPPOSE
SURPLUS
SUSPEND
TACTICS
TALKING
TARGETS
TERRAIN
THATTHE
THROUGH
TOBACCO
TONIGHT
TONNAGE
TORPEDO
TRACTOR
TRAFFIC
TRAWLER
TRIGGER
TUESDAY
TWELFTH
UNKNOWN
UNUSUAL
USELESS
UTILITY
VACANCY
VARYING
VESSELS
VICTORY
VILLAGE
VISIBLE
VISITOR
WARFARE
WARSHIP
WEATHER
WESTERN
WHETHER
WILLIAM
WINDAGE
WITHOUT
WITHTHE
WITNESS
WOUNDED
WRECKED
WRITTEN

EIGHT LETTER WORDS

ACTIVITY
ACTUALLY
ADJACENT
ADJUTANT
ADVANCED
ADVANCES
ADVISING
ADVISORY
AIRBORNE
AIRCRAFT
AIRDROME
AIRFIELD
AIRPLANE
ALTITUDE
AMERICAN
ANALYSIS
ANNOUNCE
ANTITANK
APPARENT
APPEARED
APPROACH
APPROVAL
ARMAMENT
ARRESTED
ASSEMBLE
ASSEMBLY
ASSIGNED
ASSOONAS

Table D-1 ~~(C)~~. List of words used in military text arranged alphabetically according to word length (U)--Continued

EIGHT LETTER WORDS--Continued

ATLANTIC
ATTACKED
ATTEMPTS
AVIATION
BARRACKS
BARRAGES
BATTERED
BATTLING
BESIEGED
BILLETED
BOUNDARY
BREAKING
BUILDING
BULLETIN
BUSINESS
CALAMITY
CAMPAIGN
CANISTER
CAPACITY
CAPTURED
CARELESS
CARRIAGE
CARRIERS
CARRYING
CASUALTY
CAUSEWAY
CEMETERY
CENTERED
CHAPLAIN
CHEMICAL
CIRCULAR
CITATION
CIVILIAN
CLERICAL
CODEBOOK
COMMANDS
COMMENCE
COMMERCE
COMPLETE
COMPOSED
CONCLUDE
CONCRETE
CONFLICT
CONGRESS
CONTINUE
CONTRACT
CORPORAL
CORRIDOR
COVERING
CRITICAL

CRITIQUE
CROSSING
CRUISERS
DAMAGING
DARKNESS
DAYLIGHT
DECEMBER
DECIPHER
DECISION
DECISIVE
DECLARED
DECREASE
DEDICATE
DEFEATED
DEFENDED
DEFENDER
DEFENSES
DEFERRED
DEFINITE
DELAYING
DEMANDED
DEPARTED
DEPLOYED
DEPORTED
DESCRIBE
DESERTED
DESERTER
DESPATCH
DETACHED
DETECTOR
DETONATE
DEVELOPE
DICTATED
DICTATOR
DIMINISH
DIRECTOR
DISARMED
DISASTER
DISLODGE
DISPATCH
DISPERSE
DISTANCE
DISTRESS
DISTRICT
DIVIDING
DIVISION
DOCTRINE
DOMINANT
DRESSING

DRIFTING
EASTERLY
EASTWARD
ECONOMIC
EFFECTED
EFFICACY
EIGHTEEN
ELEMENTS
ELEVENTH
ELIGIBLE
EMPLOYEE
EMPLOYER
ENCIPHER
ENCIRCLE
ENFILADE
ENGAGING
ENGINEER
ENLISTED
ENORMOUS
ENROLLED
ENTERING
ENTRENCH
ENVELOPE
EQUALIZE
EQUIPAGE
ESCORTED
ESTIMATE
EUROPEAN
EVACUATE
EXCAVATE
EXCHANGE
EXERCISE
EXPANDED
EXPEDITE
EXPELLED
EXPENDED
EXPENSES
EXTENDED
EXTERIOR
FACTIONS
FATALITY
FEBRUARY
FERRYING
FIGHTERS
FIGHTING
FINISHED
FLANKING
FLEXIBLE
FOOTHOLD

FORENOON
FORTRESS
FOURTEEN
FRONTAGE
FUSELAGE
GARRISON
GROUNDED
GROUPING
GUARDING
HAVEBEEN
HINDERED
HOSPITAL
HOWITZER
IDENTIFY
IGNITION
IMPROPER
IMPROVED
INCIDENT
INDICATE
INDIRECT
INFANTRY
INFECTED
INITIATE
INSECURE
INSIGNIA
INSTRUCT
INTEREST
INTERIOR
INTERNAL
INTRENCH
INVADING
INVASION
INVENTED
JETPLANE
JUNCTION
LANGUAGE
LATITUDE
LETTERED
LIMITING
LOCATION
LUMINOUS
MAINTAIN
MANDATED
MANEUVER
MARCHING
MARITIME
MATERIAL
MATERIEL
MECHANIC

MEDICINE
MEMORIAL
MERCIFUL
MESSAGES
MIDNIGHT
MILITARY
MISFIRES
MISSIONS
MOBILIZE
MONOPOLY
MOUNTAIN
MOVEMENT
NATIONAL
NAUTICAL
NINETEEN
NORTHERN
NOVEMBER
OBSERVED
OBSERVER
OBSOLETE
OBSTACLE
OCCUPIED
OFFENDED
OFFICERS
OFFICIAL
OPERATOR
OPPOSING
OPPOSITE
ORDINATE
ORDNANCE
OUTBOARD
OUTGUARD
OUTPOSTS
PAINTING
PARALLAX
PARALLEL
PASSPORT
PLANNING
POLITICS
PONTOONS
POSITION
POSITIVE
POSSIBLE
POSTPONE
PREPARED
PRESERVE
PRESSING
PRESSURE
PRINTING

PRIORITY
PRISONER
PROBABLE
PROBABLY
PROGRESS
PROHIBIT
PROTESTS
PROTOCOL
PURPOSES
QUARTERS
RAILHEAD
RAILROAD
RALLYING
RECEIVER
RECORDER
REDCROSS
REENLIST
REGIMENT
REGISTER
REJECTED
REJECTOR
REMEDIES
REMEMBER
REPAIRED
REPEATER
REPELLED
REPLACED
REPORTED
REPULSED
REQUIRED
RESEARCH
RESERVES
RESPECTS
RESTORED
RETIRING
RETURNED
REVIEWED
REVOLVER
RIGOROUS
SABOTAGE
SANITARY
SATURDAY
SCHEDULE
SEABORNE
SEALEVEL
SELECTED
SENTENCE
SENTINEL
SEPARATE

SERGEANT
SHELLING
SHIPPING
SIGHTING
SKIRMISH
SOLDIERS
SOUTHERN
SPECIFIC
SPOTTING
SQUADRON
STANDARD
STATIONS
STRATEGY
SUFFERED
SUITABLE
SUPERIOR
SUPPLIES
SURPRISE
SURROUND
SURVIVED
SUSPENSE
SWEEPING
SWIMMING
TACTICAL
TAXATION
TELEGRAM
TERRIBLE
TERRIFIC
THATHAVE
THIRTEEN
THOUSAND
THURSDAY
TOMORROW
TOTALING
TRAILERS
TRAINING
TRANSFER
TRAVERSE
TRAWLERS
VEHICLES
VICINITY
VIGOROUS
WARSHIPS
WESTERLY
WESTWARD
WINDWARD
WIRELESS
WITHDRAW
WITHDREW

Table D-1 (~~C~~). List of words used in military text arranged alphabetically according to word length (U)--Continued

NINE LETTER WORDS

ACCESSORY
ACCOMPANY
ACCORDING
ADDRESSED
ADDRESSES
ADMISSION
ADVANCING
ADVANTAGE
AERODROME
AEROPLANE
AFTERNOON
AGREEMENT
AIRDROMES
AIRPLANES
ALLOTMENT
ALLOWANCE
ALTERNATE
AMBULANCE
AMUSEMENT
ANNOUNCED
ANONYMOUS
APPARATUS
APPOINTED
ARBITRARY
ARTILLERY
ASCENSION
ASSAULTED
ASSISTANT
ASSOCIATE
ASSURANCE
ATTACKING
ATTEMPTED
ATTENTION
AUTOMATIC
AVAILABLE
BALLISTIC
BAROMETER
BATTALION
BATTERIES
BEACHHEAD
BEGINNING
BLOCKADED
BOMBARDED
BRIGADIER
BUILDINGS
CABLEGRAM
CAMPAIGNS
CANCELLED
CARTRIDGE

CENTERING
CHALLENGE
CHARACTER
CHAUFFEUR
CHRONICAL
CIGARETTE
CIRCULATE
CIVILIANS
CLEARANCE
COALITION
COLLAPSED
COLLISION
COMBATANT
COMMANDED
COMMANDER
COMMITTEE
COMPANIES
COMPELLED
COMPLETED
CONDEMNED
CONDENSED
CONDITION
CONFERRED
CONFIDENT
CONFLICTS
CONQUERED
CONTINUAL
CONTINUED
CONTINUES
COOPERATE
CORRECTED
CRITICISE
CRITICISM
DEBARKING
DECREASED
DEFECTIVE
DEFENSIVE
DEFICIENT
DEPARTURE
DEPENDENT
DESCRIBED
DESIGNATE
DESTITUTE
DESTROYED
DESTROYER
DETENTION
DETERMINE
DETONATED
DETRAINED

DEVELOPED
DIETITIAN
DIFFERENT
DIFFICULT
DIMENSION
DIRECTION
DIRIGIBLE
DISAPPEAR
DISCUSSED
DISINFECT
DISMISSAL
DISPERSED
DISTRICTS
DIVISIONS
DOMINANCE
DOMINATED
ECHELONED
EFFECTIVE
EFFICIENT
ELABORATE
ELEVATION
ELSEWHERE
EMBASSIES
EMERGENCY
EMPLOYING
ENDURANCE
ENGINEERS
ENLISTING
ENTRAINED
EQUIPMENT
ESTABLISH
ESTIMATED
ESTIMATES
EXCESSIVE
EXCLUSION
EXCLUSIVE
EXECUTIVE
EXERCISES
EXHIBITED
EXPANSION
EXPANSIVE
EXPENSIVE
EXPLOSION
EXPLOSIVE
EXTENDING
EXTENSION
EXTENSIVE
FIFTEENTH
FIREALARM

FORMATION
FORTIFIED
FRONTLINE
GROUPMENT
GYROMETER
HOSTILITY
HURRICANE
IDENTICAL
IMMEDIATE
IMPORTANT
IMPRESSED
INCENTIVE
INCIDENCE
INCIDENTS
INCLINING
INCLUDING
INCLUSIVE
INCREASED
INDEMNITY
INDICATED
INFLATION
INFLICTED
INFLUENCE
INHABITED
INSTANTLY
INTEGRITY
INTENSIVE
INTENTION
INTERCEPT
INTERDICT
INTERFERE
INTERMENT
INTERPOSE
INTERRUPT
INTERVENE
INTERVIEW
INVENTION
IRREGULAR
KILOMETER
LAUNCHING
LIABILITY
LOGISTICS
LONGITUDE
MAINTAINS
MANGANESE
MECHANISM
MEMORANDA
MESSENGER
MOTORIZED

MOVEMENTS
MUNITIONS
NAVALBASE
NECESSARY
NECESSITY
NEGLIGENT
NEWSPAPER
NORTHEAST
NORTHERLY
NORTHWARD
NORTHWEST
NUMBERING
OBJECTION
OBJECTIVE
OBTAINING
OCCUPYING
OFFENSIVE
OFFICIALS
OPERATING
OPERATION
OSCILLATE
OUTSKIRTS
PARACHUTE
PARAGRAPH
PARTITION
PASSENGER
PATRIOTIC
PENETRATE
PERMANENT
PERSONNEL
PLACEMENT
POLITICAL
POPULATED
POSITIONS
PRACTICAL
PRECEDING
PREFERRED
PREMATURE
PREPARING
PRESIDENT
PRINCIPAL
PRINCIPLE
PRISONERS
PROCEDURE
PROCEEDED
PROJECTOR
PROMOTION
PROPOSALS
PROTECTED

PROTECTOR
PROTESTED
PROVISION
PROXIMITY
RADIATION
RADIOGRAM
READINESS
REARGUARD
REBELLION
RECEIVING
RECOGNIZE
RECOMMEND
REENFORCE
REFERENCE
REFILLING
REGARDING
REINFORCE
REINSTATE
REMAINDER
REMAINING
REPRESENT
REPRISALS
REQUESTED
REQUIRING
RESOURCES
RESTRAINT
RETENTION
RETURNING
REVIEWING
SCREENING
SEAPLANES
SECRETARY
SEMICOLON
SEMIRIGID
SEPTEMBER
SERIOUSLY
SERVICING
SEVENTEEN
SHELLFIRE
SITUATION
SIXTEENTH
SOUTHEAST
SOUTHWARD
SOUTHWEST
SPEARHEAD
STANDARDS
STATEMENT
STRAGGLER
STRATEGIC

Table D-1 (~~C~~). List of words used in military text arranged alphabetically according to word length (U)--Continued

NINE LETTER WORDS– Continued

SUBMITTED
SUCCEEDED
SURRENDER
SUSPECTED
SUSPENDED
SUSPICION
TECHNICAL
TECHNIQUE
TELEPHONE
TENTATIVE
TERRITORY
THEREFORE
TRANSPORT
TWENTIETH
UNTENABLE
VARIATION
WATERTANK
WEDNESDAY
WITNESSES
YESTERDAY

TEN LETTER WORDS

ACCEPTABLE
ACCEPTANCE
ACCIDENTAL
ACCORDANCE
ACTIVITIES
ADDITIONAL
AIRCONTROL
AIRSUPPORT
ALLEGIANCE
ALLOCATION
AMBASSADOR
AMMUNITION
ANTEDATING
ANTICIPATE
APPARENTLY
APPEARANCE
APPROACHED
ARMOREDCAR
ARTIFICIAL
ASPOSSIBLE
ASSEMBLIES
ASSESSMENT
ASSIGNMENT
ASSISTANCE
ATOMICBOMB
ATTACHMENT
ATTAINMENT
ATTEMPTING
AUDIBILITY
AUTOMOBILE
BALLISTICS
BATTLESHIP
BEENNEEDED
BRIDGEHEAD
CAMOUFLAGE
CAPABILITY
CASUALTIES
CENSORSHIP
CENTRALIZE
CIRCUITOUS
COASTGUARD
COLLECTING
COLLECTION
COLLISIONS
COMMANDANT
COMMANDEER
COMMANDING
COMMISSARY
COMMISSION
COMMITMENT
COMMUNIQUE
COMPENSATE
COMPLETELY
COMPRESSED
CONCERNING
CONCESSION
CONCLUSION
CONDITIONS
CONFERENCE
CONFESSION
CONFIDENCE
CONNECTING
CONNECTION
CONSPIRACY
CONSTITUTE
CONTINGENT
CONTINUOUS
CONTRABAND
CONVENIENT
COORDINATE
CORRECTION
CREDENTIAL
CROSSROADS
DEBOUCHING
DECIPHERED
DECORATION
DEDICATION
DEFICIENCY
DEFINITION
DEMOBILIZE
DEPARTMENT
DEPENDABLE
DEPLOYMENT
DEPRESSION
DESIGNATED
DESPATCHED
DESPTACHES
DESTROYERS
DETACHMENT
DETERMINED
DETONATION
DETRAINING
DETRUCKING
DIFFERENCE
DIPLOMATIC
DIRECTIONS
DISCIPLINE
DISCUSSION
DISPATCHED
DISPATCHER
DISPATCHES
DISPERSION
DISTRESSED
DISTRIBUTE
DIVEBOMBER
DOMINATION
EFFICIENCY
EIGHTEENTH
ELEMENTARY
EMPLOYMENT
ENCIPHERED
ENCIRCLING
ENEMYTANKS
ENGAGEMENT
ENLISTMENT
ENROLLMENT
ENTERPRISE
ENTRENCHED
ENTRUCKING
EQUIVALENT
ESTIMATION
EVACUATING
EVACUATION
EVALUATION
EXCAVATION
EXCITEMENT
EXHIBITION
EXPEDITING
EXPEDITION
EXPENDABLE
EXPERIENCE
EXPERIMENT
EXPLOSIONS
EXTINGUISH
FACILITIES
FLASHLIGHT
FORMATIONS
FOUNDATION
FOURTEENTH
FRONTLINES
GEOGRAPHIC
GONIOMETER
GOVERNMENT
GYROSCOPIC
HYDROMETER
HYGROMETER
ILLITERATE
ILLUMINATE
ILLUSTRATE
IMPASSABLE
IMPOSSIBLE
IMPRESSION
IMPRESSIVE
INCENDIARY
INDICATING
INDICATION
INDIVIDUAL
INFLICTING
INSECURITY
INSPECTION
INSTRUCTED
INSTRUCTOR
INSTRUMENT
INTERNMENT
INVITATION
IRRIGATION
KILOMETERS
LABORATORY
LIEUTENANT
LIMITATION
LOCOMOTIVE
MACHINEGUN
MAINTAINED
MANAGEMENT
MECHANIZED
MEMORANDUM
MILLIMETER
MOTORCYCLE
NATURALIZE
NAVIGATION
NEGLIGENCE
NEWSPAPERS
NINETEENTH
OBJECTIVES
OCCUPATION
ONEHUNDRED
OPERATIONS
OPPOSITION
OVERCOMING
PATROLLING
PERMISSION
PERSISTENT
PHOSPHORUS
POPULATION
POSSESSION
POSTOFFICE
PRECEDENCE
PREFERENCE
PRESCRIBED
PROHIBITED
PROPORTION
PROTECTION
PROVISIONS
QUARANTINE
RECEPTACLE
RECREATION
RECRUITING
REENFORCED
REENLISTED
REGIMENTAL
REGULATION
REINFORCED
RESISTANCE
RESPECTFUL
RESTRICTED

Table D-1 (~~C~~). List of words used in military text arranged alphabetically according to word length (U)--Continued

TEN LETTER WORDS– Continued

REVOLUTION
SANITATION
SEPARATION
SIGNALLING
SIMILARITY
STATISTICS
SUBMARINES

SUBMISSION
SUBSTITUTE
SUCCESSFUL
SUCCESSIVE
SUFFICIENT
SUPPORTING

SUSPENSION
SUSPICIONS
SUSPICIOUS
THIRTEENTH
THREATENED
TRAJECTORY

TRANSPORTS
TRANSVERSE
TROOPSHIPS
TWENTYFIVE
UNDERSTAND
UNDERSTOOD

UNEXPENDED
UNSUITABLE
VICTORIOUS
VISIBILITY
WILLATTACK
WITHDRAWAL

ELEVEN LETTER WORDS

ACCESSORIES
AERONAUTICS
ACKNOWLEDGE
ALTERNATING
APPLICATION
APPOINTMENT
APPROACHING
APPROPRIATE
APPROXIMATE
ARBITRATION
ARMOREDCARS
ARRANGEMENT
ASSESSMENTS
ASSIGNMENTS
ASSOCIATION
BATTLEFIELD
BATTLESHIPS
BELLIGERENT
BLOCKBUSTER
BOMBARDMENT
CATASTROPHE
CERTIFICATE
CIRCULATION
COEFFICIENT
COINCIDENCE
COMMUNICATE
COMMUNIQUES
COMPARTMENT
COMPETITION
COMPOSITION
COMPUTATION

CONCEALMENT
CONCENTRATE
CONFINEMENT
CONSTITUTED
CONSUMPTION
CONTINENTAL
CONTROVERSY
COOPERATION
CORPORATION
CORRECTNESS
CREDENTIALS
CUSTOMHOUSE
DEBARKATION
DEMONSTRATE
DESCRIPTION
DESCRIPTIVE
DESIGNATION
DESTRUCTION
DETERIORATE
DEVELOPMENT
DISAPPEARED
DISCONTINUE
DISCREPANCY
DISINFECTED
DISPOSITION
DISTINCTION
DISTINGUISH
DYNAMOMETER
ECHELONMENT
EFFECTIVELY
ELECTRICITY

EMBARKATION
EMPLACEMENT
ENCOUNTERED
ENEMYPLANES
ENFORCEMENT
ENGAGEMENTS
ENGINEERING
ESTABLISHED
ESTIMATEDAT
EXAMINATION
EXPLANATION
EXTENSIVELY
EXTERMINATE
FINGERPRINT
FIRECONTROL
HEAVYBOMBER
HEAVYLOSSES
HOSTILITIES
IMMEDIATELY
IMMIGRATION
IMPEDIMENTA
IMPROVEMENT
INCOMPETENT
INDEPENDENT
INFLAMMABLE
INFORMATION
INSPIRATION
INSTITUTION
INSTRUCTION
INSTRUMENTS
INTELLIGENT

INTERCEPTED
INTERESTING
INTERFERING
INTERPRETER
INTERRUPTED
INTERVENING
INVESTIGATE
LEGISLATION
LIGHTBOMBER
MAINTENANCE
MANUFACTURE
MEASUREMENT
NATIONALISM
NATIONALITY
NAVALATTACK
NAVALBATTLE
NAVALFORCES
NECESSITATE
OBSERVATION
OVERWHELMED
PARENTHESES
PARENTHESIS
PENETRATION
PERFORMANCE
PHILIPPINES
PHOTOGRAPHY
PREARRANGED
PREPARATION
PRELIMINARY
PROGRESSIVE
RANGEFINDER

REAPPOINTED
RECOGNITION
RECOMMENDED
RECONNOITER
REPLACEMENT
REQUIREMENT
REQUISITION
RESERVATION
RESIGNATION
RESPONSIBLE
RESTRICTION
RETALIATION
RETROACTIVE
SCHOOLHOUSE
SEVENTEENTH
SEVENTYFIVE
SIGNIFICANT
SMOKESCREEN
STRATEGICAL
SUBSISTENCE
SUITABILITY
SUPERIORITY
SURRENDERED
SYNCHRONIZE
TEMPERATURE
THERMOMETER
TOPOGRAPHIC
TRADITIONAL
TRANSFERRED
WITHDRAWING

TWELVE LETTER WORDS

ADVANTAGEOUS
AGRICULTURAL
ANNOUNCEMENT
ANTIAIRCRAFT
ANTICIPATION
BREAKTHROUGH
CANCELLATION

CARELESSNESS
COMMENCEMENT
COMMENDATION
COMMISSIONED
COMMISSIONER
COMPENSATION
COMPLETENESS

CONCENTRATED
CONCILIATION
CONFIDENTIAL
CONFIRMATION
CONFISCATION
CONFORMATION
CONSCRIPTION

CONSIDERABLE
CONSTITUTING
CONSTITUTION
CONSTRUCTION
CONTINUATION
CONVALESCENT
CONVERSATION

COORDINATION
DECENTRALIZE
DECIPHERMENT
DEMONSTRATED
DEPARTMENTAL
DIFFICULTIES
DISORGANIZED

Table D-1 (~~C~~). List of words used in military text arranged alphabetically according to word length (U)--Continued

TWELVE LETTER WORDS—Continued

- DISPLACEMENT
- DISSEMINATED
- DISTRIBUTING
- DISTRIBUTION
- EMPLACEMENTS
- ENCIPHERMENT
- ENTANGLEMENT
- ENTERPRISING
- FIGHTERPLANE
- GENERALALARM
- GENERALSTAFF
- GEOGRAPHICAL
- HEADQUARTERS
- HEAVYBOMBERS
- HYDROGRAPHIC
- ILLUMINATING
- ILLUMINATION
- ILLUSTRATION
- INAUGURATION
- INCOMPETENCE
- INEFFICIENCY
- INSTRUCTIONS
- INTELLIGENCE
- INTERCEPTION
- INTERDICTION
- INTERFERENCE
- INTERMEDIATE
- INTERRUPTION
- INTERVENTION
- INTRODUCTION
- INTRODUCTORY
- IRREGULARITY
- LIGHTBOMBERS
- MARKSMANSHIP
- MEASUREMENTS
- MEDIUMBOMBER
- MOBILIZATION
- NONCOMBATANT
- NORTHWESTERN
- OBSTRUCTIONS
- ORGANIZATION
- PREPARATIONS
- PREPAREDNESS
- PRESERVATION
- PRESIDENTIAL
- PROCLAMATION
- PSYCHROMETER
- RADIOSTATION
- RECREATIONAL
- REENLISTMENT
- REGISTRATION
- REPLACEMENTS
- RESPECTFULLY
- ROADJUNCTION
- SATISFACTORY
- SEARCHLIGHTS
- SHARPSHOOTER
- SIGNIFICANCE
- SIMULTANEOUS
- SOUTHWESTERN
- SUBSTITUTION
- SUCCESSFULLY
- TRANSFERRING
- TRANSMISSION
- TRANSPACIFIC
- UNIDENTIFIED
- UNITEDSTATES
- UNSUCCESSFUL
- VERIFICATION
- VETERINARIAN

THIRTEEN LETTER WORDS

- ACCOMMODATION
- APPROXIMATELY
- CHRONOLOGICAL
- CIRCUMSTANCES
- COMMUNICATION
- CONCENTRATING
- CONCENTRATION
- CONGRESSIONAL
- CONSIDERATION
- CORRESPONDING
- COUNTERATTACK
- DECENTRALIZED
- DEMONSTRATION
- DEPENDABILITY
- DETERMINATION
- DISAPPEARANCE
- DISCREPANCIES
- DISSEMINATION
- DISTINGUISHED
- ENTERTAINMENT
- ESTABLISHMENT
- EXTERMINATION
- EXTRAORDINARY
- FIGHTERPLANES
- IMPRACTICABLE
- INDETERMINATE
- INSTALLATIONS
- INSTANTANEOUS
- INTERNATIONAL
- INVESTIGATION
- MEDIUMBOMBERS
- MISCELLANEOUS
- PRELIMINARIES
- QUALIFICATION
- QUARTERMASTER
- REAPPOINTMENT
- REENFORCEMENT
- REIMBURSEMENT
- REINFORCEMENT
- REINSTATEMENT
- REVOLUTIONARY
- SPECIFICATION
- TRANSATLANTIC

FOURTEEN LETTER WORDS

- ADMINISTRATION
- ADMINISTRATIVE
- CENTRALIZATION
- CHARACTERISTIC
- CIRCUMSTANTIAL
- CLASSIFICATION
- CORRESPONDENCE
- DEMOBILIZATION
- DISCONTINUANCE
- DISTINGUISHING
- IDENTIFICATION
- INTERPRETATION
- INVESTIGATIONS
- IRREGULARITIES
- METEOROLOGICAL
- NATURALIZATION
- RECOMMENDATION
- RECONNAISSANCE
- RECONNOITERING
- RECONSTRUCTION
- REORGANIZATION
- REPRESENTATIVE
- RESPONSIBILITY
- SATISFACTORILY
- TRANSPORTATION

Table D–2 (~~C~~). List of words used in military text arranged alphabetically in reverse order according to word length (U)

THREE LETTER WORDS

SEA
JOB
ROB
TUB
QMC
ARC
BAD
HAD
ADD
RED
AID
BID
DID
RID
OLD
AND
END

SEE
AGE
SHE
THE
DIE
ONE
ARE
USE
DUE
OWE
EYE
OFF
BAG
KEG
BIG
JIG
DOG

MAJ
ADJ
ASK
GAL
ALL
ILL
COL
CPL
CAM
HAM
AIM
HIM
ARM
SUM
CAN
MAN
NAN

TAN
GEN
MEN
PEN
TEN
PIN
TIN
TON
WON
DUN
GUN
RUN
SUN
OWN
AGO
TOO
TWO

TOP
GHQ
BAR
CAR
FAR
PAR
WAR
HER
PER
AIR
FOR
OUR
GAS
HAS
WAS
HIS
ITS

EAT
MAT
VAT
ACT
GET
LET
NET
SET
WET
YET
SGT
WGT
FIT
GOT
LOT
NOT
APT

BUT
CUT
OUT
PUT
PVT
CWT
YOU
CAV
LAW
SAW
FEW
NEW
HOW
LOW
NOW
TAX

FIX
MIX
SIX
BOX
FOX
DAY
LAY
MAY
PAY
SAY
WAY
ANY
SPY
DRY
TRY
BUY

FOUR LETTER WORDS

AREA
ASIA
BULB
BOMB
HEAD
LEAD
LOAD
ROAD
RAID
SAID
HOLD
HAND
LAND
KIND
HARD
HERD
ONCE
MADE
AIDE
SIDE
CODE
FLEE
EDGE
TAKE

MIKE
YOKE
ABLE
FILE
MILE
MULE
RULE
SAME
TIME
SOME
LINE
MINE
NINE
ZONE
JUNE
OBOE
PIPE
TYPE
TARE
HERE
WERE
FIRE
WIRE
MORE

BASE
FUSE
DATE
LATE
NOTE
BLUE
HAVE
FIVE
LOVE
MOVE
FUZE
HALF
FLAG
KING
LONG
EACH
HIGH
DASH
PUSH
RUSH
WITH
BOTH
LEAK
BACK

WEEK
TALK
BULK
RANK
SANK
TANK
SUNK
BOOK
COOK
HOOK
LOOK
TOOK
DARK
PARK
MASK
TASK
ORAL
MTCL
FEEL
RAIL
CALL
FALL
CELL
FELL

WELL
HILL
WILL
FULL
TOOL
TEAM
THEM
ITEM
MAIM
FROM
FARM
FIRM
FORM
THAN
PLAN
BEEN
SEEN
THEN
WHEN
OPEN
MAIN
RAIN
JOIN

NOON
SOON
DOWN
TOWN
ZERO
ALSO
INTO
KEEP
SHIP
DUMP
PUMP
STOP
NEAR
REAR
OVER
FOUR
YOUR
EYES
THIS
AXIS
TONS
GUNS
MASS

PASS
LESS
MESS
LOSS
HITS
DAYS
MEAT
THAT
WHAT
FEET
MEET
LEFT
OMIT
UNIT
HALT
TENT
SHOT
RIOT
DIRT
EAST
FAST
LAST
WEST

LIST
LOST
POST
JUST
ROUT
NEXT
TEXT
LIEU
DRAW
XRAY
AWAY
BODY
THEY
ALLY
ONLY
JULY
ARMY
MANY
VARY
VERY
EASY
CITY
NAVY

Table D-2 (C). List of words used in military text arranged alphabetically in reverse order according to word length (U)--Continued

FIVE LETTER WORDS

COMMA
ZEBRA
SQUAD
SPEED
WIPED
RIGID
RAPID
FIELD
BLIND
GUARD
AWARD
THIRD
BRIBE
PLACE
VOICE
FORCE
TRUCE
THREE
RIDGE
SIEGE
RANGE
BARGE
LARGE
GAUGE
STAKE
SMOKE
BROKE

SCALE
TITLE
ALINE
SLOPE
FLARE
THERE
WHERE
SHORE
CEASE
ERASE
THESE
CLOSE
HORSE
CAUSE
HOUSE
ROUTE
ISSUE
LEAVE
DRIVE
PROVE
CURVE
SEIZE
CHIEF
STAFF
PROOF
BEING
GOING

ALONG
AMONG
BEACH
REACH
WHICH
MARCH
WEIGH
FRESH
WIDTH
FIFTH
TENTH
NINTH
BOOTH
DEPTH
NORTH
SOUTH
SIXTH
BREAK
BLACK
CHECK
QUICK
TRUCK
CREEK
FLANK
CLERK
LOCAL
VOCAL

CANAL
FATAL
VITAL
TOTAL
EQUAL
USUAL
NAVAL
WHEEL
STEEL
REPEL
LEVEL
APRIL
SMALL
SHELL
SPELL
DRILL
ALARM
JAPAN
QUEEN
TAKEN
SEVEN
GIVEN
ALIGN
AGAIN
PLAIN
TRAIN
BEGIN

WAGON
UNION
COLON
DRAWN
RADIO
EQUIP
TROOP
GROUP
CLEAR
SUGAR
UNDER
ORDER
DEFER
REFER
EAGER
ROGER
ETHER
OTHER
BAKER
LATER
METER
PETER
AFTER
ENTER
RIVER
COVER
THEIR

PRIOR
MAJOR
VALOR
ARMOR
HONOR
ERROR
MOTOR
AREAS
BOMBS
RAIDS
WOODS
YARDS
MILES
FIRES
CASES
GATES
PACKS
DECKS
DOCKS
BANKS
TANKS
PLANS
SHIPS
CORPS
FEARS
PAIRS
HOURS

DRESS
PRESS
CROSS
FLATS
BOATS
RAFTS
UNITS
TRACT
FLEET
QUIET
ASSET
SHIFT
EIGHT
FIGHT
LIGHT
NIGHT
RIGHT
SIGHT
AWAIT
SPLIT
LIMIT
VISIT
AGENT
POINT
FRONT
COUNT
DEPOT

START
ALERT
LEAST
COAST
CREST
GUEST
FIRST
BURST
ABOUT
ALLOW
ANNEX
TODAY
DELAY
READY
FOGGY
DAILY
RALLY
APPLY
EARLY
ENEMY
EVERY
FERRY
FIFTY
PARTY
FORTY
SIXTY
HEAVY

SIX LETTER WORDS

CANADA
ARABIA
ALASKA
PANAMA
METRIC
CRITIC
BOMBED
BARBED
RAIDED
LANDED
WOODED
INDEED
ALLIED
KILLED
FORMED
DOWNED
SCORED
PASSED
CAUSED
UNITED

HALTED
ROUTED
LIQUID
INLAND
ISLAND
DEFEND
OFFEND
DEPEND
EXPEND
INTEND
EXTEND
SECOND
BEYOND
GROUND
METHOD
PERIOD
RECORD
OFFICE
POLICE
ADVICE

DEVICE
NOVICE
FIERCE
REDUCE
PARADE
DECIDE
DIVIDE
DECODE
ENCODE
COFFEE
DECREE
DEGREE
STRAFE
ENGAGE
DAMAGE
MANAGE
GARAGE
BRIDGE
ALLEGE
CHANGE

CHARGE
GEORGE
REFUGE
MORALE
UNABLE
CIRCLE
SINGLE
MOBILE
BEETLE
BATTLE
SETTLE
LITTLE
NOZZLE
MUZZLE
SCHEME
RESUME
ENGINE
RAVINE
EUROPE
SPHERE

SEVERE
RETIRE
ENTIRE
BEFORE
SECURE
ASSURE
FUTURE
GREASE
CHEESE
ADVISE
DEVISE
OPPOSE
COURSE
REFUSE
LOCATE
EXCITE
MINUTE
RESCUE
LEAGUE
PURSUE

ARRIVE
ACTIVE
TWELVE
BREEZE
RELIEF
ZIGZAG
RIDING
FILING
LINING
MINING
FIRING
WIRING
DURING
NOTING
MOVING
FLYING
BREACH
DETACH
ATTACH
BRANCH

TRENCH
LAUNCH
SEARCH
CHURCH
SWITCH
THOUGH
FINISH
EIGHTH
FOURTH
ATTACK
DEBARK
EMBARK
VERBAL
RADIAL
SERIAL
ANIMAL
FORMAL
NORMAL
SIGNAL
POSTAL

MANUAL
ANNUAL
CASUAL
VISUAL
CANCEL
VESSEL
DETAIL
REFILL
ENROLL
SCHOOL
PATROL
PISTOL
SYSTEM
VICTIM
SIGCOM
BOTTOM
INFORM
MEDIUM
SUDDEN
SCREEN

Table D-2 (~~C~~). List of words used in military text arranged alphabetically in reverse order according to word length (U)--Continued

SIX LETTER WORDS—Continued

SUNKEN
BROKEN
SEAMEN
HAPPEN
BATTEN
ELEVEN
REMAIN
ATTAIN
WITHIN
COLUMN
RATION
ACTION
COMMON
SUMMON
POISON
LESSON
PONTON
RETURN
DRYRUN
TATTOO
APPEAR
DOLLAR

MORTAR
RUBBER
MEMBER
BOMBER
NUMBER
PINCER
LEADER
LADDER
MURDER
PREFER
SUFFER
MEAGER
HIGHER
CIPHER
EITHER
TANKER
HAMMER
SUMMER
BANNER
MANNER
GUNNER

RUNNER
KEEPER
HELPER
PROPER
NEARER
ERASER
CENTER
BETTER
LETTER
BITTER
LITTER
AFFAIR
REPAIR
HARBOR
TERROR
MIRROR
SECTOR
VICTOR
DOCTOR
CANVAS
PLACES

FORCES
BARGES
BODIES
ALLIES
ARMIES
TABLES
PLANES
PASSES
LOSSES
STATES
ROUTES
ISSUES
CRISIS
SHELLS
SPOOLS
TRAINS
SPOONS
STRIPS
TROOPS
ORDERS
OTHERS

COLORS
ACCESS
EXCESS
UNLESS
STRESS
ACROSS
ASSETS
VISITS
POINTS
STATUS
ALWAYS
COMBAT
DEFEAT
THREAT
DEFECT
EFFECT
REJECT
SELECT
EXPECT
DIRECT
STREET

TARGET
PICKET
ROCKET
BILLET
TURRET
SUNSET
WEIGHT
FLIGHT
SLIGHT
NAUGHT
FOUGHT
NOUGHT
CREDIT
SUBMIT
COMMIT
SUMMIT
RESULT
ORIENT
INTENT
EXTENT
INVENT

CANNOT
ACCEPT
EXCEPT
PROMPT
DEPART
DESERT
DIVERT
ESCORT
EFFORT
REPORT
ARREST
RESIST
ASSIST
AUGUST
ADJUST
DUGOUT
OUTPUT
BUREAU
REVIEW
FOLLOW
FRIDAY

MONDAY
SUNDAY
ANYWAY
REMEDY
VALLEY
PARLEY
CONVEY
SURVEY
VERIFY
SUPPLY
HOURLY
DEPLOY
EMPLOY
CONVOY
OCCUPY
SALARY
ARMORY
NINETY
EIGHTY
TWENTY
THIRTY

SEVEN LETTER WORDS

MILITIA
ANTENNA
ALMANAC
BIVOUAC
TRAFFIC
PACIFIC
ASIATIC
REDUCED
INVADED
DECIDED
DECODED
ENCODED
WOUNDED
GUARDED
PROCEED
ENGAGED
DAMAGED
REACHED
MARCHED
WRECKED
SHELLED
DROPPED
STOPPED
HUNDRED
ORDERED
COVERED

RETIRED
ARMORED
PRESSED
CROSSED
OMITTED
DELAYED
COMMAND
COMMEND
SUSPEND
RESPOND
BOMBARD
AWKWARD
FORWARD
REPLACE
SERVICE
ADVANCE
ABSENCE
ENFORCE
BRIGADE
GRENADE
PRECEDE
OUTSIDE
INCLUDE
EXCLUDE
REFUGEE

WINDAGE
BAGGAGE
PACKAGE
VILLAGE
TONNAGE
AVERAGE
STORAGE
BARRAGE
PASSAGE
MESSAGE
COLLEGE
ARRANGE
WITHTHE
THATTHE
CHARLIE
PRAIRIE
VISIBLE
BICYCLE
HOSTILE
EXTREME
CONFINE
MACHINE
ROUTINE
CYCLONE
WARFARE

DECLARE
PREPARE
CALIBRE
MISFIRE
INSPIRE
REQUIRE
INQUIRE
LECTURE
RELEASE
DISEASE
SUNRISE
LICENSE
DEFENSE
OFFENSE
PROPOSE
SUPPOSE
PURPOSE
REVERSE
BECAUSE
MANDATE
RADIATE
OPERATE
ELEVATE
ENTENTE
PROMOTE

COMMUTE
REVENUE
RELIEVE
RECEIVE
PASSIVE
CAPTIVE
REVOLVE
APPROVE
OBSERVE
RESERVE
ANALYZE
JUMPOFF
BOMBING
PLACING
FORCING
HEADING
LEADING
LOADING
BEDDING
RAIDING
HOLDING
LANDING
BINDING
FINDING
FORGING

FISHING
PUSHING
NOTHING
TALKING
SINKING
SMOKING
FALLING
FILLING
KILLING
EVENING
RAINING
MANNING
RUNNING
MORNING
SLOPING
MAPPING
BEARING
GASSING
MESSING
MISSING
LIFTING
HALTING
GETTING
FITTING
ISSUING

VARYING
ICEBERG
DEBOUGH
THROUGH
FURNISH
TWELFTH
SEVENTH
SETBACK
DERRICK
DETRUCK
ENTRUCK
MEDICAL
LOGICAL
CONCEAL
ILLEGAL
MARSHAL
INITIAL
MARTIAL
FEDERAL
GENERAL
SEVERAL
CENTRAL
NATURAL
COASTAL
GRADUAL

Table D-2 ~~(C)~~. List of words used in military text arranged alphabetically in reverse order according to word length (U)--Continued

SEVEN LETTER WORDS—Continued

UNUSUAL
ARRIVAL
CHANNEL
COLONEL
COUNCIL
FUELOIL
INSTALL
DISTILL
PAYROLL
CONTROL
WILLIAM
DIAGRAM
PROGRAM
MINIMUM
MAXIMUM
HASBEEN
FIFTEEN
SIXTEEN
BETWEEN
KITCHEN
WRITTEN
EXPLAIN
TERRAIN
DETRAIN

ENTRAIN
CONTAIN
CAPTAIN
CONDEMN
ABANDON
OPINION
SESSION
MISSION
STATION
SECTION
ECHELON
BALLOON
PLATOON
LIAISON
HORIZON
EASTERN
WESTERN
FOGHORN
UNKNOWN
TOBACCO
TORPEDO
WARSHIP
DEVELOP

ENVELOP
SIMILAR
REGULAR
CALIBER
OCTOBER
OFFICER
POUNDER
TRIGGER
WEATHER
WHETHER
ANOTHER
FARTHER
FURTHER
SOLDIER
CARRIER
COURIER
HEAVIER
TRAWLER
STEAMER
CLIPPER
CRUISER
AMMETER
FIGHTER

STARTER
QUARTER
DELIVER
RECOVER
AVIATOR
TRACTOR
VISITOR
TACTICS
ISLANDS
CHANGES
ENEMIES
BATTLES
GLASSES
CHASSIS
ATTACKS
VESSELS
PATROLS
BOMBERS
NUMBERS
REPAIRS
SAILORS
SECTORS
COMPASS

SUCCESS
USELESS
ILLNESS
WITNESS
ADDRESS
EXPRESS
DISMISS
DISCUSS
TARGETS
SURPLUS
RETREAT
EXTRACT
CONTACT
COLLECT
RESPECT
CORRECT
PROTECT
INFLICT
CONDUCT
TONIGHT
CIRCUIT
RECRUIT
PURSUIT

ASSAULT
INSTANT
ELEMENT
COMMENT
CURRENT
PRESENT
APPOINT
RECEIPT
ATTEMPT
SUPPORT
SUGGEST
HIGHEST
NEAREST
PROTEST
REQUEST
AGAINST
OUTPOST
PROVOST
BOYCOTT
WITHOUT
LOOKOUT
SIMPLEX
TUESDAY

RAILWAY
SECRECY
VACANCY
SIGNIFY
SATISFY
RAPIDLY
QUICKLY
NIGHTLY
SHORTLY
COMPANY
DESTROY
PRIMARY
SUMMARY
LIBRARY
JANUARY
BRIBERY
BATTERY
INQUIRY
CAVALRY
VICTORY
EMBASSY
UTILITY
SEVENTY

EIGHT LETTER WORDS

INSIGNIA
SPECIFIC
TERRIFIC
ECONOMIC
MECHANIC
ATLANTIC
RAILHEAD
RAILROAD
REPLACED
ADVANCED
DEMANDED
EXPANDED
DEFENDED
OFFENDED
EXPENDED
EXTENDED
GROUNDED
BESIEGED
DETACHED
FINISHED
OCCUPIED
ATTACKED
REPELLED

EXPELLED
ENROLLED
DISARMED
ASSIGNED
RETURNED
APPEARED
DECLARED
PREPARED
HINDERED
SUFFERED
CENTERED
BATTERED
LETTERED
REPAIRED
REQUIRED
RESTORED
DEFERRED
CAPTURED
REPULSED
COMPOSED
MANDATED
DEFEATED
REPEATED

DICTATED
EFFECTED
INFECTED
REJECTED
SELECTED
BILLETED
INVENTED
DEPARTED
DESERTED
ESCORTED
DEPORTED
REPORTED
ARRESTED
ENLISTED
SURVIVED
IMPROVED
OBSERVED
REVIEWED
DEPLOYED
AIRFIELD
FOOTHOLD
THOUSAND
SURROUND

STANDARD
OUTBOARD
OUTGUARD
WINDWARD
EASTWARD
WESTWARD
DESCRIBE
ORDNANCE
DISTANCE
COMMENCE
SENTENCE
ANNOUNCE
COMMERCE
ENFILADE
CONCLUDE
LATITUDE
ALTITUDE
EMPLOYEE
CARRIAGE
FUSELAGE
EQUIPAGE
FRONTAGE
SABOTAGE

LANGUAGE
DISLODGE
EXCHANGE
PROBABLE
SUITABLE
ELIGIBLE
TERRIBLE
POSSIBLE
FLEXIBLE
ASSEMBLE
OBSTACLE
ENCIRCLE
SCHEDULE
MARITIME
AIRDROME
AIRPLANE
JETPLANE
MEDICINE
DOCTRINE
POSTPONE
SEABORNE
AIRBORNE
DEVELOPE

ENVELOPE
INSECURE
PRESSURE
DECREASE
EXERCISE
SURPRISE
SUSPENSE
DISPERSE
TRAVERSE
DEDICATE
INDICATE
INITIATE
ESTIMATE
ORDINATE
DETONATE
SEPARATE
EVACUATE
EXCAVATE
OBSOLETE
COMPLETE
CONCRETE
EXPEDITE
DEFINITE

OPPOSITE
CONTINUE
CRITIQUE
THATHAVE
DECISIVE
POSITIVE
PRESERVE
EQUALIZE
MOBILIZE
INVADING
DIVIDING
BUILDING
GUARDING
ENGAGING
DAMAGING
MARCHING
BREAKING
FLANKING
TOTALING
SHELLING
BATTLING
SWIMMING
TRAINING

Table D-2 (~~C~~). List of words used in military text arranged alphabetically in reverse order according to word length (U)--Continued

EIGHT LETTER WORDS—Continued

PLANNING
SWEEPING
SHIPPING
GROUPING
ENTERING
COVERING
RETIRING
ADVISING
OPPOSING
DRESSING
PRESSING
CROSSING
DRIFTING
FIGHTING
SIGHTING
LIMITING
PAINTING
PRINTING
SPOTTING
DELAYING
RALLYING
CARRYING
FERRYING
APPROACH
ENTRENCH
INTRENCH
RESEARCH
DESPATCH
DISPATCH
SKIRMISH
DIMINISH

ELEVENTH
ANTITANK
CODEBOOK
CHEMICAL
CLERICAL
TACTICAL
CRITICAL
NAUTICAL
OFFICIAL
MATERIAL
MEMORIAL
NATIONAL
INTERNAL
CORPORAL
HOSPITAL
APPROVAL
MATERIEL
PARALLEL
SENTINEL
SEALEVEL
PROTOCOL
MERCIFUL
TELEGRAM
AMERICAN
EUROPEAN
CIVILIAN
HAVEBEEN
NINETEEN
EIGHTEEN
THIRTEEN
FOURTEEN

CAMPAIGN
CHAPLAIN
MAINTAIN
MOUNTAIN
BULLETIN
INVASION
DECISION
DIVISION
LOCATION
AVIATION
CITATION
TAXATION
JUNCTION
IGNITION
POSITION
FORENOON
SQUADRON
GARRISON
NORTHERN
SOUTHERN
CIRCULAR
DECEMBER
REMEMBER
NOVEMBER
DEFENDER
RECORDER
ENGINEER
TRANSFER
DECIPHER
ENCIPHER

PRISONER
IMPROPER
REPEATER
DESERTER
DISASTER
REGISTER
CANISTER
RECEIVER
REVOLVER
OBSERVER
MANEUVER
EMPLOYER
HOWITZER
CORRIDOR
SUPERIOR
INTERIOR
EXTERIOR
OPERATOR
DICTATOR
REJECTOR
DIRECTOR
DETECTOR
ASSOONAS
POLITICS
COMMANDS
ADVANCES
BARRAGES
MESSAGES
REMEDIES
SUPPLIES

VEHICLES
MISFIRES
DEFENSES
EXPENSES
PURPOSES
RESERVES
ANALYSIS
BARRACKS
MISSIONS
STATIONS
FACTIONS
PONTOONS
WARSHIPS
OFFICERS
SOLDIERS
CARRIERS
TRAILERS
TRAWLERS
CRUISERS
FIGHTERS
QUARTERS
CARELESS
WIRELESS
BUSINESS
DARKNESS
CONGRESS
PROGRESS
FORTRESS
DISTRESS
REDCROSS

RESPECTS
ELEMENTS
ATTEMPTS
PROTESTS
OUTPOSTS
ENORMOUS
LUMINOUS
RIGOROUS
VIGOROUS
CONTRACT
INDIRECT
CONFLICT
DISTRICT
INSTRUCT
AIRCRAFT
DAYLIGHT
MIDNIGHT
PROHIBIT
SERGEANT
DOMINANT
ADJUTANT
ADJACENT
INCIDENT
ARMAMENT
MOVEMENT
REGIMENT
APPARENT
PASSPORT
INTEREST
REENLIST

WITHDRAW
WITHDREW
TOMORROW
PARALLAX
SATURDAY
THURSDAY
CAUSEWAY
EFFICACY
IDENTIFY
STRATEGY
PROBABLY
ASSEMBLY
ACTUALLY
MONOPOLY
EASTERLY
WESTERLY
BOUNDARY
MILITARY
SANITARY
FEBRUARY
CEMETERY
ADVISORY
INFANTRY
CAPACITY
FATALITY
CALAMITY
VICINITY
PRIORITY
ACTIVITY
CASUALTY

NINE LETTER WORDS

MEMORANDA
STRATEGIC
AUTOMATIC
PATRIOTIC
BALLISTIC
BEACHHEAD
SPEARHEAD
DESCRIBED
ANNOUNCED
BLOCKADED
SUCCEEDED
PROCEEDED
COMMANDED
SUSPENDED
BOMBARDED
FORTIFIED

CANCELLED
COMPELLED
DETRAINED
ENTRAINED
CONDEMNED
ECHELONED
DEVELOPED
CONQUERED
PREFERRED
CONFERRED
DECREASED
INCREASED
CONDENSED
COLLAPSED
DISPERSED
ADDRESSED

IMPRESSED
DISCUSSED
INDICATED
POPULATED
ESTIMATED
DOMINATED
DETONATED
SUSPECTED
CORRECTED
PROTECTED
INFLICTED
COMPLETED
INHABITED
EXHIBITED
ASSAULTED
APPOINTED

ATTEMPTED
PROTESTED
REQUESTED
SUBMITTED
CONTINUED
DESTROYED
MOTORIZED
SEMIRIGID
RECOMMEND
REARGUARD
NORTHWARD
SOUTHWARD
AMBULANCE
DOMINANCE
CLEARANCE
ENDURANCE

ASSURANCE
ALLOWANCE
INCIDENCE
REFERENCE
INFLUENCE
REENFORCE
REINFORCE
LONGITUDE
COMMITTEE
ADVANTAGE
CARTRIDGE
CHALLENGE
AVAILABLE
UNTENABLE
DIRIGIBLE
PRINCIPLE

AERODROME
HURRICANE
AEROPLANE
INTERVENE
FRONTLINE
DETERMINE
TELEPHONE
INTERFERE
ELSEWHERE
SHELLFIRE
THEREFORE
PROCEDURE
PREMATURE
DEPARTURE
NAVALBASE
MANGANESE

Table D-2 (~~C~~). List of words used in military text arranged alphabetically in reverse order according to word length (U)--Continued

NINE LETTER WORDS–Continued

CRITICISE
INTERPOSE
ASSOCIATE
IMMEDIATE
OSCILLATE
CIRCULATE
DESIGNATE
ALTERNATE
COOPERATE
ELABORATE
PENETRATE
REINSTATE
CIGARETTE
PARACHUTE
DESTITUTE
TECHNIQUE
EXPANSIVE
DEFENSIVE
OFFENSIVE
EXPENSIVE
INTENSIVE
EXTENSIVE
EXPLOSIVE
EXCESSIVE
INCLUSIVE
EXCLUSIVE
TENTATIVE
DEFECTIVE
EFFECTIVE
OBJECTIVE
INCENTIVE
EXECUTIVE
RECOGNIZE
SERVICING
ADVANCING
PRECEDING
EXTENDING

REGARDING
ACCORDING
INCLUDING
LAUNCHING
ATTACKING
DEBARKING
REFILLING
SCREENING
REMAINING
OBTAINING
INCLINING
BEGINNING
RETURNING
PREPARING
NUMBERING
CENTERING
REQUIRING
OPERATING
ENLISTING
RECEIVING
REVIEWING
EMPLOYING
OCCUPYING
PARAGRAPH
ESTABLISH
TWENTIETH
FIFTEENTH
SIXTEENTH
WATERTANK
TECHNICAL
CHRONICAL
PRACTICAL
POLITICAL
IDENTICAL
PRINCIPAL
DISMISSAL
CONTINUAL

PERSONNEL
CABLEGRAM
RADIOGRAM
FIREALARM
CRITICISM
MECHANISM
DIETITIAN
SEVENTEEN
SUSPICION
BATTALION
REBELLION
COLLISION
PROVISION
EXPANSION
ASCENSION
DIMENSION
EXTENSION
EXPLOSION
ADMISSION
EXCLUSION
RADIATION
VARIATION
INFLATION
FORMATION
OPERATION
SITUATION
ELEVATION
OBJECTION
DIRECTION
CONDITION
COALITION
PARTITION
DETENTION
RETENTION
INTENTION
ATTENTION

INVENTION
PROMOTION
SEMICOLON
AFTERNOON
DISAPPEAR
IRREGULAR
SEPTEMBER
COMMANDER
SURRENDER
REMAINDER
PASSENGER
MESSENGER
BRIGADIER
STRAGGLER
NEWSPAPER
CHARACTER
KILOMETER
BAROMETER
GYROMETER
DESTROYER
PROJECTOR
PROTECTOR
CHAUFFEUR
LOGISTICS
STANDARDS
RESOURCES
COMPANIES
BATTERIES
EMBASSIES
AIRDROMES
SEAPLANES
AIRPLANES
EXERCISES
WITNESSES
ADDRESSES
ESTIMATES

CONTINUES
BUILDINGS
OFFICIALS
REPRISALS
PROPOSALS
CIVILIANS
CAMPAIGNS
MAINTAINS
DIVISIONS
MUNITIONS
POSITIONS
ENGINEERS
PRISONERS
READINESS
CONFLICTS
DISTRICTS
INCIDENTS
MOVEMENTS
OUTSKIRTS
ANONYMOUS
APPARATUS
DISINFECT
INTERDICT
DIFFICULT
COMBATANT
IMPORTANT
ASSISTANT
CONFIDENT
PRESIDENT
DEPENDENT
NEGLIGENT
DEFICIENT
EFFICIENT
PLACEMENT
AGREEMENT
AMUSEMENT

STATEMENT
EQUIPMENT
GROUPMENT
INTERMENT
ALLOTMENT
PERMANENT
DIFFERENT
REPRESENT
RESTRAINT
INTERCEPT
INTERRUPT
TRANSPORT
NORTHEAST
SOUTHEAST
NORTHWEST
SOUTHWEST
INTERVIEW
YESTERDAY
WEDNESDAY
EMERGENCY
NORTHERLY
SERIOUSLY
INSTANTLY
ACCOMPANY
ARBITRARY
NECESSARY
SECRETARY
ARTILLERY
ACCESSORY
TERRITORY
LIABILITY
HOSTILITY
PROXIMITY
INDEMNITY
INTEGRITY
NECESSITY

TEN LETTER WORDS

ATOMICBOMB
GEOGRAPHIC
GYROSCOPIC
DIPLOMATIC
BRIDGEHEAD
PRESCRIBED
REENFORCED
REINFORCED
BEENNEEDED
UNEXPENDED

APPROACHED
ENTRENCHED
DESPATCHED
DISPATCHED
THREATENED
MAINTAINED
DETERMINED
ONEHUNDRED
DECIPHERED
ENCIPHERED

COMPRESSED
DISTRESSED
DESIGNATED
RESTRICTED
INSTRUCTED
PROHIBITED
REENLISTED
MECHANIZED
CONTRABAND
UNDERSTAND

UNDERSTOOD
COASTGUARD
POSTOFFICE
ACCORDANCE
ALLEGIANCE
APPEARANCE
ACCEPTANCE
RESISTANCE
ASSISTANCE
PRECEDENCE

CONFIDENCE
NEGLIGENCE
EXPERIENCE
PREFERENCE
DIFFERENCE
CONFERENCE
CAMOUFLAGE
DEPENDABLE
EXPENDABLE
IMPASSABLE

Table D-2 (~~C~~). List of words used in military text arranged alphabetically in reverse order according to word length (U)--Continued

TEN LETTER WORDS–Continued

UNSUITABLE
ACCEPTABLE
IMPOSSIBLE
ASPOSSIBLE
RECEPTACLE
MOTORCYCLE
AUTOMOBILE
DISCIPLINE
QUARANTINE
ENTERPRISE
TRANSVERSE
COORDINATE
ILLUMINATE
ANTICIPATE
ILLITERATE
ILLUSTRATE
COMPENSATE
DISTRIBUTE
SUBSTITUTE
CONSTITUTE
COMMUNIQUE
TWENTYFIVE
SUCCESSIVE
IMPRESSIVE
LOCOMOTIVE
CENTRALIZE
NATURALIZE
DEMOBILIZE
COMMANDING
DEBOUCHING
DETRUCKING
ENTRUCKING
ENCIRCLING
SIGNALLING
PATROLLING
OVERCOMING
DETRAINING
CONCERNING
INDICATING
ANTEDATING

EVACUATING
COLLECTING
CONNECTING
INFLICTING
EXPEDITING
RECRUITING
ATTEMPTING
SUPPORTING
EXTINGUISH
NINETEENTH
EIGHTEENTH
THIRTEENTH
FOURTEENTH
WILLATTACK
ARTIFICIAL
CREDENTIAL
ADDITIONAL
ACCIDENTAL
REGIMENTAL
INDIVIDUAL
WITHDRAWAL
AIRCONTROL
SUCCESSFUL
RESPECTFUL
MEMORANDUM
SUSPENSION
DISPERSION
CONCESSION
CONFESSION
DEPRESSION
IMPRESSION
POSSESSION
SUBMISSION
COMMISSION
PERMISSION
DISCUSSION
CONCLUSION
DEDICATION
INDICATION

ALLOCATION
FOUNDATION
RECREATION
IRRIGATION
NAVIGATION
REGULATION
POPULATION
ESTIMATION
DOMINATION
DETONATION
OCCUPATION
SEPARATION
DECORATION
LIMITATION
SANITATION
INVITATION
EVACUATION
EVALUATION
EXCAVATION
COLLECTION
CONNECTION
INSPECTION
CORRECTION
PROTECTION
EXHIBITION
EXPEDITION
DEFINITION
AMMUNITION
OPPOSITION
PROPORTION
REVOLUTION
MACHINEGUN
BATTLESHIP
CENSORSHIP
ARMOREDCAR
DIVEBOMBER
COMMANDEER
DISPATCHER
MILLIMETER

GONIOMETER
HYDROMETER
HYGROMETER
AMBASSADOR
INSTRUCTOR
BALLISTICS
STATISTICS
CROSSROADS
DESPATCHES
DISPATCHES
ASSEMBLIES
FACILITIES
ACTIVITIES
CASUALTIES
FRONTLINES
SUBMARINES
OBJECTIVES
ENEMYTANKS
SUSPICIONS
COLLISIONS
PROVISIONS
EXPLOSIONS
FORMATIONS
OPERATIONS
DIRECTIONS
CONDITIONS
TROOPSHIPS
NEWSPAPERS
KILOMETERS
DESTROYERS
TRANSPORTS
SUSPICIOUS
VICTORIOUS
CIRCUITOUS
CONTINUOUS
PHOSPHORUS
FLASHLIGHT
COMMANDANT
LIEUTENANT

CONTINGENT
SUFFICIENT
CONVENIENT
EQUIVALENT
ENGAGEMENT
MANAGEMENT
EXCITEMENT
DETACHMENT
ATTACHMENT
EXPERIMENT
ENROLLMENT
ASSIGNMENT
ATTAINMENT
INTERNMENT
GOVERNMENT
ASSESSMENT
COMMITMENT
DEPARTMENT
ENLISTMENT
INSTRUMENT
DEPLOYMENT
EMPLOYMENT
PERSISTENT
AIRSUPPORT
CONSPIRACY
DEFICIENCY
EFFICIENCY
COMPLETELY
APPARENTLY
INCENDIARY
COMMISSARY
ELEMENTARY
LABORATORY
TRAJECTORY
CAPABILITY
AUDIBILITY
VISIBILITY
SIMILARITY
INSECURITY

ELEVEN LETTER WORDS

IMPEDIMENTA
TOPOGRAPHIC
RECOMMENDED
PREARRANGED
ESTABLISHED
OVERWHELMED
DISAPPEARED

SURRENDERED
ENCOUNTERED
TRANSFERRED
DISINFECTED
REAPPOINTED
INTERCEPTED
INTERRUPTED

CONSTITUTED
BATTLEFIELD
PERFORMANCE
MAINTENANCE
COINCIDENCE
SUBSISTENCE
ACKNOWLEDGE

CATASTROPHE
IMFLAMMABLE
RESPONSIBLE
NAVALBATTLE
TEMPERATURE
MANUFACTURE
SCHOOLHOUSE

CUSTOMHOUSE
CERTIFICATE
COMMUNICATE
INVESTIGATE
APPROPRIATE
APPROXIMATE
EXTERMINATE

Table D-2 ~~(C)~~. List of words used in military text arranged alphabetically in reverse order according to word length (U)--Continued

ELEVEN LETTER WORDS-Continued

DETERIORATE
CONCENTRATE
DEMONSTRATE
NECESSITATE
DISCONTINUE
SEVENTYFIVE
PROGRESSIVE
RETROACTIVE
DESCRIPTIVE
SYNCHRONIZE
APPROACHING
INTERVENING
ENGINEERING
INTERFERING
ALTERNATING
INTERESTING
WITHDRAWING
DISTINGUISH
SEVENTEENTH
NAVALATTACK
STRATEGICAL
TRADITIONAL
CONTINENTAL
FIRECONTROL

NATIONALISM
SMOKESCREEN
APPLICATION
ASSOCIATION
RETALIATION
DEBARKATION
EMBARKATION
LEGISLATION
CIRCULATION
INFORMATION
EXPLANATION
DESIGNATION
RESIGNATION
EXAMINATION
PREPARATION
COOPERATION
IMMIGRATION
INSPIRATION
CORPORATION
PENETRATION
ARBITRATION
COMPUTATION
OBSERVATION
RESERVATION

RESTRICTION
DISTINCTION
DESTRUCTION
INSTRUCTION
RECOGNITION
REQUISITION
COMPOSITION
DISPOSITION
COMPETITION
DESCRIPTION
CONSUMPTION
INSTITUTION
LIGHTBOMBER
HEAVYBOMBER
RANGEFINDER
DYNAMOMETER
THERMOMETER
INTERPRETER
RECONNOITER
BLOCKBUSTER
AERONAUTICS
NAVALFORCES
ACCESSORIES
HOSTILITIES

ENEMYPLANES
PHILIPPINES
PARENTHESES
HEAVYLOSSES
COMMUNIQUES
PARENTHESIS
CREDENTIALS
BATTLESHIPS
ARMOREDCARS
CORRECTNESS
ENGAGEMENTS
ASSIGNMENTS
ASSESSMENTS
INSTRUMENTS
ESTIMATEDAT
SIGNIFICANT
INDEPENDENT
INTELLIGENT
COEFFICIENT
BOMBARDMENT
REPLACEMENT
EMPLACEMENT
ENFORCEMENT
ARRANGEMENT

CONFINEMENT
REQUIREMENT
MEASUREMENT
IMPROVEMENT
CONCEALMENT
ECHELONMENT
DEVELOPMENT
APPOINTMENT
COMPARTMENT
BELLIGERENT
INCOMPETENT
FINGERPRINT
DISCREPANCY
PHOTOGRAPHY
IMMEDIATELY
EXTENSIVELY
EFFECTIVELY
PRELIMINARY
CONTROVERSY
ELECTRICITY
NATIONALITY
SUITABILITY
SUPERIORITY

TWELVE LETTER WORDS

TRANSPACIFIC
HYDROGRAPHIC
UNIDENTIFIED
COMMISSIONED
DISSEMINATED
CONCENTRATED
DEMONSTRATED
DISORGANIZED
SIGNIFICANCE
INTELLIGENCE
INTERFERENCE
INCOMPETENCE
CONSIDERABLE
FIGHTERPLANE
INTERMEDIATE
DECENTRALIZE
GENERALSTAFF
TRANSFERRING
ENTERPRISING
ILLUMINATING
DISTRIBUTING

CONSTITUTING
BREAKTHROUGH
GEOGRAPHICAL
CONFIDENTIAL
PRESIDENTIAL
RECREATIONAL
AGRICULTURAL
DEPARTMENTAL
UNSUCCESSFUL
GENERALALARM
VETERINARIAN
TRANSMISSION
VERIFICATION
CONFISCATION
COMMENDATION
CONCILIATION
CANCELLATION
PROCLAMATION
CONFIRMATION
CONFORMATION
COORDINATION

ILLUMINATION
ANTICIPATION
REGISTRATION
ILLUSTRATION
INAUGURATION
COMPENSATION
CONVERSATION
RADIOSTATION
CONTINUATION
PRESERVATION
MOBILIZATION
ORGANIZATION
INTERDICTION
ROADJUNCTION
INTRODUCTION
CONSTRUCTION
INTERVENTION
INTERCEPTION
CONSCRIPTION
INTERRUPTION
DISTRIBUTION

SUBSTITUTION
CONSTITUTION
NORTHWESTERN
SOUTHWESTERN
MARKSMANSHIP
MEDIUMBOMBER
COMMISSIONER
PSYCHROMETER
SHARPSHOOTER
DIFFICULTIES
UNITEDSTATES
PREPARATIONS
OBSTRUCTIONS
INSTRUCTIONS
LIGHTBOMBERS
HEAVYBOMBERS
HEADQUARTERS
PREPAREDNESS
COMPLETENESS
CARELESSNESS
SEARCHLIGHTS

REPLACEMENTS
EMPLACEMENTS
MEASUREMENTS
ADVANTAGEOUS
SIMULTANEOUS
ANTIAIRCRAFT
NONCOMBATANT
CONVALESCENT
DISPLACEMENT
COMMENCEMENT
ANNOUNCEMENT
ENTANGLEMENT
DECIPHERMENT
ENCIPHERMENT
REENLISTMENT
INEFFICIENCY
SUCCESSFULLY
RESPECTFULLY
SATISFACTORY
INTRODUCTORY
IRREGULARITY

Table D-2 (~~C~~). List of words used in military text arranged alphabetically in reverse order according to word length (U)--Continued

THIRTEEN LETTER WORDS

TRANSATLANTIC
DISTINGUISHED
DECENTRALIZED
DISAPPEARANCE
IMPRACTICABLE
INDETERMINATE
CORRESPONDING
CONCENTRATING
COUNTERATTACK
CHRONOLOGICAL
CONGRESSIONAL
INTERNATIONAL
SPECIFICATION
QUALIFICATION
COMMUNICATION
ACCOMMODATION
INVESTIGATION
DISSEMINATION
DETERMINATION
EXTERMINATION
CONSIDERATION
CONCENTRATION
DEMONSTRATION
QUARTERMASTER
CIRCUMSTANCES
DISCREPANCIES
PRELIMINARIES
FIGHTERPLANES
INSTALLATIONS
MEDIUMBOMBERS
MISCELLANEOUS
INSTANTANEOUS
REENFORCEMENT
REINFORCEMENT
REIMBURSEMENT
REINSTATEMENT
ESTABLISHMENT
ENTERTAINMENT
REAPPOINTMENT
APPROXIMATELY
EXTRAORDINARY
REVOLUTIONARY
DEPENDABILITY

FOURTEEN LETTER WORDS

CHARACTERISTIC
RECONNAISSANCE
DISCONTINUANCE
CORRESPONDENCE
ADMINISTRATIVE
REPRESENTATIVE
DISTINGUISHING
RECONNOITERING
METEOROLOGICAL
CIRCUMSTANTIAL
CLASSIFICATION
IDENTIFICATION
RECOMMENDATION
ADMINISTRATION
INTERPRETATION
TRANSPORTATION
CENTRALIZATION
NATURALIZATION
DEMOBILIZATION
REORGANIZATION
RECONSTRUCTION
IRREGULARITIES
INVESTIGATIONS
SATISFACTORILY
RESPONSIBILITY

Table D–3 (~~C~~). List of words used in military text arranged alphabetically according to word pattern (U)

PATTERN AA

A	CC	EPT	FA	LL		MA	NN	ER
A	CC	ORDING	FE	LL		A	NN	EX
O	CC	UPY	FU	LL		CA	NN	OT
A	DD		HI	LL		T	OO	
SU	DD	EN	I	LL		W	OO	DS
LA	DD	ER	INSTA	LL		PR	OO	F
BE	DD	ING	PAYRO	LL		B	OO	K
FL	EE		REFI	LL		C	OO	K
S	EE		SHE	LL		H	OO	K
THR	EE		SMA	LL		L	OO	K
PROC	EE	D	SPE	LL		T	OO	K
SP	EE	D	WE	LL		SCH	OO	L
CR	EE	K	WI	LL		T	OO	L
W	EE	K	VI	LL	AGE	PLAT	OO	N
F	EE	L	CO	LL	APSED	S	OO	N
ST	EE	L	DO	LL	AR	TR	OO	PS
WH	EE	L	OSCI	LL	ATE	C	OO	RDINATE
B	EE	N	KI	LL	ED	B	OO	TH
FOURT	EE	N	BI	LL	ET	STO	PP	ED
HASB	EE	N	BU	LL	ETIN	HA	PP	EN
QU	EE	N	VA	LL	EY	CLI	PP	ER
SCR	EE	N	A	LL	IED	MA	PP	ING
S	EE	N	A	LL	IES	A	PP	LY
SIXT	EE	N	FA	LL	ING	SU	PP	LY
R	EE	NLIST	PATRO	LL	ING	A	PP	OINT
K	EE	P	SHE	LL	ING	A	PP	OINTED
SW	EE	PING	A	LL	OW	SU	PP	ORT
F	EE	T	A	LL	Y	SU	PP	ORTING
FL	EE	T	RA	LL	Y	A	PP	ROVE
M	EE	T	CO	MM	A	TE	RR	AIN
JUMPO	FF		CO	MM	AND	CU	RR	ENT
O	FF		CO	MM	ANDER	A	RR	EST
STA	FF		SU	MM	ARY	HU	RR	ICANE
O	FF	END	CO	MM	END	DE	RR	ICK
SU	FF	ER	CO	MM	ENT	GA	RR	ISON
TRA	FF	IC	HA	MM	ER	A	RR	IVE
O	FF	ICE	SU	MM	ER	CA	RR	Y
O	FF	ICER	CO	MM	IT	FE	RR	Y
E	FF	ORT	SU	MM	IT	ACRO	SS	
FO	GG	Y	SU	MM	ON	COMPA	SS	
A	LL		CO	MM	UTE	CONGRE	SS	
CA	LL		TO	NN	AGE	CRO	SS	
CE	LL		CHA	NN	EL	DARKNE	SS	
DRI	LL		BA	NN	ER	DRE	SS	
ENRO	LL		GU	NN	ER	LE	SS	

Table D-3 ~~(C)~~. List of words used in military text arranged alphabetically according to word pattern (U)--Continued

PATTERN AA— Continued

LO	SS		A	SS	IGNED	BA	TT	EN
MA	SS		CRO	SS	ING	WRI	TT	EN
ME	SS		DRE	SS	ING	BI	TT	ER
PA	SS		ME	SS	ING	LI	TT	ER
PRE	SS		PA	SS	IVE	BA	TT	ERY
UNLE	SS		LE	SS	ON	SPO	TT	ING
WITNE	SS		I	SS	UE	BA	TT	LE
PA	SS	ED	A	SS	URE	BA	TT	LESHIP
A	SS	EMBLY	EMBA	SS	Y	MU	ZZ	LE
A	SS	ET	OMI	TT	ED	NO	ZZ	LE
PO	SS	IBLE	SUBMI	TT	ED			

MISCELLANEOUS PATTERNS

AABA	AGR	EEME	NT	AABCB	SU	FFICI	ENT
AABA	K	EEPE	R	AABCB	A	LLEGE	
AABA	CH	EESE		AABCB	CO	LLEGE	
AABA	BR	EEZE		AABCB	BI	LLETE	D
AABA	MA	NNIN	G	AABCB	A	MMETE	R
AABA	PLA	NNIN	G	AABCB	W	OODED	
AABA	RU	NNIN	G	AABCB	TE	RRIFI	C
AABA	L	OOKO	UT	AABCB	BA	TTERE	D
AABA	E	RROR		AABCBDEB	DI	FFERENCE	
AABA	MI	RROR		AABCC	A	CCESS	
AABA	TE	RROR		AABCC	A	CCESS	ORY
AABA	GLA	SSES		AABCC	CO	MMISS	ARY
AABA	LO	SSES		AABCCB	WI	LLATTA	CK
AABA	PA	SSES		AABCCDD	CO	MMITTEE	
AABA	CHA	SSIS		AABCCDEFBC	A	CCESSORIES	
AABA	A	SSIS	T	AABCDA	I	LLEGAL	
AABAACB	A	SSESSME	NT	AABCDA	A	TTEMPT	
AABAACBDEA	A	SSESSMENTS		AABCDAB	A	TTEMPTE	D
AABAB	PROC	EEDED		AABCDB	O	FFENSE	
AABB	CO	FFEE		AABCDB	CHA	LLENGE	
AABB	BA	LLOO	N	AABCDB	BA	LLISTI	C
AABBAACAC	B	EENNEFDED		AABCDB	A	RRESTE	D
AABBCBC	SU	CCEEDED		AABCDB	PA	SSENGE	R
AABCA	B	EETLE		AABCDB	BA	TTERIE	S
AABCA	A	NNOUN	CE	AABCDBA	SU	RRENDER	
AABCA	F	OOTHO	LE	AABCDBABD	SU	RRENDERED	
AABCA	CA	RRIER		AABCDBC	CO	MMANDAN	T
AABCA	A	SSETS		AABCDBD	O	FFENDED	
AABCA	I	SSUES		AABCDBEC	BA	LLISTICS	
AABCADEC	CO	MMITMENT		AABCDC	E	FFICAC	Y
AABCADEC	A	TTENTION		AABCDD	A	DDRESS	
AABCADEFEA	A	NNOUNCEMEN	T	AABCDD	I	LLNESS	
AABCB	SCR	EENIN	G	AABCDDCA	A	DDRESSED	
AABCB	SU	FFERE	D	AABCDDCD	A	DDRESSES	
AABCB	DI	FFERE	NT	AABCDEB	CO	MMUNIQU	E
AABCB	O	FFICI	AL	AABCDEB	TR	OOPSHIP	

Table D-3 (~~C~~). List of words used in military text arranged alphabetically according to word pattern (U)--Continued

MISCELLANEOUS PATTERNS– Continued

AABCDEB	A	SSEMBLE		ABA	GROUN	DED	
AABCDEBC	TR	OOPSHIPS		ABA	GUAR	DED	
AABCDEC	CO	MMANDIN	G	ABA	INVA	DED	
AABCDECB	BA	TTLEFIEL	D	ABA	LAN	DED	
AABCDED	CO	MMANDED		ABA	RAI	DED	
AABCDEDFC	A	MMUNITION		ABA	WOUN	DED	
AABCDEE	CO	MMANDEE	R	ABA		DID	
AABCDEFA	R	EENLISTE	D	ABA	IC	EBE	RG
AABCDEFA	I	RREGULAR		ABA	PR	ECE	DING
AABCDEFB	O	FFENSIVE		ABA	R	ECE	IPT
AABCDEFBA	A	SSEMBLIES		ABA	CR	EDE	NTIAL
AABCDEFC	A	LLOTMENT		ABA	F	EDE	RAL
AABCDEFC	C	OOPERATE		ABA	D	EFE	AT
AABCDEFD	I	LLUSTRAT	E	ABA	D	EFE	CT
AABCDEFD	A	SSIGNMEN	T	ABA	D	EFE	R
AABCDEFDGA	A	SSIGNMENTS		ABA	SI	EGE	
AABCDEFGA	C	OOPERATIO	N	ABA	R	EJE	CT
AABCDEFGABF	R	EENLISTMENT		ABA	S	ELE	CT
AABCDEFGD	BA	TTLESHIPS		ABA	T	ELE	GRAM
AABCDEFGDAE	C	OORDINATION		ABA		ELE	VATION
AABCDEFGDE	A	PPOINTMENT		ABA	SCH	EME	
ABA		AGA	IN	ABA	R	EME	DY
ABA		AGA	INST	ABA	DISPLAC	EME	NT
ABA	C	ALA	MITY	ABA	PLAC	EME	NT
ABA		ALA	RM	ABA		ENE	MY
ABA	S	ALA	RY	ABA	G	ENE	RAL
ABA	D	AMA	GE	ABA	R	EPE	L
ABA	M	ANA	GE	ABA	H	ERE	
ABA	C	ANA	L	ABA	SPH	ERE	
ABA		ANA	LYZE	ABA	TH	ERE	
ABA	J	APA	N	ABA	W	ERE	
ABA	P	ARA	CHUTE	ABA	WH	ERE	
ABA	P	ARA	DE	ABA	CONQU	ERE	D
ABA	SEP	ARA	TION	ABA	COV	ERE	D
ABA	F	ATA	L	ABA	TH	ESE	
ABA	N	AVA	L	ABA	PR	ESE	NT
ABA	N	AVA	LFORCES	ABA	D	ESE	RT
ABA	C	AVA	LRY	ABA	COMPL	ETE	
ABA	EXC	AVA	TION	ABA	KILOM	ETE	R
ABA		AWA	IT	ABA	M	ETE	R
ABA		AWA	RD	ABA	P	ETE	R
ABA		AWA	Y	ABA	D	EVE	LOP
ABA	PRO	BAB	LE	ABA	S	EVE	N
ABA	PRO	BAB	LY	ABA	S	EVE	NTH
ABA	BI	CYC	LE	ABA	S	EVE	NTY
ABA		CYC	LONE	ABA	S	EVE	RAL
ABA	BLOCKA	DED		ABA		EVE	RY

Table D-3 (Ø). List of words used in military text arranged alphabetically according to word pattern (U)--Continued

MISCELLANEOUS PATTERNS–Continued

ABA		EYE	
ABA		FIF.	TH
ABA		FIF	TY
ABA	EIG	HTH	
ABA	L	IAI	SON
ABA	PROH	IBI	T
ABA	SERV	ICI	NG
ABA	RA	IDI	NG
ABA	R	IDI	NG
ABA	R	IGI	D
ABA	F	ILI	NG
ABA	M	ILI	TARY
ABA	MOB	ILI	ZE
ABA	S	IMI	LAR
ABA	L	IMI	T
ABA	PROX	IMI	TY
ABA	F	INI	SH
ABA	F	IRI	NG
ABA	RET	IRI	NG
ABA	W	IRI	NG
ABA	V	ISI	BLE
ABA	D	ISI	NFECT
ABA	ADV	ISI	NG
ABA	DEC	ISI	ON
ABA	V	ISI	T
ABA	V	ISI	TOR
ABA	POL	ITI	CS
ABA	CR	ITI	QUE
ABA	POS	ITI	VE
ABA		MEM	ORIAL
ABA		NAN	
ABA	DOMI	NAN	CE
ABA	ORD	NAN	CE
ABA	DOMI	NAN	T
ABA		NIN	E
ABA		NIN	ETY
ABA	MOR	NIN	G
ABA		NIN	TH
ABA		OBO	E
ABA	C	OLO	N
ABA	SEMIC	OLO	N
ABA	C	OLO	RS
ABA	AUT	OMO	BILE
ABA	PR	OMO	TE
ABA	H	ONO	R
ABA	VIG	ORO	US
ABA	M	OTO	R
ABA	M	OTO	RIZED
ABA	PR	OVO	ST
ABA		PIP	E
ABA		POP	ULATED
ABA	LIB	RAR	Y
ABA	AI	RDR	OME
ABA	CA	RTR	IDGE
ABA	D	RYR	UN
ABA	DI	SAS	TER
ABA	CA	SES	
ABA	RE	SIS	T
ABA		SUS	PEND
ABA		SYS	TEM
ABA	S	TAT	ION
ABA	DIC	TAT	OR
ABA		TIT	LE
ABA	AL	TIT	UDE
ABA	LA	TIT	UDE
ABA		TOT	AL
ABA		TOT	ALING
ABA	A	UGU	ST
ABA		USU	AL
ABA	F	UTU	RE
ABA	SUR	VIV	ED
ABAA	HAV	EBEE	N
ABAA		SESS	ION
ABAACC		TATTOO	
ABAB	DETRA	ININ	G
ABAB	L	ININ	G
ABAB	M	ININ	G
ABAB	OBTA	ININ	G
ABAB	RA	ININ	G
ABAB	REMA	ININ	G
ABAB	TRA	ININ	G
ABAB	CR	ISIS	
ABAB	WI	THTH	E
ABAB	PAR	TITI	ON
ABACA	C	ANADA	
ABACA	P	ANAMA	
ABACA	PR	ECEDE	
ABACA		ELEME	NT
ABACA		ELEME	NTARY
ABACA		ELEVE	N
ABACA	C	EMETE	RY
ABACA	S	EVERE	
ABACA	AUD	IBILI	TY
ABACA	EXH	IBITI	ON

Table D-3 ~~(C)~~. List of words used in military text arranged alphabetically according to word pattern (U)-- Continued

MISCELLANEOUS PATTERNS–Continued

ABACA	V	ICINI	TY	ABACDA	R	ECEIVE	
ABACA	M	ILITI	A	ABACDA	D	ECEMBE	R
ABACA	FAC	ILITI	ES	ABACDA	D	EFENSE	
ABACA	D	IMINI	SH	ABACDA	R	EJECTE	D
ABACA	L	IMITI	NG	ABACDA	R	ELEASE	
ABACA		INITI	AL	ABACDA	S	ELECTE	D
ABACA	DEF	INITI	ON	ABACEA	R	EMEDIE	S
ABACA	D	IRIGI	BLE	ABACDA		EMERGE	NCY
ABACA	SEM	IRIGI	D	ABACDA		ENEMIE	S
ABACA	REQU	ISITI	ON	ABACDA	R	EPEATE	D
ABACA	C	IVILI	AN	ABACDA	R	EVENUE	
ABACA	D	IVISI	ON	ABACDA	U	NKNOWN	
ABACA	L	OCOMO	TIVE	ABACDA	PR	OMOTIO	N
ABACA	M	ONOPO	LY	ABACDAAC	S	EVENTEEN	
ABACA	PR	OTOCO	L	ABACDAACD	S	EVENTEENT	H
ABACA	CONS	TITUT	E	ABACDAC	D	ESERTER	
ABACA		UNUSU	AL	ABACDAD	D	EFENSES	
ABACADA	V	ISIBILI	TY	ABACDAED		AVAILABL	E
ABACADB	DEF	INITION		ABACDAEEC	N	AVALBATTL	E
ABACADBA	PR	ECEDENCE		ABACDB	F	ATALIT	Y
ABACADC		INITIAT	E	ABACDB	A	NONYMO	US
ABACADD	COMPL	ETENESS		ABACDB	C	OLONEL	
ABACADDA	N	AVALATTA	CK	ABACDBA	TH	EREFORE	
ABACADEC	D	IVISIONS		ABACDC	R	ECEIVI	NG
ABACB	V	ACANC	Y	ABACDC		EVENIN	G
ABACB	COMB	ATANT		ABACDC	DYNA	MOMETE	R
ABACB	C	ATAST	ROPHE	ABACDCA	L	IMITATI	ON
ABACB	D	ETECT	OR	ABACDCCA		NINETEEN	
ABACB	V	ISITS		ABACDCCAD		NINETEENT	H
ABACB		MEMBE	R	ABACDCEA	S	TATEMENT	
ABACBDEC	D	ETENTION		ABACDCECFGHIE	M	ETEOROLOGICAL	
ABACBDEC	R	ETENTION		ABACDD		FIFTEE	N
ABACBDEFGFAG		NONCOMBATANT		ABACDD	FO	RTRESS	
ABACC	R	EBELL	ION	ABACDDEC		FIFTEENT	H
ABACC	N	ECESS	ARY	ABACDEA		ELEVATE	
ABACC	N	ECESS	ITY	ABACDEA	D	EVELOPE	
ABACC	CAR	ELESS		ABACDEA	VER	IFICATI	ON
ABACC	WIR	ELESS		ABACDEA	S	IMILARI	TY
ABACCA	P	ARALLA	X	ABACDEAD		SUSPENSE	
ABACCA	R	EPELLE	D	ABACDEAFGE		SUSPENSION	
ABACCA	T	OMORRO	W	ABACDEB	EXPL	ANATION	
ABACCDACC	CAR	ELESSNESS		ABACDEB	T	OPOGRAP	HIC
ABACCDC	P	ARALLEL		ABACDEBFA	R	ECEPTACLE	
ABACCDEFEA	N	ECESSITATE		ABACDEC		ABANDON	
ABACDA		ALASKA		ABACDEC	D	AMAGING	
ABACDA		ARABIA		ABACDEC	QU	ARANTIN	E
ABACDA	N	AVALBA	SE	ABACDECA	P	ENETRATE	

Table D-3 (~~C~~). List of words used in military text arranged alphabetically according to word pattern (U)--Continued

MISCELLANEOUS PATTERNS–Continued

ABACDECFBA	D	ETERIORATE		ABBA	COMP	ELLE	D
ABACDECFGB	P	ENETRATION		ABBA	SH	ELLE	D
ABACDED	C	APABILI	TY	ABBA	CONF	ERRE	D
ABACDED	M	OTORCYC	LE	ABBA	COMPR	ESSE	D
ABACDED		SUSPICI	ON	ABBA	IMPR	ESSE	D
ABACDEDEDC	G	ENERALALAR	M	ABBA	PR	ESSE	D
ABACDEDFBA		SUSPICIOUS		ABBA	V	ESSE	L
ABACDEDFGA		SUSPICIONS		ABBA	CIGAR	ETTE	
ABACDEFA	D	EFECTIVE		ABBA	B	ETTE	R
ABACDEFA	D	EFENSIVE		ABBA	L	ETTE	R
ABACDEFA	T	ELEPHONE		ABBA	D	IFFI	CULT
ABACDEFA	D	ETERMINE		ABBA	W	ILLI	AM
ABACDEFA	D	EVELOPME	NT	ABBA	F	ILLI	NG
ABACDEFA		EXERCISE		ABBA	K	ILLI	NG
ABACDEFAF		EXERCISES		ABBA	REF	ILLI	NG
ABACDEFB		DEDICATE		ABBA	SW	IMMI	NG
ABACDEFB		ENEMYTAN	KS	ABBA	SH	IPPI	NG
ABACDEFC		DEDICATI	ON	ABBA	M	ISSI	NG
ABACDEFCDFE	V	ETERINARIAN		ABBA	ADM	ISSI	ON
ABACDEFCFD		ELECTRICIT	Y	ABBA	M	ISSI	ON
ABACDEFD		SUSPECTE	D	ABBA	PERM	ISSI	ON
ABACDEFDF		SUSPENDED		ABBA	F	ITTI	NG
ABACDEFE		ANALYSIS		ABBA	AFTER	NOON	
ABACDEFGA		EXECUTIVE		ABBA		NOON	
ABACDEFGB		POPULATIO	N	ABBA	F	OLLO	W
ABACDEFGBA		ENEMYPLANE	S	ABBA	C	OMMO	N
ABACDEFGBA	S	EVENTYFIVE		ABBA		OPPO	SE
ABACDEFGBEHF	D	ETERMINATION		ABBA		OPPO	SITE
ABACDEFGDHH	G	ENERALSTAFF		ABBA	B	OTTO	M
ABACDEFGE		MEMORANDA		ABBAB	B	AGGAG	E
ABACDEFGHA		MEMORANDUM		ABBAB	WITN	ESSES	
ABACDEFGHIA	D	ECENTRALIZE		ABBACA		APPARA	TUS
ABBA		AFFA	IR	ABBACA	L	ETTERE	D
ABBA		APPA	RENT	ABBACB	V	ESSELS	
ABBA		APPA	RENTLY	ABBACDA	M	ESSENGE	R
ABBA	B	ARRA	CKS	ABBACDA		EFFECTE	D
ABBA	B	ARRA	GE	ABBACDB	M	ISSIONS	
ABBA		ARRA	NGE	ABBACDEA		IRRIGATI	ON
ABBA		ASSA	ULT	ABBACDEDA		OPPOSITIO	N
ABBA	P	ASSA	GE	ABBACDEFA		EFFECTIVE	
ABBA	IMP	ASSA	BLE	ABBACDEFA	D	IFFICULTI	ES
ABBA		ATTA	CH	ABBACDEFA		IMMIGRATI	ON
ABBA		ATTA	CK	ABBACDEFCD		ILLITERATE	
ABBA		ATTA	IN	ABBACDEFDB		ATTAINMENT	
ABBA	B	ATTA	LION	ABBACDEFEC		ARRANGEMEN	T
ABBA	IN	DEED		ABBACDEFGB		ATTACHMENT	
ABBA		EFFE	CT	ABBCA		ANNUA	L

Table D-3 (~~C~~). List of words used in military text arranged alphabetically according to word pattern (U)--Continued

MISCELLANEOUS PATTERNS–Continued

ABBCA		APPEA	R	ABBCDEAFBGBC		REENFORCEMEN	T
ABBCA	DIS	APPEA	R	ABBCDEAFD		APPLICATI	ON
ABBCA	C	ARRIA	GE	ABBCDEAFEC		ASSOCIATIO	N
ABBCA	S	ETTLE		ABBCDEAFGC		ACCEPTABLE	
ABBCA		ISSUI	NG	ABBCDEAFGC		ALLEGIANCE	
ABBCA	FOUR	TEENT	H	ABBCDEAFGHF	C	ORRESPONDIN	G
ABBCA	SIX	TEENT	H	ABBCDEFGA		ACCIDENTA	L
ABBCA	CHA	UFFEU	R	ABBCDEFGA		APPROXIMA	TE
ABBCA	S	URROU	ND	ABBCDEFGA		OCCUPATIO	N
ABBCADAEFC		APPEARANCE		ABBCDEFGBA		IRREGULARI	TY
ABBCADAEFC	DIS	APPEARANCE		ABBCDEFGBAHAC		IRREGULARITIE	S
ABBCADC		APPEARE	D	ABBCDEFGEA		ILLUSTRATI	ON
ABBCBBDA	P	OSSESSIO	N	ABBCDEFGHAD	C	OMMENDATION	
ABBCBDA		ASSISTA	NCE	ABCA	P	ACKA	GE
ABBCBDAED		ASSISTANT		ABCA	EV	ACUA	TING
ABBCCDAB		ASSOONAS		ABCA	EV	ACUA	TION
ABBCDA		ALLOWA	NCE	ABCA	R	ADIA	L
ABBCDA		APPROA	CH	ABCA	R	ADIA	TE
ABBCDA		ARRIVA	L	ABCA		ADJA	CENT
ABBCDA		ASSURA	NCE	ABCA	GR	ADUA	L
ABBCDA	M	ESSAGE		ABCA		ADVA	NCE
ABBCDA		ILLUMI	NATE	ABCA	DI	AGRA	M
ABBCDAB	M	ESSAGES		ABCA	EV	ALUA	TION
ABBCDAB	C	ORRIDOR		ABCA		ALWA	YS
ABBCDAEA	B	ELLIGERE	NT	ABCA	C	AMPA	IGN
ABBCDAEFC		ALLOCATIO	N	ABCA	M	ANDA	TE
ABBCDAEFC		IMMEDIATE		ABCA	M	ANUA	L
ABBCDAEFGAE		ILLUMINATIN	G	ABCA	J	ANUA	RY
ABBCDAEFGAHE		ILLUMINATION		ABCA	C	ANVA	S
ABBCDAEFGAHE	D	ISSEMINATION		ABCA	CH	APLA	IN
ABBCDBCEA		APPROPRIA	TE	ABCA	C	APTA	IN
ABBCDCA		EFFICIE	NT	ABCA		AREA	
ABBCDCA	C	OLLISIO	N	ABCA	DEB	ARKA	TION
ABBCDCAED		EFFICIENC	Y	ABCA	EMB	ARKA	TION
ABBCDCAED	C	OLLISIONS		ABCA		ASIA	
ABBCDCEFA		ADDITIONA	L	ABCA	CO	ASTA	L
ABBCDDCA	C	OMMISSIO	N	ABCA	C	ASUA	L
ABBCDDCA	C	OMMISSIO	NER	ABCA	C	ASUA	LTY
ABBCDDCEAFGC		ACCOMMODATIO	N	ABCA		AVIA	TOR
ABBCDEA		ACCOMPA	NY	ABCA		BARB	ED
ABBCDEA		APPROVA	L	ABCA		BOMB	
ABBCDEA		ASSOCIA	TE	ABCA		BOMB	ARD
ABBCDEA	SH	ELLFIRE		ABCA		BOMB	ER
ABBCDEA	T	ERRIBLE		ABCA	LIGHT	BOMB	ER
ABBCDEAFB		ACCORDANC	E	ABCA		BRIB	E
ABBCDEAFB		REENFORCE		ABCA		BULB	
ABBCDEAFBC		ACCEPTANCE		ABCA		CANC	EL

Table D-3 ~~(C)~~. List of words used in military text arranged alphabetically according to word pattern (U)--Continued

MISCELLANEOUS PATTERNS– Continued

ABCA		CHEC	K
ABCA		CIRC	LE
ABCA		CIRC	ULATE
ABCA		CONC	EAL
ABCA		CONC	LUDE
ABCA	HUN	DRED	
ABCA	L	EADE	R
ABCA		EAGE	R
ABCA	M	EAGE	R
ABCA	S	EAME	N
ABCA	ST	EAME	R
ABCA	N	EARE	ST
ABCA	C	EASE	
ABCA	GR	EASE	
ABCA	INCR	EASE	D
ABCA	L	EAVE	
ABCA		ECHE	LON
ABCA	WR	ECKE	D
ABCA	INF	ECTE	D
ABCA		EDGE	
ABCA	S	EIZE	
ABCA	R	ELIE	F
ABCA	H	ELPE	R
ABCA	TW	ELVE	
ABCA	NOV	EMBE	R
ABCA	ABS	ENCE	
ABCA	LIC	ENSE	
ABCA	C	ENTE	R
ABCA		ENTE	R
ABCA		ENVE	LOP
ABCA	R	EQUE	ST
ABCA	FI	ERCE	
ABCA	S	ERGE	ANT
ABCA	MAT	ERIE	L
ABCA	REV	ERSE	
ABCA	OBS	ERVE	
ABCA	R	ESPE	CT
ABCA	W	ESTE	RLY
ABCA	W	ESTE	RN
ABCA		ETHE	R
ABCA	MAN	EUVE	R
ABCA	R	EVIE	W
ABCA		EXCE	PT
ABCA		EXPE	CT
ABCA		EXPE	ND
ABCA		EXTE	ND
ABCA		GAUG	E
ABCA		GEOG	RAPHIC
ABCA	FOR	GING	
ABCA	W	HICH	
ABCA		HIGH	
ABCA		HIGH	ER
ABCA		HIGH	EST
ABCA	V	ICTI	M
ABCA	M	IDNI	GHT
ABCA	DR	IFTI	NG
ABCA	L	IFTI	NG
ABCA	S	IGNI	FY
ABCA	BU	ILDI	NG
ABCA		INDI	CATE
ABCA		INDI	RECT
ABCA	DESCR	IPTI	ON
ABCA	L	IQUI	D
ABCA	A	IRFI	ELD
ABCA		REPR	ISAL
ABCA	M	ISFI	RE
ABCA	F	ISHI	NG
ABCA	W	ITHI	N
ABCA	FUE	LOIL	
ABCA		MAIM	
ABCA	LA	NDIN	G
ABCA	I	NFAN	TRY
ABCA	CO	NFIN	E
ABCA	U	NION	
ABCA	SU	NKEN	
ABCA	FLA	NKIN	G
ABCA	I	NLAN	D
ABCA	I	NTEN	D
ABCA	CO	NTIN	UAL
ABCA	CO	NTIN	UE
ABCA	I	NVEN	T
ABCA		OCTO	BER
ABCA	D	OCTO	R
ABCA	F	OGHO	RN
ABCA	P	OISO	N
ABCA	C	OMPO	SED
ABCA	C	ONVO	Y
ABCA	EN	ORMO	US
ABCA	EXPL	OSIO	N
ABCA		PUMP	
ABCA		PURP	OSE
ABCA	HA	RBOR	
ABCA	AI	RBOR	NE
ABCA	MU	RDER	

Table D-3 (~~C~~). List of words used in military text arranged alphabetically according to word pattern (U)--Continued

MISCELLANEOUS PATTERNS– Continued

ABCA	O	RDER	
ABCA	O	RDER	S
ABCA		REAR	
ABCA		RECR	UIT
ABCA	COU	RIER	
ABCA	P	RIOR	
ABCA	SUPE	RIOR	
ABCA	A	RMOR	
ABCA	A	RMOR	Y
ABCA	P	ROGR	AM
ABCA	MO	RTAR	
ABCA	QUA	RTER	
ABCA	QUA	RTER	S
ABCA	FEB	RUAR	Y
ABCA	FO	RWAR	D
ABCA	CEN	SORS	HIP
ABCA		SUNS	ET
ABCA	IMPOR	TANT	
ABCA	S	TART	
ABCA	PRO	TECT	
ABCA		TENT	
ABCA		TENT	H
ABCA	PRO	TEST	
ABCA		TEXT	
ABCA		THAT	
ABCA	S	TRAT	EGIC
ABCA	S	TRAT	EGY
ABCA	D	UGOU	T
ABCA		UNSU	ITABLE
ABCA	P	URSU	E
ABCA	P	URSU	IT
ABCA	O	UTGU	ARD
ABCAA	D	ECREE	
ABCAA	D	EGREE	
ABCAA	B	ETWEE	N
ABCAA	DI	SCUSS	
ABCAA	A	SPOSS	IBLE
ABCAAB	P	ONTOON	
ABCAAB		THATTH	E
ABCAACDEB	P	REARRANGE	D
ABCAB	W	ARFAR	E
ABCAB	S	ECREC	Y
ABCAB	OBS	ERVER	
ABCAB	W	HETHE	R
ABCAB	B	INDIN	G
ABCAB	F	INDIN	G
ABCAB	S	INKIN	G
ABCAB	PA	INTIN	G
ABCAB	PR	INTIN	G
ABCAB	I	NTENT	
ABCAB	P	ONTON	
ABCAB	C	ORPOR	AL
ABCAB		RECRE	ATION
ABCAB	P	RIORI	TY
ABCAB	SUPE	RIORI	TY
ABCAB	DI	SEASE	
ABCAB	PRO	TECTE	D
ABCAB	PRO	TESTE	D
ABCAB	O	UTPUT	
ABCABA	INT	ERFERE	
ABCABB	D	ISMISS	
ABCABB	D	ISMISS	AL
ABCABC		THATHA	VE
ABCABCA		ENTENTE	
ABCABDA	S	ENTENCE	
ABCABDB		REPRESE	NT
ABCABDBEFGFHIB		REPRESENTATIVE	
ABCABDBEFGFHIED		REPRESENTATIONS	
ABCABDC		RETREAT	
ABCABDED	M	ANGANESE	
ABCABDEFA	C	ORPORATIO	N
ABCABDEFGHD		RECREATIONA	L
ABCAC		ARMAM	ENT
ABCAC	N	EARER	
ABCAC		PROPO	SE
ABCAC	P	RAIRI	E
ABCAC	PRO	TESTS	
ABCACA	D	IETITI	AN
ABCACB	O	RDERED	
ABCACBDEC		PROPORTIO	N
ABCACDEFD		PROPOSALS	
ABCADA		ALMANA	C
ABCADA	R	ELIEVE	
ABCADA	C	ENTERE	D
ABCADA	B	ESIEGE	D
ABCADA	R	EVIEWE	D
ABCADAB	CO	NTINENT	AL
ABCADAC	S	EALEVEL	
ABCADAC		INDIVID	UAL
ABCADAEC		IGNITION	
ABCADAEFB		TENTATIVE	
ABCADAEFC	S	IGNIFICAN	T
ABCADAEFCE	S	IGNIFICANC	E
ABCADAEFGHF		SUBSISTENCE	

Table D-3 ~~(C)~~. List of words used in military text arranged alphabetically according to word pattern (U)--Continued

MISCELLANEOUS PATTERNS- Continued

ABCADB		ATLANT	IC	ABCADEAB	CO	NTINGENT	
ABCADB		BRIBER	Y	ABCADEAE		EXPENDED	
ABCADB		CIRCUI	T	ABCADEAE		EXPENSES	
ABCADB	W	EDNESD	AY	ABCADEAE		EXTENDED	
ABCADB	LOG	ISTICS		ABCADEAFA		ELSEWHERE	
ABCADB	EXPL	OSIONS		ABCADEAFGA		EXPERIENCE	
ABCADB		PREPAR	ING	ABCADEB	C	ENTERIN	G
ABCADB	IM	PROPER		ABCADEB		ENTERIN	G
ABCADB		PROPER		ABCADEB	R	ESPECTS	
ABCADBA		INSIGNI	A	ABCADEB		INCIDEN	T
ABCADBC		PREPARE		ABCADEB	M	ISFIRES	
ABCADBCEFCGG		PREPAREDNESS		ABCADEBCE		INCIDENCE	
ABCADBD		PREPARA	TION	ABCADEC	M	ANDATED	
ABCADBEFD		CIRCUITOU	S	ABCADEC	S	ECRETAR	Y
ABCADC	R	ADIATI	ON	ABCADEC	GYR	OSCOPIC	
ABCADC	ST	ANDARD		ABCADECA		REARGUAR	D
ABCADC	V	ARIATI	ON	ABCADECAFD	D	ISTINCTION	
ABCADC		ASIATI	C	ABCADECFC		CONCERNIN	G
ABCADC		AVIATI	ON	ABCADEDA	CO	NFINEMEN	T
ABCADC	R	EVIEWI	NG	ABCADEDAFB		INVITATION	
ABCADC		EXTENT		ABCADEDBD		SUBSTITUT	E
ABCADC	I	NVENTE	D	ABCADEDBDE		SUBSTITUTI	ON
ABCADC		TACTIC	S	ABCADEDC	LI	EUTENANT	
ABCADC	S	TARTER		ABCADEDFGA		ENTERPRISE	
ABCADC		ZIGZAG		ABCADEDFGDBC		CONCILIATION	
ABCADCA	CO	NVENIEN	T	ABCADEDFGFB		ENTERPRISIN	G
ABCADCB	CO	NDENSED		ABCADEE	P	ROGRESS	
ABCADCB		TACTICA	L	ABCADEEBFGHC		CANCELLATION	
ABCADCEFBGABC		ENTERTAINMENT		ABCADEED		CANCELLE	D
ABCADCEFGED		CONCENTRATE		ABCADEEFBC		CONCESSION	
ABCADCEFGEHC		CONCENTRATIN	G	ABCADEEFGD	P	ROGRESSIVE	
ABCADCEFGEHBC		CONCENTRATION		ABCADEFA		ECHELONE	D
ABCADD	D	EPRESS	ION	ABCADEFA		ENVELOPE	
ABCADD		EXCESS		ABCADEFA		EXPEDITE	
ABCADD	D	ISTILL		ABCADEFA		EXPERIME	NT
ABCADD	P	OSTOFF	ICE	ABCADEFAB		INDICATIN	G
ABCADD	B	OYCOTT		ABCADEFAB	D	ISTINGUIS	H
ABCADDA		AMBASSA	DOR	ABCADEFABGADE	D	ISTINGUISHING	
ABCADDA		EXPELLE	D	ABCADEFAGB		INDICATION	
ABCADDECCFA		UNSUCCESSFU	L	ABCADEFB		ADVANCED	
ABCADDEFA		EXCESSIVE		ABCADEFBA	EXT	RAORDINAR	Y
ABCADEA		ADVANTA	GE	ABCADEFC		BOMBARDM	ENT
ABCADEA		ADVANTA	GEOUS	ABCADEFC		CIRCULAR	
ABCADEA	D	ECREASE		ABCADEFC	U	NTENABLE	
ABCADEA	S	EPTEMBE	R	ABCADEFCGHB		RETROACTIVE	
ABCADEA	R	EQUESTE	D	ABCADEFD		ADVANCIN	G
ABCADEA	D	ISCIPLI	NE	ABCADEFD		EXTENDIN	G

Table D-3 (~~C~~). List of words used in military text arranged alphabetically according to word pattern (U)--Continued

MISCELLANEOUS PATTERNS– Continued

ABCADEFD		EXTERIOR	
ABCADEFE		CONCRETE	
ABCADEFE		EXPEDITI	NG
ABCADEFE		EXPEDITI	ON
ABCADEFE		OBSOLETE	
ABCADEFE	G	ONIOMETE	R
ABCADEFE		PURPOSES	
ABCADEFE		RECRUITI	NG
ABCADEFEA	C	COMPOSITIO	N
ABCADEFGA		EXPENSIVE	
ABCADEFGA		EXTENSIVE	
ABCADEFGAF		ECHELONMEN	T
ABCADEFGB	C	ASUALTIES	
ABCADEFGB		CIRCULATI	ON
ABCADEFGBC		CONCLUSION	
ABCADEFGC		INDICATED	
ABCADEFGC	S	TRATEGICA	L
ABCADEFGD		EXTENSION	
ABCADEFGDC		CONCEALMEN	T
ABCADEFGE		REPRISALS	
ABCADEFGF		BOMBARDED	
ABCADEFGHAB	C	ONFORMATION	
ABCADEFGHCA		EXTERMINATE	
ABCADEFGHCFIG		EXTERMINATION	
ABCADEFGHEIGCF		REORGANIZATION	
ABCADEFGHH	R	ESPECTFULL	Y
ABCADEFGHIAJF		CIRCUMSTANCES	
ABCADEFGHIB		RETROACTIVE	
ABCADEFGHIE		GEOGRAPHICA	L
ABCADEFGHIGBH		CIRCUMSTANTIA	L
ABCBA	COMP	LETEL	Y
ABCBA		AWKWA	RD
ABCBA		CAPAC	ITY
ABCBA	PA	CIFIC	
ABCBA	SPA	CIFIC	
ABCBA	HIN	DERED	
ABCBA		DIVID	E
ABCBA		GARAG	E
ABCBA	C	ITATI	ON
ABCBA		LEVEL	
ABCBA	P	REFER	
ABCBA		REFER	
ABCBA	P	RESER	VATION
ABCBA		RESER	VATION
ABCBA		TAXAT	ION
ABCBA	HOS	TILIT	Y
ABCBA	U	TILIT	Y
ABCBA	AC	TIVIT	Y
ABCBAA	U	SELESS	
ABCBAAB	P	REFERRE	D
ABCBAB		DIVIDI	NG
ABCBAB	AC	TIVITI	ES
ABCBABDEB	P	REFERENCE	
ABCBABDEB		REFERENCE	
ABCBADA		MINIMUM	
ABCBADB	P	RESERVE	
ABCBADB		RESERVE	
ABCBADB		REVERSE	
ABCBADBC		RESERVES	
ABCBADEB	SPE	CIFICATI	ON
ABCBCDBA		REMEMBER	
ABCBDA		DEFEND	
ABCBDA		DEPEND	
ABCBDA	MU	NITION	S
ABCBDA		RESEAR	CH
ABCBDA		STATES	
ABCBDA		STATUS	
ABCBDA	IN	TEREST	
ABCBDAB		DEFENDE	R
ABCBDAB	E	NGAGING	
ABCBDABA		DEFENDED	
ABCBDABD		DEPENDEN	T
ABCBDABDEA		STATISTICS	
ABCBDAEFGB		DEPENDABLE	
ABCBDAEFGHG		DEPENDABILI	TY
ABCBDCBA		PARAGRAP	H
ABCBDDBA		DEFERRED	
ABCBDEA	E	CONOMIC	
ABCBDEA		DAMAGED	
ABCBDEA	PO	LITICAL	
ABCBDEAEC		MANAGEMEN	T
ABCBDEBA		DEFEATED	
ABCBDEBA		DESERTED	
ABCBDEBA		RECEIVER	
ABCBDEBA		REPEATER	
ABCBDEFA		REJECTOR	
ABCBDEFA		STATIONS	
ABCBDEFBA		DEVELOPED	
ABCBDEFGA	R	ESISTANCE	
ABCBDEFGBA		DETERMINED	
ABCBDEFGHFA		DISINFECTED	
ABCBDEFGHIJBA		DECENTRALIZED	
ABCCA		LITTL	E
ABCCA		PASSP	ORT

Table D-3 (C). List of words used in military text arranged alphabetically according to word pattern (U)--Continued

MISCELLANEOUS PATTERNS-Continued

ABCCA	S	TREET		ABCDA	M	ARTIA	L
ABCCABDEC	C	ROSSROADS		ABCDA	E	ASTWA	RD
ABCCBADED		MILLIMETE	R	ABCDA	N	ATURA	L
ABCCBCA	BE	GINNING		ABCDA	N	ATURA	LIZE
ABCCBDA	INF	LAMMABL	E	ABCDA	TE	CHNIC	AL
ABCCDA		COLLEC	T	ABCDA		COUNC	IL
ABCCDA		CORREC	T	ABCDA	R	EACHE	D
ABCCDA	T	RIGGER		ABCDA	L	EAGUE	
ABCCDA		RUBBER		ABCDA		EASTE	RLY
ABCCDA		RUNNER		ABCDA		EASTE	RN
ABCCDA		SPOOLS		ABCDA	W	EATHE	R
ABCCDA		SPOONS		ABCDA	H	EAVIE	R
ABCCDA		SUGGES	T	ABCDA	INS	ECURE	
ABCCDA		SUPPOS	E	ABCDA	S	ECURE	
ABCCDA		TURRET		ABCDA	R	EDUCE	
ABCCDAA		SUCCESS		ABCDA	SCH	EDULE	
ABCCDAAEB		SUCCESSFU	L	ABCDA	B	EFORE	
ABCCDAAEBFF		SUCCESSFUL	Y	ABCDA	R	EFUGE	
ABCCDAAEFD		SUCCESSIVE		ABCDA	R	EFUSE	
ABCCDAB	P	RESSURE		ABCDA	R	EGIME	NT
ABCCDAEC		TERRITOR	Y	ABCDA	R	EGIME	NTAL
ABCCDAED		CORRECTE	D	ABCDA		EITHE	R
ABCCDAEFB		COLLECTIO	N	ABCDA	FUS	ELAGE	
ABCCDAEFB		CORRECTIO	N	ABCDA	D	ELIVE	R
ABCCDAEFBC		CONNECTION		ABCDA	GR	ENADE	
ABCCDAEFC		CONNECTIN	G	ABCDA		ERASE	
ABCCDAEFDGG		CORRECTNESS		ABCDA	OP	ERATE	
ABCCDEA		GASSING		ABCDA	R	ESCUE	
ABCCDEA		GETTING		ABCDA	PR	ESIDE	NT
ABCCDEA	ST	RAGGLER		ABCDA	R	ESUME	
ABCCDEA	IN	TERRUPT		ABCDA	D	EVICE	
ABCCDEAB	IN	TERRUPTE	D	ABCDA	D	EVISE	
ABCCDEAD		COMMENCE		ABCDA		GOING	
ABCCDEAD		COMMERCE		ABCDA	T	HOUGH	
ABCCDEADCDE		COMMENCEMEN	T	ABCDA	C	HURCH	
ABCCDEBFGHDA		DISSEMINATED		ABCDA	F	IGHTI	NG
ABCCDEFA		COMMUNIC	ATE	ABCDA		INFLI	CT
ABCCDEFA		SUPPLIES		ABCDA	EXT	INGUI	SH
ABCCDEFAGHFBE		COMMUNICATION		ABCDA		INQUI	RE
ABCCDEFBGHDGAD		CORRESPONDENCE		ABCDA		INQUI	RY
ABCCDEFGA	R	EAPPOINTE	D	ABCDA		INSPI	RE
ABCCDEFGHAFG	R	EAPPOINTEMENT		ABCDA		LOCAL	
ABCDA	S	ABOTA	GE	ABCDA	LAU	NCHIN	G
ABCDA	R	AILWA	Y	ABCDA	CO	NDEMN	
ABCDA		ANIMA	L	ABCDA	MACHI	NEGUN	
ABCDA	S	ANITA	RY	ABCDA		NOTIN	G
ABCDA	M	ARSHA	L	ABCDA	EXPA	NSION	

Table D-3 (~~C~~). List of words used in military text arranged alphabetically according to word pattern (U)--Continued

MISCELLANEOUS PATTERNS–Continued

ABCDA	CO	NTAIN		ABCDABAB		INCLININ	G
ABCDA	MOU	NTAIN		ABCDABC	M	AINTAIN	
ABCDA	I	NTERN	AL	ABCDABC	M	AINTAIN	ED
ABCDA	FRO	NTLIN	E	ABCDABCEFD		PHOSPHORUS	
ABCDA	I	NTREN	CH	ABCDABEFA		ENTRENCHE	D
ABCDA	C	ONTRO	L	ABCDAC	L	ANGUAG	E
ABCDA	H	ORIZO	N	ABCDAC		ANYWAY	
ABCDA		OUTBO	ARD	ABCDAC	GOV	ERNMEN	T
ABCDA		PROMP	T	ABCDAC	I	NSTANT	
ABCDA		RECOR	D	ABCDAC	I	NSTANT	LY
ABCDA		REPOR	T	ABCDAC	DI	SPERSE	
ABCDA		RETUR	N	ABCDAC	RES	TRICTI	ON
ABCDA	P	RIMAR	Y	ABCDAC	PA	TRIOTI	C
ABCDA		RIVER		ABCDACB	CO	NDEMNED	
ABCDA		ROGER		ABCDACDAEFGB	I	NSTANTANEOUS	
ABCDA	FA	RTHER		ABCDACEFDAF		COINCIDENCE	
ABCDA	FU	RTHER		ABCDAD		MOVEME	NT
ABCDA	NO	RTHER	LY	ABCDAD	A	MUSEME	NT
ABCDA		SATIS	FY	ABCDAD		RIGORO	US
ABCDA		SHIPS		ABCDADC	S	ANITATI	ON
ABCDA	WAR	SHIPS		ABCDADEDAFB		INSTITUTION	
ABCDA		THIRT	Y	ABCDADEFEAGC		ANTIAIRCRAFT	
ABCDA	WI	THOUT		ABCDAEA		EXTREME	
ABCDA	EX	TRACT		ABCDAEA		MAXIMUM	
ABCDA		TRACT		ABCDAEAB	SU	ITABILIT	Y
ABCDA	INS	TRUCT		ABCDAEABD	UNI	TEDSTATES	
ABCDA	DES	TRUCT	ION	ABCDAEAE	PAR	ENTHESES	
ABCDA		TWENT	Y	ABCDAEB	F	IGHTING	
ABCDA	B	UREAU		ABCDAEB	S	IGHTING	
ABCDA		WESTW	ARD	ABCDAEB		RAILROA	D
ABCDAA	R	EFUGEE		ABCDAEB		REPORTE	D
ABCDAA	C	ODEBOO	K	ABCDAEB		RETURNE	D
ABCDAA	BU	SINESS		ABCDAEB		TRACTOR	
ABCDAA	DI	STRESS		ABCDAEB	INS	TRUCTOR	
ABCDAA		STRESS		ABCDAEBA		RECORDER	
ABCDAAD	F	ORENOON		ABCDAEBC	DE	TONATION	
ABCDAB		DECIDE		ABCDAEBFBDC	U	NIDENTIFIED	
ABCDAB		DECODE		ABCDAEBFC		SATISFACT	ORY
ABCDAB	SP	EARHEA	D	ABCDAEC		AVERAGE	
ABCDAB	R	EDUCED		ABCDAEC	D	ISTRICT	
ABCDAB		ENTREN	CH	ABCDAEC		OUTPOST	
ABCDAB		ERASER		ABCDAECA		TWENTIET	H
ABCDAB		GEORGE		ABCDAECAB	I	NTERNMENT	
ABCDAB		POSTPO	NE	ABCDAECB	D	ISTRICTS	
ABCDAB		RETIRE		ABCDAECD	L	ABORATOR	Y
ABCDAB	ES	TIMATI	ON	ABCDAECE		OUTPOSTS	
ABCDABA		DECIDED		ABCDAECFD	EX	AMINATION	

Table D-3 (~~C~~). List of words used in military text arranged alphabetically according to word pattern (U)--Continued

MISCELLANEOUS PATTERNS– Continued

ABCDAED	T	RAVERSE	
ABCDAEE		ACTUALL	Y
ABCDAEE		EXPRESS	
ABCDAEE		THIRTEE	N
ABCDAEEFAB		THIRTEENTH	
ABCDAEFA	OV	ERWHELME	D
ABCDAEFAB		INFLICTIN	G
ABCDAEFB	P	RESCRIBE	D
ABCDAEFBE	O	NEHUNDRED	
ABCDAEFC	M	ANUFACTU	RE
ABCDAEFC	PR	ESIDENTI	AL
ABCDAEFC	D	ISTRIBUT	E
ABCDAEFCA	D	ISTRIBUTI	NG
ABCDAEFCA	D	ISTRIBUTI	ON
ABCDAEFD	F	LASHLIGH	T
ABCDAEFD	C	ONTROVER	SY
ABCDAEFD	A	SCENSION	
ABCDAEFD		WINDWARD	
ABCDAEFDB		RESTRICTE	D
ABCDAEFDE		RESTRICTI	ON
ABCDAEFE	PAR	ENTHESIS	
ABCDAEFE		RETURNIN	G
ABCDAEFEGE	RE	SPONSIBILI	TY
ABCDAEFF		REDCROSS	
ABCDAEFGAHB		INSPIRATION	
ABCDAEFGC		REGARDING	
ABCDAEFGD		RESTRAINT	
ABCDAEFGFE	TR	ANSPACIFIC	
ABCDAEFGHC		TWENTYFIVE	
ABCDAEFGHFBC		CONSCRIPTION	
ABCDBA	PR	ACTICA	L
ABCDBA	W	ATERTA	NK
ABCDBA	DIV	EBOMBE	R
ABCDBA		ENGINE	
ABCDBA	S	ENTINE	L
ABCDBA	R	EVOLVE	
ABCDBA	S	ITUATI	ON
ABCDBAA		ENGINEE	R
ABCDBAAEDBC		ENGINEERING	
ABCDBAB		LIABILI	TY
ABCDBAD	RE	TALIATI	ON
ABCDBAEAD	D	ISPOSITIO	N
ABCDBAEBE	U	NEXPENDED	
ABCDBBA		ANTENNA	
ABCDBBA	D	ISCUSSI	ON
ABCDBBDEA	TRA	NSMISSION	
ABCDBCAEB		INTENTION	
ABCDBCEA	A	ERODROME	
ABCDBEA		INCENDI	ARY
ABCDBEA	PR	OTECTIO	N
ABCDBEA	IN	TERCEPT	
ABCDBEAB	IN	TERCEPTE	D
ABCDBEAE	C	ONTINUOU	S
ABCDBEAFB		INVENTION	
ABCDBEAFCDB	QU	ARTERMASTER	
ABCDBEAFD		INCENTIVE	
ABCDBEAFD		INTENSIVE	
ABCDBECA	E	NCIRCLIN	G
ABCDBEFAGABC		ENTANGLEMENT	
ABCDBEFAGEB		TEMPERATURE	
ABCDBEFBA		DECREASED	
ABCDBEFCDAB	C	ONTINUATION	
ABCDBEFGA		YESTERDAY	
ABCDBEFGAB		ARMOREDCAR	
ABCDBEFGBCHIA		DISTINGUISHED	
ABCDBEFGHA	P	ERFORMANCE	
ABCDCA		AIRCRA	FT
ABCDCA		CRITIC	
ABCDCA		CRITIC	AL
ABCDCA	D	EFICIE	NT
ABCDCA		ENGAGE	
ABCDCA	P	OSITIO	N
ABCDCA	PR	OVISIO	N
ABCDCA	FI	REALAR	M
ABCDCAAC		PHILIPPI	NES
ABCDCAB		ANTITAN	K
ABCDCABCA	I	NDEPENDEN	T
ABCDCAC		CRITICI	SE
ABCDCAC		CRITICI	SM
ABCDCAD		OPINION	
ABCDCAEAB		ENGAGEMEN	T
ABCDCAEB	P	OSITIONS	
ABCDCAED	D	EFICIENC	Y
ABCDCAED	PR	OVISIONS	
ABCDCAEFD		CHARACTER	
ABCDCAEFDGHEGA		CHARACTERISTIC	
ABCDCBABC	IN	TERPRETER	
ABCDCBCEA	HO	STILITIES	
ABCDCEA	BRI	DGEHEAD	
ABCDCEA	M	EDICINE	
ABCDCEA	D	EFINITE	
ABCDCEA	S	EPARATE	
ABCDCEA		SURPRIS	E
ABCDCEAFC	QU	ALIFICATI	ON

Table D-3 (~~C~~). List of words used in military text arranged alphabetically according to word pattern (U)--Continued

MISCELLANEOUS PATTERNS– Continued

ABCDCEAFE	P	ERSISTENT	
ABCDCEBA		ELIGIBLE	
ABCDCECA	D	ESTITUTE	
ABCDCECDA	CO	NSTITUTIN	G
ABCDCEFGAB		PHOTOGRAPH	Y
ABCDCEFGCA	DEM	OBILIZATIO	N
ABCDCEFGCA	M	OBILIZATIO	N
ABCDDA	R	ECOMME	ND
ABCDDA	T	OBACCO	
ABCDDA		SHELLS	
ABCDDAB	B	EACHHEA	D
ABCDDAEACBE		INEFFICIENC	Y
ABCDDAEFAF	R	ECOMMENDED	
ABCDDAEFGHICE	R	ECOMMENDATION	
ABCDDEA		DROPPED	
ABCDDEA	AI	RSUPPOR	T
ABCDDEA	A	RTILLER	Y
ABCDDEAEC		COEFFICIE	NT
ABCDDECDFA		SCHOOLHOUS	E
ABCDDEFCGHA	MI	SCELLANEOUS	
ABCDDEFEACGE		CLASSIFICATI	ON
ABCDDEFGGEDBA	R	ECONNAISSANCE	
ABCDEA		AERONA	UTICS
ABCDEA	R	AILHEA	D
ABCDEA		AIRPLA	NE
ABCDEA		AMBULA	NCE
ABCDEA	CO	ASTGUA	RD
ABCDEA	M	ATERIA	L
ABCDEA	S	ATURDA	Y
ABCDEA	C	AUSEWA	Y
ABCDEA	N	AUTICA	L
ABCDEA		BLOCKB	USTER
ABCDEA	ME	CHANIC	
ABCDEA		CHEMIC	AL
ABCDEA		CONDUC	T
ABCDEA		DISLOD	GE
ABCDEA		DOWNED	
ABCDEA	B	ECAUSE	
ABCDEA	D	ECIPHE	R
ABCDEA	D	ECLARE	
ABCDEA	OBJ	ECTIVE	
ABCDEA	L	ECTURE	
ABCDEA	V	EHICLE	S
ABCDEA		ENCODE	
ABCDEA	COMP	ENSATE	
ABCDEA		ENTIRE	
ABCDEA	R	EPLACE	
ABCDEA	R	EPULSE	D
ABCDEA	CONSID	ERABLE	
ABCDEA	INT	ERPOSE	
ABCDEA	S	ERVICE	
ABCDEA		EUROPE	
ABCDEA		EUROPE	AN
ABCDEA		EXCITE	
ABCDEA	T	HROUGH	
ABCDEA		IDENTI	CAL
ABCDEA		IDENTI	FY
ABCDEA		INHABI	TED
ABCDEA	D	IRECTI	ON
ABCDEA		MEDIUM	
ABCDEA	SY	NCHRON	IZE
ABCDEA	JU	NCTION	
ABCDEA	CO	NFIDEN	T
ABCDEA		NOTHIN	G
ABCDEA	E	NTRAIN	
ABCDEA	L	OCATIO	N
ABCDEA	REV	OLUTIO	N
ABCDEA	DEC	ORATIO	N
ABCDEA	T	ORPEDO	
ABCDEA		OVERCO	MING
ABCDEA	T	RAILER	S
ABCDEA	T	RAWLER	
ABCDEA	DI	RECTOR	
ABCDEA		REPAIR	
ABCDEA	NO	RTHWAR	D
ABCDEA	C	RUISER	
ABCDEA	I	SLANDS	
ABCDEA		STRIPS	
ABCDEA		SUNRIS	E
ABCDEA		TARGET	
ABCDEA	NOR	THEAST	
ABCDEA		THREAT	
ABCDEA	NOR	THWEST	
ABCDEA		TWELFT	H
ABCDEA	L	UMINOU	S
ABCDEAA		EIGHTEE	N
ABCDEAAE		SUBMISSI	ON
ABCDEAAFED		EIGHTEENTH	
ABCDEAB		INVADIN	G
ABCDEAB	F	LEXIBLE	
ABCDEAB		NATIONA	L
ABCDEAB		REQUIRE	
ABCDEAB		RESTORE	D
ABCDEAB	OU	TSKIRTS	

Table D-3 ~~(C)~~. List of words used in military text arranged alphabetically according to word pattern (U)--Continued

MISCELLANEOUS PATTERNS– Continued

ABCDEABA		DEMANDED	
ABCDEABD		IMPEDIME	NTA
ABCDEABE	AT	OMICBOMB	
ABCDEABF		REPAIRED	
ABCDEABFB		REQUIREME	NT
ABCDEABFD		NATIONALI	SM
ABCDEABFDC		NATIONALIT	Y
ABCDEABFE		MARKSMANS	HIP
ABCDEABFFGHD		SHARPSHOOTER	
ABCDEAC		AUTOMAT	IC
ABCDEAC	AI	RCONTRO	L
ABCDEACFB		ANTEDATIN	G
ABCDEAD		CONTACT	
ABCDEAD	V	ICTORIO	US
ABCDEAD	C	RUISERS	
ABCDEADFD		THREATENE	D
ABCDEAE		ENCODED	
ABCDEAE	P	ERMANEN	T
ABCDEAE		FORTIFI	ED
ABCDEAE		REQUIRI	NG
ABCDEAEFGC		TRADITIONA	L
ABCDEAFA	R	EPLACEME	NT
ABCDEAFAGE		EXCITEMENT	
ABCDEAFAGHEAID		IDENTIFICATION	
ABCDEAFB		CLERICAL	
ABCDEAFB		INVASION	
ABCDEAFBC		RESOURCES	
ABCDEAFC	DES	IGNATION	
ABCDEAFC	RES	IGNATION	
ABCDEAFC	CO	NFIDENTI	AL
ABCDEAFD	D	IMENSION	
ABCDEAFE		ADJUTANT	
ABCDEAFE		INTERIOR	
ABCDEAFE	I	NFLUENCE	
ABCDEAFF	R	EADINESS	
ABCDEAFGA	D	ECIPHERME	NT
ABCDEAFGAFB		MEDIUMBOMBE	R
ABCDEAFGD		LEGISLATI	ON
ABCDEAFGE	CO	MPARTMENT	
ABCDEAFGEE		SMOKESCREE	N
ABCDEBA		DELAYED	
ABCDEBA	D	ETONATE	
ABCDEBA		INDEMNI	TY
ABCDEBA	D	ISPERSI	ON
ABCDEBA		RECOVER	
ABCDEBA		SURPLUS	
ABCDEBAB		ARBITRAR	Y
ABCDEBAED		ARBITRATI	ON
ABCDEBFA	B	RIGADIER	
ABCDEBFAGA		ENCOUNTERE	D
ABCDEBFCAGBF		INTERNATIONA	L
ABCDEBFDGA		NAVIGATION	
ABCDEBFGAF	H	EADQUARTER	S
ABCDEBFGHA	R	ESPONSIBLE	
ABCDEBFGHBCGIA		NATURALIZATION	
ABCDECA	E	NLISTIN	G
ABCDECA		PRINCIP	AL
ABCDECA		PRINCIP	LE
ABCDECA		SKIRMIS	H
ABCDECAB	I	NTERMENT	
ABCDECAC	I	NTERVENE	
ABCDECACFE	M	AINTENANCE	
ABCDECAFCDA		TRANSATLANT	IC
ABCDECBA		NEGLIGEN	T
ABCDECBA		REVOLVER	
ABCDECBA	P	ROTECTOR	
ABCDECBAFB		NEGLIGENCE	
ABCDECCFA		DISCUSSED	
ABCDECDCAFC	I	NTERFERENCE	
ABCDECFA		ENCIRCLE	
ABCDECFA		EVACUATE	
ABCDECFBA		SEAPLANES	
ABCDECFEA		STANDARDS	
ABCDEDA	N	EWSPAPE	R
ABCDEDA		MARITIM	E
ABCDEDA	CO	NTRABAN	D
ABCDEDA	C	OALITIO	N
ABCDEDA	BA	ROMETER	
ABCDEDA	GY	ROMETER	
ABCDEDA	HYD	ROMETER	
ABCDEDA	HYG	ROMETER	
ABCDEDA	PSYCH	ROMETER	
ABCDEDAB	C	ONDITION	
ABCDEDAC	REC	OGNITION	
ABCDEDAFC	N	EWSPAPERS	
ABCDEDFA		DICTATED	
ABCDEDFA		EXCAVATE	
ABCDEDFA		EXHIBITE	D
ABCDEDFAC		ANTICIPAT	E
ABCDEDFAC		CLEARANCE	
ABCDEDFACDGB		ANTICIPATION	
ABCDEDFCAB		INTERESTIN	G
ABCDEDFCGAHB		INAUGURATION	
ABCDEDFDA		ARTIFICIA	L

Table D-3 ~~(C)~~. List of words used in military text arranged alphabetically according to word pattern (U)--Continued

MISCELLANEOUS PATTERNS– Continued

ABCDEDFDEAB	C	ONSTITUTION		ABCDEFA		SERIOUS	LY
ABCDEDFDGHAIF		CHRONOLOGICAL		ABCDEFA	E	STABLIS	H
ABCDEDFGA	PR	OCLAMATIO	N	ABCDEFA		TONIGHT	
ABCDEDFGA	P	RELIMINAR	Y	ABCDEFAA		EMPLOYEE	
ABCDEDFGABHED		INDETERMINATE		ABCDEFAAF	T	RANSFERRE	D
ABCDEDFGADB	P	RELIMINARIE	S	ABCDEFAAGC	T	RANSFERRIN	G
ABCDEDFGHAGD		ADMINISTRATI	VE	ABCDEFAB		INCLUDIN	G
ABCDEDFGHAGDIE		ADMINISTRATION		ABCDEFAB		RADIOGRA	M
ABCDEEA		ENROLLE	D	ABCDEFAB	P	REMATURE	
ABCDEEA	P	ERSONNE	L	ABCDEFABA		EMPLACEME	NT
ABCDEEA		IMPOSSI	BLE	ABCDEFAC		INTEGRIT	Y
ABCDEEACB	S	IGNALLING		ABCDEFAC	P	RISONERS	
ABCDEEAFDBC		INTELLIGENT		ABCDEFACB	IN	TRODUCTOR	Y
ABCDEEAFDBGD		INTELLIGENCE		ABCDEFACD		ALTERNATE	
ABCDEEDFGBA		RECONNOITER		ABCDEFACGF		ALTERNATIN	G
ABCDEEDFGBAFE		RECONNOITERIN	G	ABCDEFAD		CONTRACT	
ABCDEEFAB		ENROLLMEN	T	ABCDEFAD	D	ESTROYER	
ABCDEEFAB	C	ONFESSION		ABCDEFAD		INTERVIE	W
ABCDEEFAE		EMBASSIES		ABCDEFAD		OPERATOR	
ABCDEEFDGFA		DISAPPEARED		ABCDEFAD	FI	RECONTRO	L
ABCDEEFGCAHB		INTERRUPTION		ABCDEFAD	P	ROCEDURE	
ABCDEFA	C	ABLEGRA	M	ABCDEFADB	D	ESTROYERS	
ABCDEFA		AMERICA	N	ABCDEFADF	T	RANSVERSE	
ABCDEFA	C	AMOUFLA	GE	ABCDEFAE	D	ISCONTIN	UE
ABCDEFA		CHRONIC	AL	ABCDEFAEGHEC	D	ISCONTINUANC	E
ABCDEFA		CONFLIC	T	ABCDEFAF		EXPANDED	
ABCDEFA	DIS	CREPANC	Y	ABCDEFAF	I	MPROVEME	NT
ABCDEFA	S	EABORNE		ABCDEFAFCD	R	ADIOSTATIO	N
ABCDEFA		EMPLOYE	R	ABCDEFAGA		ENCIPHERE	D
ABCDEFA		ENCIPHE	R	ABCDEFAGAB		ENFORCEMEN	T
ABCDEFA		ENFORCE		ABCDEFAGB		AEROPLANE	
ABCDEFA		ENLISTE	D	ABCDEFAGB	D	ETACHMENT	
ABCDEFA	D	EPLOYME	NT	ABCDEFAGB		INFLATION	
ABCDEFA		EQUIPME	NT	ABCDEFAGB		REINFORCE	
ABCDEFA	FIGHT	ERPLANE		ABCDEFAGB		TRAJECTOR	Y
ABCDEFA		ESCORTE	D	ABCDEFAGBDB		REIMBURSEME	NT
ABCDEFA	D	ESCRIBE		ABCDEFAGBHBD		REINFORCEMEN	T
ABCDEFA	J	ETPLANE		ABCDEFAGC		INTERDICT	
ABCDEFA		EXCLUDE		ABCDEFAGCAHB		INTERDICTION	
ABCDEFA		INCLUSI	VE	ABCDEFAGE	D	EPARTMENT	
ABCDEFA		LOGICAL		ABCDEFAGEC	D	EPARTMENTA	L
ABCDEFA	F	ORMATIO	N	ABCDEFAGFD		REGISTRATI	ON
ABCDEFA	T	RANSFER		ABCDEFAGHAB		ENCIPHERMEN	T
ABCDEFA		REGULAR		ABCDEFAGHEBC		CONFISCATION	
ABCDEFA	P	RISONER		ABCDEFAGHFD		INVESTIGATE	
ABCDEFA		SAILORS		ABCDEFAGHFAIB		INVESTIGATION	
ABCDEFA		SECTORS		ABCDEFAGHFAIBE		INVESTIGATIONS	

Table D-3 (C). List of words used in military text arranged alphabetically according to word pattern (U)--Continued

MISCELLANEOUS PATTERNS—Continued

ABCDEFAGHIF	B	REAKTHROUGH	
ABCDEFBA		DECLARED	
ABCDEFBA		DEPARTED	
ABCDEFBA		DEPLOYED	
ABCDEFBA		DEPORTED	
ABCDEFBA		DETACHED	
ABCDEFBA		EMPLOYME	NT
ABCDEFBA		ENTRAINE	D
ABCDEFBA		REGISTER	
ABCDEFBA	P	ROJECTOR	
ABCDEFBAB		MEASUREME	NT
ABCDEFBABGHD		MEASUREMENTS	
ABCDEFBGA		ENDURANCE	
ABCDEFBGBA		DECIPHERED	
ABCDEFCA		ESTIMATE	
ABCDEFCA		NORTHERN	
ABCDEFCAB		ESTIMATES	
ABCDEFCAD	D	OMINATION	
ABCDEFCAGFC		ESTIMATEDAT	
ABCDEFCBA		DETONATED	
ABCDEFCCFA		DISTRESSED	
ABCDEFCEA		DISPERSED	
ABCDEFCGA		ELABORATE	
ABCDEFDA	D	EPARTURE	
ABCDEFDAB	C	USTOMHOUS	E
ABCDEFDBAB		INTERVENIN	G
ABCDEFDBCAGB		INTERVENTION	
ABCDEFDEAB		INTERFERIN	G
ABCDEFDGAB	DEM	ONSTRATION	
ABCDEFDGAHCD		INTERMEDIATE	
ABCDEFDGHA		HYDROGRAPH	IC
ABCDEFEA	R	EINSTATE	
ABCDEFEAB	F	INGERPRIN	T
ABCDEFEAGACE	R	EINSTATEMENT	
ABCDEFEAGDB		CERTIFICATE	
ABCDEFECACD		THERMOMETER	
ABCDEFECAE		CONFERENCE	
ABCDEFEDCGCAHB		INTERPRETATION	
ABCDEFEFA	C	OMPETITIO	N
ABCDEFEGA	D	EMOBILIZE	
ABCDEFEGA	C	OMPUTATIO	N
ABCDEFFA	UN	DERSTOOD	
ABCDEFFA		IMPRESSI	ON
ABCDEFFAGE		IMPRESSIVE	
ABCDEFFEDAGBC		INSTALLATIONS	
ABCDEFFGAB	C	ONGRESSION	AL
ABCDEFGA		DISARMED	
ABCDEFGA	M	ECHANIZE	D
ABCDEFGA	T	ECHNIQUE	
ABCDEFGA	R	ECOGNIZE	
ABCDEFGA		ENFILADE	
ABCDEFGA		EQUALIZE	
ABCDEFGA		EQUIPAGE	
ABCDEFGA		EQUIVALE	NT
ABCDEFGA	D	ESIGNATE	
ABCDEFGA		EXCHANGE	
ABCDEFGA		GROUPING	
ABCDEFGA		GUARDING	
ABCDEFGA		INSECURI	TY
ABCDEFGA	D	IPLOMATI	C
ABCDEFGA	E	NTRUCKIN	G
ABCDEFGA		NUMBERIN	G
ABCDEFGA		OBJECTIO	N
ABCDEFGA		OPERATIO	N
ABCDEFGA		SOLDIERS	
ABCDEFGA	DI	SPATCHES	
ABCDEFGA		WITHDRAW	
ABCDEFGA		WITHDREW	
ABCDEFGAB	D	ESPATCHES	
ABCDEFGAB	U	NDERSTAND	
ABCDEFGAB		WITHDRAWI	NG
ABCDEFGABF		ENLISTMENT	
ABCDEFGAC	I	NSTRUMENT	
ABCDEFGAC	F	OUNDATION	
ABCDEFGACB	I	NSTRUMENTS	
ABCDEFGAD		SOUTHEAST	
ABCDEFGAD		SOUTHWEST	
ABCDEFGADG		SOUTHWESTE	RN
ABCDEFGAEHBC		CONSTRUCTION	
ABCDEFGAFE		IMPRACTICA	BLE
ABCDEFGAG		WITHDRAWA	L
ABCDEFGAHB		INSPECTION	
ABCDEFGAHCGIDE		RECONSTRUCTION	
ABCDEFGBA		DESCRIBED	
ABCDEFGBA		DESTROYED	
ABCDEFGBA		DETRAINED	
ABCDEFGBA		REMAINDER	
ABCDEFGBA		TRANSPORT	
ABCDEFGBACAHGD		TRANSPORTATION	
ABCDEFGBAE		TRANSPORTS	
ABCDEFGBHA		ESTABLISHE	D
ABCDEFGBHIAKC		ESTABLISHMENT	
ABCDEFGCAG		CONFIDENCE	
ABCDEFGCHEA		RANGEFINDER	

Table D-3 ~~(C)~~. List of words used in military text arranged alphabetically according to word pattern (U)--Continued

MISCELLANEOUS PATTERNS–Continued

ABCDEFGDAHB		INSTRUCTION	
ABCDEFGDAHBC		INSTRUCTIONS	
ABCDEFGDBFHA	CE	NTRALIZATION	
ABCDEFGDHAIC		OBSTRUCTIONS	
ABCDEFGDHFAE		ORGANIZATION	
ABCDEFGEA	H	EAVYBOMBE	R
ABCDEFGEHA	D	ESCRIPTIVE	
ABCDEFGFABF	I	NCOMPETENCE	
ABCDEFGFAG	I	NCOMPETENT	
ABCDEFGGAG	H	EAVYLOSSES	
ABCDEFGHA		CONSPIRAC	Y
ABCDEFGHA		DOMINATED	
ABCDEFGHA	C	ENTRALIZE	
ABCDEFGHA		EXCLUSIVE	
ABCDEFGHA		EXPANSIVE	
ABCDEFGHA		EXPLOSIVE	
ABCDEFGHA		MECHANISM	
ABCDEFGHAB	C	ONSUMPTION	
ABCDEFGHADB		INFORMATION	
ABCDEFGHAGC		CONVALESCEN	T
ABCDEFGHBA		DESIGNATED	
ABCDEFGHBA		DESPATCHED	
ABCDEFGHBIKA		DISORGANIZED	
ABCDEFGHCAEB		INTRODUCTION	
ABCDEFGHCAEB	D	ISCREPANCIES	
ABCDEFGHDAB	C	ONFIRMATION	
ABCDEFGHDGCA		NORTHWESTERN	
ABCDEFGHDIKA		REVOLUTIONAR	Y
ABCDEFGHEEHA		COUNTERATTAC	K
ABCDEFGHFA	D	EMONSTRATE	
ABCDEFGHFCAG		AGRICULTURAL	
ABCDEFGHIA		DISPATCHED	
ABCDEFGHIA		OBSERVATIO	N
ABCDEFGHIA		SUBMARINES	
ABCDEFGHIAB	C	ONVERSATION	
ABCDEFGHIAE	C	OMPENSATION	
ABCDEFGHIAF	R	OADJUNCTION	
ABCDEFGHIDAB	C	ONSIDERATION	
ABCDEFGHIFKA		SEARCHLIGHTS	
ABCDEFGHIGBA		DEMONSTRATED	
ABCDEFGHIJDA		SIMULTANEOUS	

Table D–4 (~~C~~). List of general digraphic idiomorphs (U)

			AB	AB				
–G	EN	ER	AL	AL	AR	M–		
		NE	ED	ED				
–P	RO	CE	ED	ED				
–S	UC	CE	ED	ED				
–D	ET	RA	IN	IN	G–			
		–L	IN	IN	G–			
		–M	IN	IN	G–			
	OB	TA	IN	IN	G–			
		QU	IN	IN	E–			
		RA	IN	IN	G–			
	RE	MA	IN	IN	G–			
		SH	IN	IN	G–			
	–T	RA	IN	IN	G–			
		CR	IS	IS				
PO	SI	TI	ON	ON				
		–A	RE	RE	EN	FO	RC	ED
		–A	SU	SU	AL			
		BO	TH	TH	E–			
		WI	TH	TH	E–			
	–P	AR	TI	TI	ON			
	RE	PE	TI	TI	ON			
			VI	VI	D–			

		AB	––	AB		
	–M	AI	NT	AI	N–	
	RE	AR	GU	AR	D–	
		CH	UR	CH		
		DE	CI	DE		
		DE	CO	DE		
		DI	VI	DI	NG	
	SP	EA	RH	EA	D–	
	–R	ED	UC	ED		
–S	CH	ED	UL	ED		
	–B	EE	NN	EE	DE	D–
		EM	BL	EM		
	AM	EN	DM	EN	T–	
CO	NT	EN	TM	EN	T–	
–S	EV	EN	TE	EN		
–S	EV	EN	TE	EN	TH	
		EN	TR	EN	CH	
		ER	AS	ER		

			AB	––	AB		
		TH	ER	EF	ER	EN	CE
		TH	ER	ES	ER	VE	
		WH	ER	EV	ER		
–C	AR	EL	ES	SN	ES	S–	
			GE	OR	GE		
		SC	HO	OL	HO	US	E–
–I	LL	UM	IN	AT	IN	G	
			IN	CL	IN	E–	
	–F	IR	IN	GL	IN	E–	
		MA	IN	TA	IN		
–I	NF	AL	LI	BI	LI	TY	
		–A	ME	ND	ME	NT	
		SO	ME	TI	ME		
		–O	NE	NI	NE		
			NO	TK	NO	WN	
			NO	WK	NO	WN	
–A	PP	OI	NT	ME	NT		
–C	ON	TE	NT	ME	NT		
		–C	OM	PR	OM	IS	E–
		–P	ON	TO	ON		
	–T	HR	OU	GH	OU	T–	
		–N	OW	KN	OW	N–	
			PH	OS	PH	OR	US
			PO	ST	PO	NE	
	TR	OO	PS	HI	PS		
		PA	RA	PH	RA	SE	
		–P	RE	FE	RE	NC	E–
			RE	FE	RE	NC	E–
	–T	HE	RE	FO	RE		
		–P	RE	PA	RE		
			RE	TI	RE		
			RE	VE	RE	NT	
		–C	RO	SS	RO	AD	S–
CA	RE	LE	SS	NE	SS		
		AT	TE	MP	TE	D–	
			TH	AT	TH	E–	
	–F	OR	TH	WI	TH		
–I	NV	ES	TI	GA	TI	ON	
		ES	TI	MA	TI	ON	
	–D	ES	TI	NA	TI	ON	
		AC	TI	VI	TI	ES	
		–H	UM	DR	UM		

Table D–4 (~~C~~). List of general digraphic idiomorphs (U) –Continued

			AB	—	—	AB			
		–P	AN	AM	AC	AN	AL		
			AR	BI	TR	AR	Y–		
			AS	SO	ON	AS			
		AC	CE	PT	AN	CE			
			EM	PL	AC	EM	EN	T–	
–Q	UA	RT	ER	MA	ST	ER			
	–I	NT	ER	PR	ET	ER			
	–A	CC	ES	SO	RI	ES			
			IN	CL	UD	IN	G–		
		–D	IR	EC	TF	IR	E–		
		TO	MO	RR	OW	MO	RN	IN	G–
		PA	NA	MA	CA	NA	L–		
		–I	NT	ER	ME	NT			
		–I	NT	ER	VE	NT	IO	N–	
		CO	NT	IN	GE	NT			
		–C	ON	DI	TI	ON			
	–T	OM	OR	RO	WM	OR	NI	NG	
			RA	DI	OG	RA	M–		
			RE	AS	SU	RE			
		–P	RE	MA	TU	RE			
–D	EF	EN	SI	VE	PO	SI	TI	ON	
		IN	TE	RD	IC	TE	D–		
	QU	AR	TE	RM	AS	TE	R–		
		IN	TE	RP	RE	TE	R–		
		IN	TE	RR	UP	TE	D–		
	–F	OR	TI	FI	CA	TI	ON		

		AB	—	—	—	AB		
		AR	MO	RE	DC	AR		
		EN	FO	RC	EM	EN	T–	
	RE	EN	FO	RC	EM	EN	TS	
		IN	DE	TE	RM	IN	AT	E–
		IN	TE	RE	ST	IN	G–	
		IN	TE	RF	ER	IN	G–	
		IN	TE	RV	EN	IN	G–	
	–I	NC	OM	PE	TE	NC	E–	
	–C	ON	GR	ES	SI	ON	AL	
–D	EM	ON	ST	RA	TI	ON		
	–C	ON	SU	MP	TI	ON		
		PH	OT	OG	RA	PH		
		TH	IR	TE	EN	TH		

	AB	—	—	—	—	AB
–I	NS	TA	LL	AT	IO	NS
–C	ON	CE	NT	RA	TI	ON
–C	ON	FL	AG	RA	TI	ON
–C	ON	SI	DE	RA	TI	ON

	AB	—	AB	AB	
	IN	CL	IN	IN	G–
MA	IN	TA	IN	IN	G–

Table D–5 (~~C~~). List of playfair digraphic idiomorphs (U)

		AB	BA			
	SC	AB	BA	RD		
		AF	FA	BL	E–	
		AF	FA	IR		
	–B	AG	GA	GE		
–H	AW	AI	IA	N–		
		AL	LA	RE	AS	
	–B	AL	LA	ST		
	–F	AL	LA	CY		
IN	ST	AL	LA	TI	ON	S–
–P	AR	AL	LA	X–		
		AP	PA	RA	TU	S–
		AP	PA	RE	L–	
		AP	PA	RE	NT	
		AP	PA	RE	NT	LY
		AR	RA	NG	E–	
		AR	RA	Y–		
	–B	AR	RA	CK	S–	
	–B	AR	RA	GE		
–E	MB	AR	RA	SS	ED	
	–N	AR	RA	TI	ON	
		AS	SA	IL	AN	T–
		AS	SA	UL	T–	
–A	MB	AS	SA	DO	R–	
–I	MP	AS	SA	BL	E–	
	–M	AS	SA	CR	E–	
	–P	AS	SA	GE		
		AT	TA	CH		
		AT	TA	CK		
		AT	TA	IN		
	–B	AT	TA	LI	ON	
	–R	AT	TA	N–		
		BO	OB	YT	RA	P–
	IN	DE	ED			
	–W	EB	BE	D–		
		EF	FE	CT		
		EF	FE	CT	IV	E–
CO	MP	EL	LE	D–		
–E	XC	EL	LE	NC	E–	
–E	XC	EL	LE	NT		
–E	XP	EL	LE	D–		
–I	MP	EL	LE	D–		
	–P	EL	LE	T–		
PR	OP	EL	LE	D–		
–R	EP	EL	LE	D–		

		AB	BA				
	SH	EL	LE	D–			
	–H	EM	ME	DI	N–		
	ST	EM	ME	D–			
	ST	EP	PE	D–			
	AV	ER	RE	D–			
CO	NF	ER	RE	D–			
–I	NT	ER	RE	D–			
–R	EF	ER	RE	D–			
		ES	SE	NC	E–		
		ES	SE	NT	IA	L–	
AD	DR	ES	SE	S–			
–C	OM	PR	ES	SE	D–		
CO	NF	ES	SE	D–			
IM	PR	ES	SE	D–			
	–L	ES	SE	N–			
	–M	ES	SE	NG	ER		
	PR	ES	SE	D–			
PR	OF	ES	SE	D–			
–P	RO	GR	ES	SE	D–		
–S	TR	ES	SE	D–			
–S	TR	ES	SE	S–			
	–V	ES	SE	L–			
WI	TN	ES	SE	S–			
	AB	ET	TE	D–			
–C	IG	AR	ET	TE	S–		
	–B	ET	TE	R–			
	–L	ET	TE	R–			
–E	IG	HT	TH	RE	E–		
	–R	IB	BI	NG			
FO	RB	ID	DI	NG			
	–D	IF	FI	CU	LT		
	–B	IL	LI	ON			
	–F	IL	LI	NG			
	–K	IL	LI	NG			
	–M	IL	LI	ME	TE	R–	
	–M	IL	LI	NG			
	–M	IL	LI	ON			
	SH	IL	LI	NG			
	SP	IL	LI	NG			
	–T	IL	LI	NG			
	–W	IL	LI	AM			
	–W	IL	LI	NG			
		IM	MI	GR	AN	T–	
		IM	MI	GR	AT	IO	N–

Table D–5 (~~C~~). List of playfair digraphic idiomorphs (U) –Continued

			AB	BA				
			IM	MI	NE	NT		
		SW	IM	MI	NG			
	–B	EG	IN	NI	NG			
		SP	IN	NI	NG			
		–W	IN	NI	NG			
		CL	IP	PI	NG			
		SH	IP	PI	NG			
	–S	TR	IP	PI	NG			
			IR	RI	GA	TI	ON	
		–M	IS	SI	NG			
		–M	IS	SI	ON			
	–A	DM	IS	SI	ON			
		EM	IS	SI	ON			
		–H	IS	SI	NG			
	PE	RM	IS	SI	ON			
TR	AN	SM	IS	SI	ON			
		EM	IT	TI	NG			
		–F	IT	TI	NG			
	–S	PL	IT	TI	NG			
	PE	RM	IT	TI	NG			
–A	FT	ER	NO	ON				
	FO	RE	NO	ON				
			NO	ON	TI	ME		
		–F	OL	LO	W–			
		–H	OL	LO	W–			
		–C	OM	MO	N–			
		–C	OM	MO	TI	ON		
PO	SI	TI	ON	NO	RT	HO	F–	
	–R	EC	ON	NO	IT	ER		
			OP	PO	RT	UN	E–	
			OP	PO	RT	UN	IT	Y–
			OP	PO	SE			
			OP	PO	SI	TE		
			OP	PO	SI	TI	ON	
		–C	OR	RO	BO	RA	TE	
		–C	OR	RO	DE			
	–T	OM	OR	RO	W–			
		–B	OT	TO	M–			
		–C	OT	TO	N–			
		CA	RE	ER				
		–S	UC	CU	MB	ED		

			AB	––	BA		
		PR	AC	TI	CA	BL	E–
		PR	AC	TI	CA	L–	
		–T	AC	TI	CA	L–	
	–D	IV	EB	OM	BE	R–	
			EN	GI	NE	ER	
		–G	EN	UI	NE		
	–I	NT	ER	FE	RE		
	–I	NT	ER	FE	RE	NC	E–
	–P	EN	ET	RA	TE		
		–R	EV	OL	VE	R–	
			IN	FI	NI	TE	
		–D	IS	PO	SI	TI	ON
		–S	IT	UA	TI	ON	
		CA	NA	DI	AN		
VE	TE	RI	NA	RI	AN		
		NI	NE	TE	EN		
		NI	NE	TE	EN	TH	
			PE	RC	EP	TI	ON
		–P	RE	MI	ER		
	–S	UR	RE	ND	ER		
	–O	UR	SE	LV	ES		
	TH	EM	SE	LV	ES		
		DE	SE	RV	ES		
		RE	SE	RV	ES		
			SE	RV	ES		

Table D–5 (~~C~~). List of playfair digraphic idiomorphs (U) —Continued

	AB	––	––	BA		
	DE	BA	RK	ED		
	DE	CL	AR	ED		
	DE	FE	ND	ED		
	DE	MA	ND	ED		
	DE	PA	RT	ED		
	DE	PL	OY	ED		
	DE	PO	RT	ED		
	DE	SE	RT	ED		
	DE	TA	CH	ED		
PR	EC	ED	EN	CE		
	EM	PL	OY	ME	NT	
	EN	TR	AI	NE	D–	
	ME	AS	UR	EM	EN	T–
	NE	GL	IG	EN	CE	
	NO	TA	TI	ON		
	PA	RA	GR	AP	H–	
	RE	CE	IV	ER		
	RE	CO	RD	ER		
	RE	GI	ST	ER		
	RE	PE	AT	ER		
	RE	PO	RT	ER		
	RE	VO	LV	ER		
–P	RO	JE	CT	OR		
AS	SE	MB	LI	ES		

	AB	––	––	––	BA	
	DE	SE	CR	AT	ED	
	DE	SI	GN	AT	ED	
	DE	SP	AT	CH	ED	
	EN	EM	YP	LA	NE	S–
–D	ET	ER	IO	RA	TE	
–S	EV	EN	TY	FI	VE	
	IR	RE	GU	LA	RI	TY
	NO	MI	NA	TI	ON	
	SU	SP	IC	IO	US	

AB	––	––	––	––	BA
DE	MO	NS	TR	AT	ED
NO	TI	FI	CA	TI	ON

Table D–6 (₵). List of four–square digraphic idiomorphs (U)

(Grouped by number of significant letters in the idiomorphic pattern)

TWO LETTERS

	A–	A–	
B LO CK	AD	ED	
I NV	AD	ED	
D	AM	AG	E
CO MM	AN	DS	
I SL	AN	DS	
A IR PL	AN	ES	
E NE MY PL	AN	ES	
DE SI GN	AT	ED	
E ST IM	AT	ED	
I ND IC	AT	ED	
C	AV	AL	RY
N	AV	AL	
P RO	CE	DU	RE
ME	CH	AN	IZ ED
IM ME	DI	AT	EL Y
WI TH	DR	AW	
WI TH	DR	EW	
	EM	ER	GE NC Y
L IE UT	EN	AN	T
	FI	FT	EE N
	FI	FT	H
	FI	FT	Y
BR ID	GE	HE	AD
V	IC	IN	IT Y
W	IT	HD	RA W
A DD	IT	IO	NA L
A MM UN	IT	IO	N
CO ND	IT	IO	N
RE CO GN	IT	IO	N
E	LE	ME	NT
	MI	LI	TA RY
	MI	NI	MU M
	NI	NT	H
P	OI	NT	
T	OM	OR	RO W
	PO	NT	ON

	A–	A–	
	RE	QU	ES T
	RE	QU	IR E
P	RI	SO	NE R
RE	SI	ST	AN CE
D IS PO	SI	TI	ON
PO	SI	TI	ON
	SO	UT	H
	SQ	UA	DR ON
FI GH	TE	RP	LA NE
MO	TO	RI	ZE D
D EP AR	TU	RE	
	UN	US	UA L

	A–	—	A–	
S	AB	OT	AG	E
D ET	AC	HM	EN	T
H	AS	BE	EN	
	BA	TT	AL	IO N
	BO	MB	ED	
	CA	SU	AL	TI ES
	CA	SU	AL	TY
	CO	MB	AT	
	CO	OR	DI	NA TE S
	DI	RE	CT	IO N
	DI	SP	AT	CH
ME	DI	UM	BO	MB ER
	DI	VE	BO	MB ER
R OA	DJ	UN	CT	IO N
R	EP	LA	CE	ME NT
R	ET	RE	AT	
S	EV	ER	AL	
JU	NC	TI	ON	
CO	NF	IR	MA	TI ON
I	NF	OR	MA	TI ON
I	NT	EL	LI	GE NC E
	PA	TR	OL	

	A–	—	A–	
	SA	BO	TA	GE
	SE	VE	RE	
AC	TI	VI	TY	
A	TT	EN	TI	ON
S	UC	CE	SS	FU LL Y

	A–	—	—	A–	
	AR	TI	LL	ER	Y
	AT	TA	CK	ED	
R	EE	NF	OR	CE	
R	EE	NF	OR	CE	ME NT
	ID	EN	TI	FY	
	IM	PO	SS	IB	LE
	MO	VE	ME	NT	
E	MP	LA	CE	ME	NT
	PE	RS	ON	NE	L
A	RT	IL	LE	RY	

	A–	—	—	—	A–	
	CO	MM	UN	IC	AT	IO NS
	CO	NC	EN	TR	AT	E
R	EO	RG	AN	IZ	AT	IO N
	LI	EU	TE	NA	NT	
CO	NS	TR	UC	TI	ON	

A–	—	—	—	—	A–
CO	MM	IS	SI	ON	ED

		–B	–B		
	UN	AB	LE		
OB	ST	AC	LE		
		AD	VA	NC	E
		AG	AI	NS	T
	R	AI	LH	EA	D
PR	EP	AR	AT	IO	N
A	SS	AU	LT		

Table D-6 (~~C~~). List of four-square digraphic idiomorphs (U)--Continued

TWO LETTERS --Continued

				-B	-B			
		B	OM	BA	RD			
		A	IR	BO	RN	E		
		S	EA	BO	RN	E		
	A	DV	AN	CI	NG			
			VI	CI	NI	TY		
				DE	TA	CH		
				DE	TA	CH	ME	NT
		H	AV	EB	EE	N		
		M	OV	EM	EN	T		
				EN	EM	Y		
			R	ES	ER	VE		
			R	ET	UR	N		
				FL	AN	K		
				FO	LL	OW		
		B	AG	GA	GE			
				HA	SB	EE	N	
A	PP	RO	AC	HI	NG			
	DE	BO	UC	HI	NG			
	L	AU	NC	HI	NG			
	I	MM	ED	IA	TE	LY		
		IN	IT	IA	TE			
			F	IF	TH			
		TE	RR	IT	OR	Y		
			S	IX	TY			
	M	IS	CE	LL	AN	EO	US	
			E	LE	VA	TI	ON	
			E	LE	VE	N		
				LI	AI	SO	N	
			DA	MA	GE			
				MO	RN	IN	G	
			U	NU	SU	AL		
				OB	JE	CT	IV	E

			-B	-B			
		C	OL	ON			
		C	OL	ON	EL		
SU	PE	RI	OR	IT	Y		
		M	OT	OR	IZ	ED	
			OU	TS	KI	RT	S
	EQ	UI	PM	EN	T		
	A	VE	RA	GE			
	B	AR	RA	GE			
		AI	RC	RA	FT		
AN	TI	AI	RC	RA	FT		
			RE	MA	IN		
R	EQ	UI	RE	ME	NT		
	M	IS	SI	NG			
		P	ER	SO	NN	EL	
	ES	TI	MA	TE	DA	T	
		P	LA	TO	ON		
			S	UP	PL	Y	
			S	UP	PO	RT	
			NA	VA	LB	AS	E
		F	OR	WA	RD		
		WI	ND	WA	RD		

			-B	—	-B		
		C	AS	UA	LT	Y	
		P	AT	RO	LS		
B	AT	TL	ES	HI	PS		
			GE	NE	RA	L	
	W	IL	LA	TT	AC	K	
	T	RA	NS	MI	SS	IO	N
	R	EC	OG	NI	TI	ON	
	T	RO	OP	SH	IP		
			RE	GI	ME	NT	

		-B	—	-B
	CA	RR	IE	RS
	MI	SS	IO	NS
		TW	EN	TY
R	EQ	UE	ST	ED

	-B	—	—	-B			
I	DE	NT	IF	IC	AT	IO	N
M	EC	HA	NI	ZE	D		
D	EP	LO	YM	EN	T		
M	ES	SE	NG	ER			
D	ES	TR	OY	ER			
A	IR	SU	PP	OR	T		
V	IS	IB	IL	IT	Y		
	ME	SS	EN	GE	R		
I	MP	AS	SA	BL	E		
I	MP	OS	SI	BL	E		
A	NT	IA	IR	CR	AF	T	
C	OM	MA	ND	IN	G		
	OP	ER	AT	IO	N		
	PR	IS	ON	ER			
	PR	OC	ED	UR	E		
	RE	EN	FO	RC	E		
	TR	AN	SP	OR	TA	TI	ON
	YE	ST	ER	DA	Y		

		-B	—	—	—	-B	
	R	EC	OM	ME	ND	ED	
		HE	AV	YL	OS	SE	S
R	EC	OM	ME	ND	AT	IO	N
	C	OM	MU	NI	CA	TI	ON
R	EC	ON	NO	IT	ER	IN	G

Table D-6 (~~C~~). List of four-square digraphic idiomorphs (U)--Continued

THREE LETTERS

```
     A- A- A-
   N|AV AL BA|SE
R EQ|UI SI TI|ON

 A- A- — A-
|RE QU ES TE|D

        -B -B -B
B OM|BA RD ME|NT
    |EL EM EN|TS
  EN|GA GE ME|NT
```

FOUR LETTERS

```
   AB A- -B
H|EA DQ UA|RT ER S
 |EL EV EN|

   AB -B A-
  |CA NC EL|
RE|CO NN AI|SS AN CE

 AB -B — A-
|AD VA NC ED|
|EN EM YT AN|KS

 AB — A- -B
|SI GH TI NG|

 A- AB -B
|AD DI TI|ON AL

 A- AB — -B
|SO UT HW ES|T

  A- A- -B -B
W|IT HD RA WA|L

 A- A- — A- A-
|CO MM AN DI NG|
```

```
 A- A- — -B -B
|RE QU IR EM EN|T

  A- -B AB
M|OR NI NG|
P|OS TP ON|E

 A- -B -B — A-
|RE CO NN OI TE|R

 A- -B — AB
|IN TE RD IC|T

  A- -B — A- -B
S|AT IS FA CT OR|Y

 A- — A- C- C-
|DI SP AT CH ES|

 A- — — C- A- C-
|RO AD JU NC TI ON|

      -B AB A-
DI SP|OS IT IO|N
    P|OS IT IO|N
     |PR ES EN|T
   RE|PR ES EN|T
```

```
   -B A- AB
RE|PE AT ED|

 -B A- A- -B
|DE ST RO YE|R

 -B A- -B — A-
|UN ID EN TI FI|ED

  -B A- — AB
U|NS UC CE SS|FU L

 -B A- — A- -B
|ME DI UM BO MB|ER

 -B A- — -B A-
|VI SI BI LI TY|

 -B A- — — AB
|IN FO RM AT IO|N

 -B A- — — A- -B
|IN ST AL LA TI ON|

 -B -D -B — -D
|CR OS SR OA DS|
```

Table D-6 (~~C~~). List of four-square digraphic idiomorphs (U)--Continued

FOUR LETTERS --Continued

<table>
<tr><td>−B −D −D −B
AI |RS UP PO RT|

−B −D — −D −B
|IN ST RU CT IO|N
C|ON ST RU CT IO|N</td><td>−B — A− AB
F IG HT |ER PL AN ES|

−B — A− — — AB
E|ST AB LI SH ME NT|</td><td>−B — −B A− A−
|EN CO UN TE RE|D

−B — — −B −D −D
|RE IN FO RC EM EN|T</td></tr>
</table>

FIVE LETTERS

<table>
<tr><td>A− −B AB — −B
|NA VA LA TT AC|K

A− −B — −B AB
R EC|ON NA IS SA NC|E</td><td>−B A− A− — AB
|DI ST RI BU TI|ON

−B A− −B AB
RE|PL AC EM EN|T</td><td>−B −D — −D −B −D
|IN ST RU CT IO NS|</td></tr>
</table>

SIX LETTERS

<table>
<tr><td>AB CB C− A−
P|OS IT IO NS|

AB −D −D AB
C|ON DI TI ON|
|RA DI OG RA|M</td><td>A− A− −B AB A−
|RE QU IS IT IO|N

A− CB — A− CB
Q UA|RT ER MA ST ER|

A− CB — CB A−
|SC HO OL HO US|E</td><td>A− — CB A− — CB
|ID EN TI FI CA TI|ON

−B AB AD −D
A|DM IN IS TR|AT IV E</td></tr>
</table>

Table D-6 (~~C~~). List of four-square digraphic idiomorphs (U)--Continued

SEVEN LETTERS

<table>
<tr><td>−B AD — −B −D AD
|RE EN FO RC EM EN|T</td></tr>
</table>

EIGHT LETTERS

<table>
<tr><td>AB −B AD — −B AD
|QU AR TE RM AS TE|R</td><td>AB −B C− AB CB
|EM PL AC EM EN|T</td><td>AB −D C− AD C− −B
|IN TE RD IC TI ON|</td></tr>
</table>

Table D–7 (U). List of words containing like letters repeated at various intervals (U)

AA	RU	BBER	AA	CR	EEK
AA	RU	BBLE	AA	DECR	EE
AA	A	CCEPT	AA	DEGR	EE
AA	A	CCEPTABLE	AA	EIGHT	EEN
AA(5)A	A	CCEPTANCE	AA	EIGHT	EENTH
AA	A	CCESS	AA	EMPLOY	EE
AA	A	CCESSORY	AA	ENGIN	EER
AA	A	CCIDENTIAL	AA	ENGIN	EERING
AA	A	CCOMPANY	AA	F	EEL
AA	A	CCOMMODATION	AA	F	EET
AA(5)A	A	CCORDANCE	AA	FIFT	EEN
AA	A	CCORDING	AA	FIFT	EENTH
AA	O	CCUPATION	AA	FL	EE
AA	O	CCUPY	AA	FL	EET
AA	SU	CCEEDED	AA	FOURT	EEN
AA	SU	CCESS	AA	FOURT	EENTH
AA	SU	CCESSFUL	AA	HASB	EEN
AA	SU	CCESSFULLY	AA	HAVEB	EEN
AA	SU	CCESSIVE	AA	IND	EED
AA	TOBA	CCO	AA	K	EEP
AA	UNSU	CCESSFUL	AA(1)A	K	EEPER
AA	A	DD	AA	M	EET
AA	A	DDITIONAL	AA	NINET	EEN
AA	A	DDRESSES	AA	NINET	EENTH
AA	A	DDRESS	AA	PROC	EED
AA(5)A	A	DDRESSED	AA(1)A	PROC	EEDED
AA	BE	DDING	AA	QU	EEN
AA	LA	DDER	AA(5)A	R	EENFORCE
AA	SU	DDEN	AA(5)A(1)A	R	EENFORCEMENT
AA(1)A	AGR	EEMENT	AA	R	EENLIST
AA	B	EEN	AA(5)A	R	EENLISTED
AA(1)A	BEENN	EEDED	AA(6)A	R	EENLISTMENT
AA(2)AA(1)A	B	EENNEEDED	AA	REFUG	EE
AA(2)A	B	EETLE	AA	SCR	EEN
AA	BETW	EEN	AA	SCR	EENING
AA(1)A	BR	EEZE	AA	S	EE
AA(1)A	CH	EESE	AA	S	EEN
AA	COFF	EE	AA	SEVENT	EEN
AA	COMMAND	EER	AA	SEVENT	EENTH
AA	COMMITT	EE	AA	SIXT	EEN

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U)–Continued

AA	SIXT	EENTH	AA	SU	GGEST
AA	SMOKESCR	EEN	AA	TRI	GGER
AA	SP	EED	AA	BEAC	HHEAD
AA	ST	EEL	AA	ACTUA	LLY
AA	STR	EET	AA	A	LL
AA(1)A	SUCC	EEDED	AA	A	LLEGE
AA	SW	EEPING	AA	A	LLEGIANCE
AA	THIRT	EEN	AA	A	LLIED
AA	THIRT	EENTH	AA	A	LLIES
AA	THR	EE	AA	A	LLOCATION
AA	W	EEK	AA	A	LLOTMENT
AA	WH	EEL	AA	A	LLOWANCE
AA	A	FFAIR	AA	A	LLOW
AA	CHAU	FFEUR	AA	A	LLY
AA	COE	FFICINT	AA	ARTI	LLERY
AA	CO	FFEE	AA	BA	LLISTICS
AA	DI	FFERENCE	AA	BA	LLOON
AA	DI	FFERENT	AA	BE	LLIGERENT
AA	DI	FFICULT	AA	BI	LLET
AA	DI	FFICULTIES	AA	BI	LLETED
AA	E	FFECT	AA	BU	LLETIN
AA	E	FFECTED	AA	CA	LL
AA	E	FFECTIVE	AA	CANCE	LLATION
AA	E	FFICACY	AA	CANCE	LLED
AA	E	FFICIENT	AA	CE	LL
AA	E	FFICIENCY	AA	CHA	LLENGE
AA	E	FFORT	AA	CO	LLAPSED
AA	GENERALSTA	FF	AA	CO	LLECT
AA	INE	FFICIENCY	AA	CO	LLECTION
AA	JUMPO	FF	AA	CO	LLEGE
AA	O	FF	AA	CO	LLISION
AA	O	FFEND	AA	COMPE	LLED
AA	O	FFENDED	AA	DISTI	LL
AA	O	FFENSE	AA	DO	LLAR
AA	O	FFENSIVE	AA	DRI	LL
AA	O	FFICE	AA	ENRO	LL
AA	O	FFICER	AA	ENRO	LLED
AA	O	FFICIAL	AA	ENRO	LLMENT
AA	POSTO	FFICE	AA	EXPE	LLED
AA	STA	FF	AA	FA	LL
AA	SU	FFER	AA	FA	LLING
AA	SU	FFERED	AA	FE	LL
AA	SU	FFICIENT	AA	FI	LLING
AA	TRA	FFIC	AA	FO	LLOW
AA(1)A	BA	GGAGE	AA	FU	LL
AA	FO	GGY	AA	HI	LL
AA	STRA	GGLER	AA	I	LL

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U)–Continued

AA(3)A	I	LLEGAL
AA	I	LLITERATE
AA	I	LLNESS
AA	I	LLUMINATE
AA	I	LLUMINATING
AA	I	LLUMINATION
AA	I	LLUSTRATE
AA	I	LLUSTRATION
AA	INSTA	LL
AA	INSTA	LLATIONS
AA	INTE	LLIGENCE
AA	INTE	LLIGENT
AA	KI	LLED
AA	KI	LLING
AA	MI	LLIMETER
AA	MISCE	LLANEOUS
AA	OSCI	LLATE
AA	PARA	LLAX
AA(1)A	PARA	LLEL
AA	PATRO	LLING
AA	PAYRO	LL
AA	RA	LLY
AA	REBE	LLION
AA	REFI	LL
AA	REFI	LLING
AA	REPE	LLED
AA	RESPECTFU	LLY
AA	SHE	LL
AA	SHE	LLED
AA	SHE	LLFIRE
AA	SHE	LLING
AA	SHE	LLS
AA	SIGNA	LLING
AA	SMA	LL
AA	SPE	LL
AA	SUCCESSFU	LLY
AA	VA	LLEY
AA	VI	LLAGE
AA	WE	LL
AA	WI	LL
AA	WI	LLATTACK
AA	WI	LLIAM
AA	ACCO	MMODATION
AA	A	MMETER
AA	A	MMUNITION
AA	CO	MMA
AA	CO	MMAND
AA	CO	MMANDANT
AA	CO	MMANDED
AA	CO	MMANDEER
AA	CO	MMANDER
AA	CO	MMANDING
AA	CO	MMENCE
AA(4)A	CO	MMENCEMENT
AA	CO	MMEND
AA	CO	MMENDATION
AA	CO	MMENT
AA	CO	MMERCE
AA	CO	MMISSARY
AA	CO	MMISSION
AA	CO	MMISSIONER
AA	CO	MMIT
AA(2)A	CO	MMITMENT
AA	CO	MMITTEE
AA	CO	MMON
AA	CO	MMUNICATE
AA	CO	MMUNICATION
AA	CO	MMUNIQUE
AA	CO	MMUTE
AA	HA	MMER
AA	I	MMEDIATE
AA	I	MMIGRATION
AA	INFLA	MMABLE
AA	RECO	MMEND
AA	RECO	MMENDATION
AA	RECO	MMENDED
AA	SU	MMARY
AA	SU	MMER
AA	SU	MMIT
AA	SU	MMON
AA	SWI	MMING
AA	A	NNEX
AA	A	NNOUNCE
AA(2)A(4)A	A	NNOUNCEMENT
AA	A	NNUAL
AA	ANTE	NNA
AA	BA	NNER
AA	BEE	NNEEDED
AA(1)A	BEGI	NNING
AA	CA	NNOT
AA	CHA	NNEL
AA(4)A	CO	NNECTING
AA(5)A	CO	NNECTION
AA	GU	NNER

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U)–Continued

AA	MA	NNER	AA	A	PPARATUS
AA(1)A	MA	NNING	AA	A	PPARENT
AA	PERSO	NNEL	AA	A	PPARENTLY
AA(1)A	PLA	NNING	AA	A	PPEAR
AA(5)A	RECO	NNAISSANCE	AA	A	PPEARANCE
AA	RECO	NNOITER	AA	A	PPEARED
AA(6)A	RECO	NNOITERING	AA	A	PPLICATION
AA	RU	NNER	AA	A	PPLY
AA(1)A	RU	NNING	AA	A	PPOINT
AA	TO	NNAGE	AA	A	PPOINTED
AA	AFTERN	OON	AA	A	PPOINTMENT
AA	ASS	OONAS	AA	A	PPROACH
AA	BALL	OON	AA(2)A	A	PPROPRIATE
AA	B	OOK	AA	A	PPROVAL
AA	B	OOTH	AA	A	PPROVE
AA	CODEB	OOK	AA	A	PPROXIMATE
AA	C	OOK	AA	CLI	PPER
AA	C	OOPERATE	AA	DISA	PPEAR
AA(6)A	C	OOPERATION	AA	DISA	PPEARANCE
AA	C	OORDINATE	AA	DISA	PPEARED
AA(7)A	C	OORDINATION	AA	DRO	PPED
AA(2)A	F	OOTHOLD	AA	HA	PPEN
AA	FOREN	OON	AA	MA	PPING
AA	H	OOK	AA	O	PPOSE
AA	L	OOK	AA	O	PPOSITE
AA(1)A	L	OOKOUT	AA	O	PPOSITION
AA	N	OON	AA	PHILI	PPINES
AA	PLAT	OON	AA	REA	PPOINTED
AA	PONT	OON	AA	REA	PPOINTMENT
AA	PR	OOF	AA	SHI	PPING
AA	SCH	OOL	AA	STO	PPED
AA(2)A	SCH	OOLHOUSE	AA	SU	PPLIES
AA	SHARPSH	OOTER	AA	SU	PPLY
AA	S	OON	AA	SU	PPORT
AA	SP	OOLS	AA	SU	PPORTING
AA	SP	OONS	AA	SU	PPOSE
AA	TATT	OO	AA	A	RRANGE
AA	T	OO	AA	A	RRANGEMENT
AA	T	OOK	AA	A	RREST
AA	T	OOL	AA	A	RESTED
AA	TR	OOPS	AA	A	RRIVAL
AA	TR	OOPSHIP	AA	A	RRIVE
AA	TR	OOPSHIPS	AA	BA	RRACKS
AA	UNDERST	OOD	AA	BA	RRAGE
AA	W	OODED	AA	CA	RRIAGE
AA	W	OODS	AA(2)A	CA	RRIER
AA	AIRSU	PPORT	AA	CA	RRY

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) –Continued

AA	CONFE	RRED	AA	A	SSEMBLE
AA	CO	RRECT	AA	A	SSEMBLY
AA	CO	RRECTED	AA(6)A	A	SSEMBLIES
AA	CO	RRECTION	AA(1)AA(4)A	A	SSESSMENTS
AA	CO	RRECTNESS	AA(4)A	ASSE	SSMENTS
AA	CO	RRESPONDENCE	AA	A	SSET
AA	CO	RRESPONDING	AA(2)A	A	SSETS
AA(3)A	CO	RRIDOR	AA	A	SSIGNED
AA	CU	RRENT	AA	A	SSIGNMENT
AA	DEFE	RRED	AA(7)A	A	SSIGNMENTS
AA	DE	RRICK	AA(1)A	A	SSIST
AA(1)A	E	RROR	AA(1)A	A	SSISTANT
AA	FE	RRY	AA(1)A	A	SSISTANCE
AA	GA	RRISON	AA	A	SSOCIATE
AA	HU	RRICANE	AA	A	SSOCIATION
AA	INTE	RRUPT	AA(4)A	A	SSOONAS
AA	INTE	RRUPTED	AA	A	SSURANCE
AA	INTE	RRUPTION	AA	A	SSURE
AA(5)A	I	RREGULAR	AA	BUSINE	SS
AA(5)A	I	RREGULARITIES	AA	CARELE	SS
AA(5)A	I	RREGULARITY	AA(2)AA	CARELE	SSNESS
AA	I	RRIGATION	AA	CARELESSNE	SS
AA(1)A	MI	RROR	AA(1)A	CHA	SSIS
AA	PREA	RRANGED	AA	CLA	SSIFICATION
AA	PREFE	RRED	AA	COMMI	SSARY
AA(4)A	SU	RRENDER	AA	COMMI	SSION
AA(4)A	SU	RRENDERED	AA	COMMI	SSIONER
AA	SU	RROUND	AA	COMPA	SS
AA	TE	RRAIN	AA	COMPLETENE	SS
AA	TE	RRIBLE	AA	COMPRE	SSED
AA	TE	RRIFIC	AA	CONCE	SSION
AA(3)A	TE	RRITORY	AA	CONFE	SSION
AA(1)A	TE	RROR	AA	CONGRE	SS
AA	TOMO	RROW	AA	CONGRE	SSIONAL
AA	TRANSFE	RRED	AA	CORRECTNE	SS
AA	TRANSFE	RRING	AA	CRO	SS
AA	TU	RRET	AA	CRO	SSING
AA	ACCE	SS	AA(4)A	CRO	SSROADS
AA	ACCE	SSORY	AA	DARKNE	SS
AA	ACRO	SS	AA	DEPRE	SSION
AA	ADDRE	SSED	AA	DISCU	SS
AA	ADDRE	SS	AA	DISCU	SSED
AA(1)A	ADDRE	SSES	AA	DISCU	SSION
AA	ADMI	SSION	AA	DISMI	SS
AA	AMBA	SSADOR	AA	DISMI	SSAL
AA	ASPO	SSIBLE	AA	DI	SSEMINATED
AA	A	SSAULT	AA	DI	SSEMINATION

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) —Continued

AA	DISTRE	SS	AA(1)AA	PO	SSESSION
AA	DISTRE	SSED	AA	PO	SSIBLE
AA	DRE	SS	AA	PREPAREDNE	SS
AA	DRE	SSING	AA	PRE	SS
AA(2)A	EMBA	SSIES	AA	PRE	SSED
AA	EMBA	SSY	AA	PRE	SSURE
AA	EXCE	SS	AA	PROGRE	SSIVE
AA	EXCE	SSIVE	AA	PROGRE	SS
AA	EXPRE	SS	AA	READINE	SS
AA	FORTRE	SS	AA	RECONNAI	SSANCE
AA	GA	SSING	AA	REDCRO	SS
AA(1)A	GLA	SSES	AA	SE	SSION
AA(1)A	HEAVYLO	SSES	AA	STRE	SS
AA	ILLNE	SS	AA	SUBMI	SSION
AA	IMPA	SSABLE	AA	SUCCE	SS
AA	IMPO	SSIBLE	AA	SUCCE	SSFUL
AA	IMPRE	SSED	AA	SUCCE	SSFULLY
AA	IMPRE	SSION	AA	SUCCE	SSIVE
AA	IMPRE	SSIVE	AA	TRANSMI	SSION
AA	I	SSUE	AA	UNLE	SS
AA(2)A	I	SSUES	AA	UNSUCCE	SSFUL
AA	I	SSUING	AA	USELE	SS
AA	LE	SS	AA	VE	SSEL
AA	LE	SSON	AA(2)A	VE	SSELS
AA	LO	SS	AA	WIRELE	SS
AA(1)A	LO	SSES	AA	WITNE	SS
AA	MA	SS	AA(1)A	WITNE	SSES
AA	ME	SS	AA	A	TTACH
AA	ME	SSAGE	AA(6)A	A	TTACHMENT
AA(3)A	ME	SSAGES	AA	A	TTACK
AA	ME	SSENGER	AA	A	TTAIN
AA	ME	SSING	AA(6)A	A	TTAINMENT
AA	MI	SSING	AA(3)A	A	TTEMPT
AA	MI	SSION	AA(3)A	A	TTEMPTED
AA(3)A	MI	SSIONS	AA(2)A	A	TTENTION
AA	NECE	SSARY	AA	BA	TTALION
AA	NECE	SSITY	AA	BA	TTEN
AA	NECE	SSITATE	AA	BA	TTERED
AA	PA	SS	AA	BA	TTERIES
AA	PA	SSAGE	AA	BA	TTERY
AA	PA	SSED	AA	BA	TTLE
AA	PA	SSENGER	AA	BA	TTLEFIELD
AA(1)A	PA	SSES	AA	BA	TTLESHIP
AA	PA	SSIVE	AA	BE	TTER
AA	PA	SSPORT	AA	BI	TTER
AA	PERMI	SSION	AA	BO	TTOM
AA	POSSE	SSION	AA	BOYCO	TT

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) – Continued

AA	CIGARE	TTE	A–A	COMB	ATANT
AA	COMMI	TTEE	A–A	CONTR	ABAND
AA	COUNTERA	TTACK	A–A	D	AMAGE
AA	FI	TTING	A–A	D	AMAGED
AA	GE	TTING	A–A	D	AMAGING
AA	LE	TTER	A–A	DISAPPE	ARANCE
AA	LE	TTERED	A–A	EXC	AVATE
AA	LI	TTER	A–A	EXC	AVATION
AA	LI	TTLE	A–A	EXPL	ANATION
AA	NAVALA	TTACK	A–A	F	ATAL
AA	NAVALBA	TTLE	A–A	F	ATALITY
AA	OMI	TTED	A–A	FIRE	ALARM
AA	SE	TTLE	A–A	G	ARAGE
AA	SPO	TTING	A–A(1)A	GENER	ALALARM
AA	SUBMI	TTED	A–A	GENERAL	ALARM
AA	TA	TTOO	A–A	J	APAN
AA	THA	TTHE	A–A	M	ANAGE
AA	WILLA	TTACK	A–A	M	ANAGEMENT
AA	WRI	TTEN	A–A	N	AVAL
AA	MU	ZZLE	A–A(1)A(2)A	N	AVALATTACK
AA	NO	ZZLE	A–A(2)A	NAV	ALATTACK
A–A		ABANDON	A–A(2)A	N	AVALBASE
A–A		AGAIN	A–A(2)A	N	AVALBATTLE
A–A		AGAINST	A–A	N	AVALFORCES
A–A		ALARM	A–A	NONCOMB	ATANT
A–A(2)A		ALASKA	A–A(1)A	P	ANAMA
A–A	ALM	ANAC	A–A	PAN	AMA
A–A		ANALYSIS	A–A	P	ARACHUTE
A–A		ANALYZE	A–A	P	ARADE
A–A	APP	ARATUS	A–A(2)A	P	ARAGRAPH
A–A	APPE	ARANCE	A–A(2)A	P	ARALLAX
A–A(2)A		ARABIA	A–A	P	ARALLEL
A–A(2)A		AVAILABLE	A–A	PREP	ARATION
A–A		AWAIT	A–A	PROCL	AMATION
A–A		AWARD	A–A	QU	ARANTINE
A–A		AWAY	A–A	S	ALARY
A–A	C	ALAMITY	A–A	SEP	ARATE
A–A(1)A	C	ANADA	A–A	SEP	ARATION
A–A	CAN	ADA	A–A	T	AXATION
A–A	C	ANAL	A–A	V	ACANCY
A–A	C	APABILITY	A–A	WITHDR	AWAL
A–A	C	APACITY	A–A	PRO	BABLE
A–A	C	ATASTROPHE	A–A	PRO	BABLY
A–A	C	AVALRY	A–A	BI	CYCLE
A–A	CH	ARACTER	A–A		CYCLONE
A–A	CH	ARACTERISTIC	A–A	EFFI	CACY
A–A	CLE	ARANCE	A–A	MOTOR	CYCLE

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) –Continued

A–A	BEENNEE	DED	A–A	COLL	EGE
A–A	BLOCKA	DED	A–A	COMMENC	EMENT
A–A	BOMBAR	DED	A–A	COMPL	ETELY
A–A	COMMAN	DED	A–A	COMPL	ETE
A–A	DECI	DED	A–A	COMPLET	ENESS
A–A		DEDICATE	A–A(1)A	COMPL	ETENESS
A–A		DEDICATION	A–A	CONCR	ETE
A–A	DEFEN	DED	A–A(2)A	CONF	ERENCE
A–A	DEMAN	DED	A–A	CONFIN	EMENT
A–A	ENCO	DED	A–A	CONQU	ERED
A–A	EXPAN	DED	A–A	COV	ERED
A–A	EXPEN	DED	A–A	CR	EDENTIAL
A–A	EXTEN	DED	A–A(2)A	D	ECEMBER
A–A	GROUN	DED	A–A(7)A	D	ECENTRALIZE
A–A	GUAR	DED	A–A(7)A	D	ECENTRALIZED
A–A	INVA	DED	A–A	DECIPH	ERED
A–A	LAN	DED	A–A	D	EFEAT
A–A	OFFEN	DED	A–A(2)A	D	EFEATED
A–A	PROCEE	DED	A–A	D	EFECT
A–A	RAI	DED	A–A(4)A	D	EFECTIVE
A–A	RECOMMEN	DED	A–A	D	EFEND
A–A	SUCCEE	DED	A–A(2)A	D	EFENDER
A–A	SUSPEN	DED	A–A(2)A	D	EFENDED
A–A	UNEXPEN	DED	A–A(2)A	D	EFENSE
A–A	WOO	DED	A–A(4)A	D	EFENSIVE
A–A	WOUN	DED	A–A	D	EFER
A–A		DID	A–A(2)A	D	EFERRED
A–A	AGRE	EMENT	A–A	D	EPEND
A–A	ALL	EGE	A–A	D	EPENDABILITY
A–A	AMM	ETER	A–A(5)A	D	EPENDABLE
A–A	AMUS	EMENT	A–A(2)A	D	EPENDENT
A–A	ANNOUNC	EMENT	A–A	D	ESERT
A–A	ARRANG	EMENT	A–A(2)A	D	ESERTED
A–A	BAROM	ETER	A–A(2)A	D	ESERTER
A–A	BATT	ERED	A–A	D	ETECTOR
A–A	BEENNE	EDED	A–A	D	ETENTION
A–A	BELLIG	ERENT	A–A(6)A	D	ETERIORATE
A–A	BESI	EGED	A–A	D	ETERMINATION
A–A	BILL	ETED	A–A(4)A	D	ETERMINE
A–A	BRE	EZE	A–A(4)A	D	ETERMINED
A–A	BRIDG	EHEAD	A–A	D	EVELOP
A–A	CAR	ELESS	A–A(3)A	D	EVELOPED
A–A(3)A	CAR	ELESSNESS	A–A(4)A	D	EVELOPMENT
A–A	CEM	ETERY	A–A	DIFF	ERENT
A–A(1)A	C	EMETERY	A–A(2)A	DIFF	ERENCE
A–A	CENT	ERED	A–A	DISPLAC	EMENT
A–A	CHE	ESE	A–A	DYNAMOM	ETER

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) —Continued

A–A		ELECTRICITY	A–A(2)A	INTERF	ERENCE
A–A	EL	EMENT	A–A	INTERPR	ETER
A–A	EL	EMENTARY	A–A	INTERV	ENE
A–A(1)A		ELEMENT	A–A	KE	EPER
A–A(1)A		ELEMENTARY	A–A	KILOM	ETER
A–A(3)A		ELEVATE	A–A	LETT	ERED
A–A		ELEVATION	A–A	L	EVEL
A–A(1)A		ELEVEN	A–A	MANAG	EMENT
A–A	EL	EVEN	A–A	MANGAN	ESE
A–A	ELSEWH	ERE	A–A	MEASUR	EMENT
A–A(2)A		EMERGENCY	A–A	MEASUR	EMENTS
A–A	EMPLAC	EMENT	A–A	M	ETEOROLOGICAL
A–A	ENCIPH	ERED	A–A	M	ETER
A–A	ENCOUNT	ERED	A–A	MILLIM	ETER
A–A(2)A		ENEMIES	A–A	MOV	EMENT
A–A		ENEMY	A–A	N	ECESSARY
A–A(6)A		ENEMYPLANES	A–A	N	ECESSITY
A–A		ENEMYTANKS	A–A(6)A	N	ECESSITATE
A–A	ENFORC	EMENT	A–AA	NIN	ETEEN
A–A	ENGAG	EMENT	A–AA	NIN	ETEENTH
A–A	ENTANGL	EMENT	A–A	OBSOL	ETE
A–A		EVERY	A–A	ORD	ERED
A–A	EXCIT	EMENT	A–A	PARENTH	ESES
A–A(5)A		EXECUTIVE	A–A	P	ENETRATION
A–A(4)A		EXERCISE	A–A(4)A	P	ENETRATE
A–A	EXTR	EME	A–A	P	ETER
A–A		EYE	A–A	PLAC	EMENT
A–A	F	EDERAL	A–A	PREC	EDE
A–A	G	ENERAL	A–A(1)A	PR	ECEDE
A–A	G	ENERALALARM	A–A(2)A	PREC	EDENCE
A–A	G	ENERALSTAFF	A–A(1)A(2)A	PR	ECEDENCE
A–A	GONIOM	ETER	A–A	PR	ECEDING
A–A	GYROM	ETER	A–A	PR	EFER
A–AA	HAV	EBEEN	A–A(2)A	PREF	ERENCE
A–A	H	ERE	A–A(1)A(2)A	PR	EFERENCE
A–A	HIND	ERED	A–A(2)A	PR	EFERRED
A–A	HYDROM	ETER	A–A	PR	ESENT
A–A	HYGROM	ETER	A–A	PR	ESERVATION
A–A	IC	EBERG	A–A(2)A	PR	ESERVE
A–A	IMPROV	EMENT	A–A	PROCE	EDED
A–A(2)A	INCOMP	ETENCE	A–A	PSYCHROM	ETER
A–A	INCOMP	ETENT	A–A	R	EBELLION
A–A(2)A	IND	EPENDENT	A–A	R	ECEIPT
A–A(6)A	IND	ETERMINATE	A–A(2)A	R	ECEIVE
A–A	INT	EREST	A–A(2)A	R	ECEIVER
A–A	INT	ERESTING	A–A	R	ECEIVING
A–A	INTERF	ERE	A–A(5)A	R	ECEPTACLE

Table D–7 (b). List of words containing like letters repeated at various intervals (U) —Continued

A–A	REENFORC	EMENT	A–A	SUCCE	EDED
A–A	R	EFER	A–A	SUFF	ERED
A–A(2)A	REF	ERENCE	A–A	SURREND	ERED
A–A(1)A(2)A	R	EFERENCE	A–A	T	ELEGRAM
A–A	REIMBURS	EMENT	A–A(4)A	T	ELEPHONE
A–A	REINFORC	EMENT	A–A	TH	ERE
A–A	REINSTAT	EMENT	A–A(3)A	TH	EREFORE
A–A	R	EJECT	A–A	THERMOM	ETER
A–A(2)A	R	EJECTED	A–A	TH	ESE
A–A	R	EJECTOR	A–A	THREAT	ENED
A–A(2)A	R	ELEASE	A–A	US	ELESS
A–A	RELI	EVE	A–A	V	ETERINARIAN
A–A(2)A	R	EMEDIES	A–A	W	ERE
A–A	R	EMEDY	A–A	WH	ERE
A–A(2)A	R	EMEMBER	A–A	WIR	ELESS
A–A(2)A	R	EPEATED	A–A		FIFTEEN
A–A(2)A	R	EPEATER	A–A		FIFTEENTH
A–A	R	EPEL	A–A		FIFTH
A–A(2)A	R	EPELLED	A–A		FIFTY
A–A	REPLAC	EMENT	A–A	BAG	GAGE
A–A	REPR	ESENT	A–A	EN	GAGE
A–A	REPR	ESENTATION	A–A	EN	GAGEMENT
A–A(6)A	REPR	ESENTATIVE	A–A(2)A	EN	GAGING
A–A	REQUIR	EMENT	A–A	EIG	HTH
A–A	R	ESEARCH	A–A	WIT	HTHE
A–A	R	ESERVATION	A–A	ACT	IVITY
A–A(2)A	R	ESERVE	A–A	ACTIV	ITIES
A–A	R	ETENTION	A–A(1)A	ACT	IVITIES
A–A(2)A	R	EVENUE	A–A	ADD	ITIONAL
A–A(2)A	R	EVERSE	A–A(5)A	ADM	INISTRATIVE
A–A	REVI	EWED	A–A(5)A	ADM	INISTRATION
A–A	SCH	EME	A–A	ADV	ISING
A–A	SEAL	EVEL	A–A	AMMUN	ITION
A–A	S	ELECT	A–A	ANT	IAIRCRAFT
A–A(2)A	S	ELECTED	A–A	ANT	ICIPATE
A–A	S	EVEN	A–A(3)A	ANT	ICIPATION
A–A(2)AA	S	EVENTEEN	A–A	ARTIF	ICIAL
A–A(2)AA	S	EVENTEENTH	A–A(1)A	ART	IFICIAL
A–A	S	EVENTH	A–A	AUDIB	ILITY
A–A	S	EVENTY	A–A(1)A	AUD	IBILITY
A–A(6)A	S	EVENTYFIVE	A–A	CAPAB	ILITY
A–A	S	EVERAL	A–A	CERT	IFICATE
A–A	SEV	ERE	A–A	CIV	ILIAN
A–A(1)A	S	EVERE	A–A(1)A	C	IVILIAN
A–A	SI	EGE	A–A(3)A	CLASS	IFICATION
A–A	SPH	ERE	A–A	COAL	ITION
A–A	STAT	EMENT	A–A	COEFF	ICIENT

Table D–7 (¢). List of words containing like letters repeated at various intervals (U) —Continued

A–A	COLL	ISION	A–A	FACIL	ITIES
A–A	COLL	ISIONS	A–A(1)A	FAC	ILITIES
A–A	COMPET	ITION	A–A	F	ILING
A–A	COMPOS	ITION	A–A	F	INISH
A–A(2)A	CONC	ILIATION	A–A	F	IRING
A–A	COND	ITION	A–A	FORT	IFIED
A–A	CR	ISIS	A–A	HOST	ILITY
A–A	CR	ITIC	A–A	HOSTIL	ITIES
A–A	CR	ITICAL	A–A(1)A	HOST	ILITIES
A–A	CRIT	ICISE	A–A(3)A	IDENT	IFICATION
A–A	CRIT	ICISM	A–A	IGN	ITION
A–A(1)A	CR	ITICISE	A–A	INCL	INING
A–A(1)A	CR	ITICISM	A–A	IND	IVIDUAL
A–A	CR	ITIQUE	A–A	INEFF	ICIENCY
A–A	DEC	ISION	A–A	IN	ITIAL
A–A	DEF	ICIENCY	A–A(1)A		INITIAL
A–A	DEF	ICIENT	A–A	IN	ITIATE
A–A	DEF	INITE	A–A(1)A		INITIATE
A–A	DEFIN	ITION	A–A	IRREGULAR	ITIES
A–A(1)A	DEF	INITION	A–A	LIAB	ILITY
A–A	DEMOB	ILIZE	A–A	L	IAISON
A–A(3)A	DEMOB	ILIZATION	A–A	L	IMIT
A–A	DEPENDAB	ILITY	A–A(3)A	L	IMITATION
A–A	DETRA	INING	A–A(1)A	L	IMITING
A–A	DIET	ITIAN	A–A	LIM	ITING
A–A	DIM	INISH	A–A	L	INING
A–A(1)A	D	IMINISH	A–A	MAR	ITIME
A–A	DIR	IGIBLE	A–A	MED	ICINE
A–A(1)A	D	IRIGIBLE	A–A	M	ILITARY
A–A	D	ISINFECT	A–A(1)A	M	ILITIA
A–A	D	ISINFECTED	A–A	MIL	ITIA
A–A	DISPOS	ITION	A–A	M	INIMUM
A–A	D	IVIDE	A–A	M	INING
A–A	DIV	IDING	A–A(3)A	MOB	ILIZATION
A–A(1)A	D	IVIDING	A–A	MOB	ILIZE
A–A	DIV	ISION	A–A	MUN	ITIONS
A–A(1)A	D	IVISION	A–A	OBTA	INING
A–A	EFF	ICIENT	A–A	OFF	ICIAL
A–A	EFF	ICIENCY	A–A	OP	INION
A–A	ELECTR	ICITY	A–A	OPPOS	ITION
A–A	EL	IGIBLE	A–A	PAC	IFIC
A–A	ENTERPR	ISING	A–A	PART	ITION
A–A	EXH	IBITED	A–A(2)A	PH	ILIPPINES
A–A	EXHIB	ITION	A–A	POL	ITICAL
A–A(1)A	EXH	IBITION	A–A	POL	ITICS
A–A	EXPED	ITING	A–A	POS	ITION
A–A	EXPED	ITION	A–A	POS	ITIONS

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) —Continued

A–A	POS	ITIVE
A–A	PRA	IRIE
A–A(3)A	PREL	IMINARIES
A–A	PREL	IMINARY
A–A	PROH	IBIT
A–A	PROV	ISION
A–A	PROV	ISIONS
A–A	PROX	IMITY
A–A(3)A	QUAL	IFICATION
A–A	RA	IDING
A–A	RA	INING
A–A	RECE	IVING
A–A	RECOGN	ITION
A–A	RECRU	ITING
A–A	REMA	INING
A–A	REQU	IRING
A–A(1)A	REQU	ISITION
A–A	REQUIS	ITION
A–A(1)A	RESPONS	IBILITY
A–A	RESPONSIB	ILITY
A–A	RET	IRING
A–A	R	IDING
A–A	R	IGID
A–A	SEMIR	IGID
A–A(1)A	SEM	IRIGID
A–A	SERV	ICING
A–A	SIGN	IFICANT
A–A	SIGN	IFICANCE
A–A	S	IMILAR
A–A(3)A	S	IMILARITY
A–A	SPEC	IFIC
A–A(3)A	SPEC	IFICATION
A–A	SUFF	ICIENT
A–A	SUITAB	ILITY
A–A	SUSP	ICION
A–A	SUSP	ICIONS
A–A	SUSP	ICIOUS
A–A	TERR	IFIC
A–A	TRAD	ITIONAL
A–A	TRA	INING
A–A	TRANSPAC	IFIC
A–A	UNIDENT	IFIED
A–A	UT	ILITY
A–A(3)A	VER	IFICATION
A–A	VIC	INITY
A–A(1)A	V	ICINITY
A–A	VISIB	ILITY
A–A(1)A	VIS	IBILITY
A–A(1)A(1)A	V	ISIBILITY
A–A	V	ISIBLE
A–A	V	ISIT
A–A	V	ISITOR
A–A	V	ISITS
A–A	W	IRING
A–A	GENERA	LALARM
A–A	PARAL	LEL
A–A	AR	MAMENT
A–A	DYNA	MOMETER
A–A	MAXI	MUM
A–A		MEMBER
A–A		MEMORANDA
A–A(6)A		MEMORANDUM
A–A		MEMORIAL
A–A	MINI	MUM
A–A	RE	MEMBER
A–A	THER	MOMETER
A–A	A	NONYMOUS
A–A	BEGIN	NING
A–A	CONCER	NING
A–A	CONTI	NENTAL
A–A	DETRAI	NING
A–A	DOMI	NANCE
A–A	DOMI	NANT
A–A	INCLI	NING
A–A	INTERVE	NING
A–A	LIEUTE	NANT
A–A	LI	NING
A–A	MAINTE	NANCE
A–A	MAN	NING
A–A	MI	NING
A–A	MOR	NING
A–A		NAN
A–A		NINE
A–A(4)A		NINETEEN
A–A(4)A		NINETEENTH
A–A		NINETY
A–A		NINTH
A–A(7)A		NONCOMBATANT
A–A	OBTAI	NING
A–A	ORD	NANCE
A–A	PERMA	NENT
A–A	PLAN	NING
A–A	RAI	NING
A–A	REMAI	NING

Table D–7 (₵). List of words containing like letters repeated at various intervals (U) —Continued

A–A	RETUR	NING	A–A	CA	RTRIDGE
A–A	RUN	NING	A–A	D	RYRUN
A–A	SCREE	NING	A–A	ENTE	RPRISE
A–A	TRAI	NING	A–A	ENTE	RPRISING
A–A(2)A	U	NKNOWN	A–A	ER	ROR
A–A	AUT	OMOBILE	A–A	FINGE	RPRINT
A–A	CHRON	OLOGICAL	A–A	FO	RTRESS
A–A(1)A	CHR	ONOLOGICAL	A–A	INTE	RPRETATION
A–A	C	OLON	A–A(3)A	INTE	RPRETER
A–A	C	OLONEL	A–A	LIB	RARY
A–A	C	OLORS	A–A	MIR	ROR
A–A	EC	ONOMIC	A–A	NEA	RER
A–A	H	ONOR	A–A	SU	RPRISE
A–A	LOC	OMOTIVE	A–A	TER	ROR
A–A(1)A	L	OCOMOTIVE	A–A	ADDRES	SES
A–A	LO	OKOUT	A–A	ANALY	SIS
A–A	METEOR	OLOGICAL	A–AA	AS	SESSMENT
A–A(1)A	METE	OROLOGICAL	A–AA(4)A	AS	SESSMENTS
A–A	MON	OPOLY	A–A	AS	SIST
A–A(1)A	M	ONOPOLY	A–A	AS	SISTANT
A–A	M	OTOR	A–A	AS	SISTANCE
A–A	M	OTORCYCLE	A–A	CA	SES
A–A	M	OTORIZED	A–A	CHAS	SIS
A–A		OBOE	A–A	CRI	SIS
A–A	PH	OTOGRAPHY	A–A	DEFEN	SES
A–A	PR	OMOTE	A–A	DI	SASTER
A–A(2)A	PR	OMOTION	A–A	EXERCI	SES
A–A(3)A	PR	OPORTION	A–A	EXPEN	SES
A–A	PR	OPOSALS	A–A	CLAS	SES
A–A	PR	OPOSE	A–A	HEAVYLOS	SES
A–A	PROT	OCOL	A–A	LOS	SES
A–A(1)A	PR	OTOCOL	A–A	OUTPO	STS
A–A	PR	OVOST	A–A	PARENTHE	SES
A–A	RIG	OROUS	A–A	PARENTHE	SIS
A–A	SEMIC	OLON	A–A	PAS	SES
A–A(2)A	T	OMORROW	A–A	PER	SISTENT
A–A	T	OPOGRAPHIC	A–AA	POS	SESSION
A–A	VIG	OROUS	A–A	PROTE	STS
A–A	NEWS	PAPER	A–A	PURPO	SES
A–A	NEWS	PAPERS	A–A	RE	SIST
A–A		PIPE	A–A	RE	SISTANCE
A–A		POPULATED	A–AA		SESSION
A–A		POPULATION	A–A	SUB	SISTENCE
A–A	AI	RCRAFT	A–A		SUSPECTED
A–A	AI	RDROME	A–A		SUSPEND
A–A	ANTIAI	RCRAFT	A–A		SUSPENDED
A–A	ARBIT	RARY	A–A(3)A		SUSPENSE

Table D–7 (¢). List of words containing like letters repeated at various intervals (U) —Continued

A–A(3)A		SUSPENSION
A–A		SUSPICION
A–A(6)A		SUSPICIONS
A–A(6)A		SUSPICIOUS
A–A		SYSTEM
A–A	WITNES	SES
A–A	AL	TITUDE
A–A	AN	TITANK
A–A	CI	TATION
A–A	COMPE	TITION
A–A	COMPU	TATION
A–A	CONSTI	TUTE
A–A	CONSTI	TUTING
A–A(1)A	CONS	TITUTING
A–A	CONSTI	TUTION
A–A(1)A	CONS	TITUTE
A–A(1)A	CONS	TITUTION
A–A	DESTI	TUTE
A–A(1)A	DES	TITUTE
A–A	DIC	TATED
A–A	DIC	TATOR
A–A	DIE	TITIAN
A–A	INSTI	TUTION
A–A(1)A	INS	TITUTION
A–A	INTERPRE	TATION
A–A	INVI	TATION
A–A	LA	TITUDE
A–A	LIMI	TATION
A–A	NECESSI	TATE
A–A	PAR	TITION
A–A	RADIOS	TATION
A–A	REINS	TATE
A–A(4)A	REINS	TATEMENT
A–A	REPRESEN	TATIVE
A–A	REPRESEN	TATIONS
A–A	SANI	TATION
A–A(4)A	S	TATEMENT
A–A	S	TATES
A–A	S	TATION
A–A	S	TATIONS
A–A(2)A	S	TATISTICS
A–A	S	TATUS
A–A	SUBSTI	TUTE
A–A	SUBSTI	TUTION
A–A(1)A	SUBS	TITUTE
A–A(1)A	SUBS	TITUTION
A–AA		TATTOO
A–A	TEN	TATIVE
A–A		TITLE
A–A		TOTAL
A–A		TOTALING
A–A	TRANSPOR	TATION
A–A	UNITEDS	TATES
A–A	WI	THTHE
A–A	A	UGUST
A–A	CONTIN	UOUS
A–A	F	UTURE
A–A	INA	UGURATION
A–A	UN	USUAL
A–A(1)A		UNUSUAL
A–A		USUAL
A–A	SUR	VIVED
A–A	A	WKWARD
A(2)A		ADJACENT
A(2)A		ADVANCING
A(2)A	ADV	ANTAGEOUS
A(2)A	ADV	ANTAGE
A(2)A(2)A		ADVANTAGE
A(2)A(2)A		ADVANTAGEOUS
A(2)A		ADVANCE
A(2)A		ADVANCED
A(2)A		AFFAIR
A(2)A	AL	ASKA
A(2)A(1)A		ALMANAC
A(2)A		ALWAYS
A(2)A	AMB	ASSADOR
A(2)A(2)A		AMBASSADOR
A(2)A(1)A		APPARATUS
A(2)A		APPARENT
A(2)A		APPARENTLY
A(2)A	AR	ABIA
A(2)A		AREA
A(2)A		ARMAMENT
A(2)A		ARRANGE
A(2)A		ARRANGEMENT
A(2)A		ASIA
A(2)A		ASIATIC
A(2)A		ASSAULT
A(2)A		ATLANTIC
A(2)A		ATTACH
A(2)A		ATTACHEMENT
A(2)A		ATTACK
A(2)A		ATTAIN
A(2)A		ATTAINMENT

Table D–7 (₵). List of words containing like letters repeated at various intervals (U) —Continued

A(2)A	AV	AILABLE
A(2)A		AVIATION
A(2)A		AVIATOR
A(2)A	B	AGGAGE
A(2)A	B	ARRACKS
A(2)A	B	ARRAGE
A(2)A	B	ATTALION
A(2)A	C	AMPAIGN
A(2)A	C	ANVAS
A(2)A	C	APTAIN
A(2)A	C	ASUAL
A(2)A	C	ASUALTIES
A(2)A	C	ASUALTY
A(2)A	CH	APLAIN
A(2)A	CO	ASTAL
A(2)A	COMM	ANDANT
A(2)A	COUNTER	ATTACK
A(2)A	DEB	ARKATION
A(2)A	DI	AGRAM
A(2)A	EMB	ARKATION
A(2)A	EV	ACUATE
A(2)A	EV	ACUATING
A(2)A	EV	ACUATION
A(2)A	EV	ALUATION
A(2)A	GR	ADUAL
A(2)A	INFL	AMMABLE
A(2)A	INST	ALLATIONS
A(2)A	INST	ANTANEOUS
A(2)A	J	ANUARY
A(2)A	M	ANDATE
A(2)A	M	ANDATED
A(2)A	M	ANGANESE
A(2)A	M	ANUAL
A(2)A	MEMOR	ANDA
A(2)A	NAVAL	ATTACK
A(2)A	NAV	ALBASE
A(2)A	NAV	ALBATTLE
A(2)A	P	ACKAGE
A(2)A	PAR	AGRAPH
A(2)A	PAR	ALLAX
A(2)A	P	ASSAGE
A(2)A	PRE	ARRANGED
A(2)A	R	ADIAL
A(2)A	R	ADIATE
A(2)A	R	ADIATION
A(2)A	RET	ALIATION
A(2)A	SE	APLANES
A(2)A	ST	ANDARD
A(2)A	ST	ANDARDS
A(2)A	TH	ATHAVE
A(2)A	TRANS	ATLANTIC
A(2)A(2)A	TR	ANSATLANTIC
A(2)A	V	ARIATION
A(2)A	VETERIN	ARIAN
A(2)A	W	ARFARE
A(2)A	WILL	ATTACK
A(2)A	ATOMIC	BOMB
A(2)A		BARBED
A(2)A		BOMB
A(2)A		BOMBARD
A(2)A		BOMBARDED
A(2)A		BOMBARDMENT
A(2)A		BOMBER
A(2)A		BRIBE
A(2)A		BRIBERY
A(2)A		BULB
A(2)A	DIVE	BOMBER
A(2)A	HEAVY	BOMBER
A(2)A	LIGHT	BOMBER
A(2)A	MEDIUM	BOMBER
A(2)A		CANCEL
A(2)A		CANCELLATION
A(2)A		CANCELLED
A(2)A		CHECK
A(2)A		CIRCLE
A(2)A		CIRCUIT
A(2)A		CIRCUITOUS
A(2)A		CIRCULAR
A(2)A		CIRCULATE
A(2)A		CIRCULATION
A(2)A		CIRCUMSTANTIAL
A(2)A(6)A		CIRCUMSTANCES
A(2)A		CONCEAL
A(2)A		CONCEALMENT
A(2)A		CONCENTRATE
A(2)A		CONCENTRATING
A(2)A		CONCENTRATION
A(2)A		CONCERNING
A(2)A		CONCESSION
A(2)A		CONCILIATION
A(2)A		CONCLUDE
A(2)A		CONCLUSION
A(2)A		CONCRETE
A(2)A	EN	CIRCLE

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) –Continued

A(2)A	EN	CIRCLING	A(2)A	CONVAL	ESCENT
A(2)A	IMPRA	CTICABLE	A(2)A	CONV	ENIENT
A(2)A	PRA	CTICAL	A(2)A	CORR	ECTED
A(2)A	SE	CRECY	A(2)A	CORRESPOND	ENCE
A(2)A	SIGNIFI	CANCE	A(2)A	DEC	EMBER
A(2)A	TA	CTICAL	A(2)A	DECIPH	ERMENT
A(2)A	TA	CTICS	A(2)A	DECR	EASE
A(2)A	VA	CANCY	A(2)A	DECR	EASED
A(2)A	HUN	DRED	A(2)A(2)A	D	ECREASE
A(2)A	IN	DEED	A(2)A(2)A	D	ECREASED
A(2)A	ONEHUN	DRED	A(2)AA	D	ECREE
A(2)A	STAN	DARD	A(2)A	DEF	EATED
A(2)A	STAN	DARDS	A(2)A	DEF	ENDER
A(2)A	ABS	ENCE	A(2)A	DEF	ENDED
A(2)A	ADDR	ESSED	A(2)A	DEF	ENSE
A(2)A	ADDR	ESSES	A(2)A	DEF	ENSES
A(2)A	AGR	EEMENT	A(2)A	DEF	ERRED
A(2)A	APP	EARED	A(2)AA	D	EGREE
A(2)A	ARR	ESTED	A(2)A	DEP	ENDENT
A(2)A	BATT	ERIES	A(2)A	D	EPRESSION
A(2)A	BATTL	EFIELD	A(2)A	DES	ERTED
A(2)AA(1)A	BE	ENNEEDED	A(2)A	DES	ERTER
A(2)A	BEENN	EEDED	A(2)A	DIFFER	ENCE
A(2)A	BE	ETLE	A(2)A	DISAPP	EARED
A(2)A(1)A	B	ESIEGED	A(2)A	DIS	EASE
A(2)A	B	ETTER	A(2)A	DISINF	ECTED
A(2)AA	B	ETWEEN	A(2)A	DISP	ERSED
A(2)A	BR	EEZE	A(2)A	DISP	ERSE
A(2)A	CANC	ELLED	A(2)A	DISTR	ESSED
A(2)A	C	EASE	A(2)A		EAGER
A(2)A	C	ENTER	A(2)A		ECHELON
A(2)A(1)A	C	ENTERED	A(2)A(3)A		ECHELONED
A(2)A	C	ENTERING	A(2)A(4)A		ECHELONMENT
A(2)A	CHALL	ENGE	A(2)A		EDGE
A(2)A	CH	EESE	A(2)A		EFFECT
A(2)A	CIGAR	ETTE	A(2)A	EFF	ECTED
A(2)A	COINCID	ENCE	A(2)A(2)A		EFFECTED
A(2)A	COMM	ENCE	A(2)A(4)A		EFFECTIVE
A(2)A(1)A	COMM	ENCEMENT	A(2)A(1)A	ELS	EWHERE
A(2)A	COMM	ERCE	A(2)A(2)A(1)A		
A(2)A	COMP	ELLED	A(2)A	EM	ERGENCY
A(2)A	COMPR	ESSED	A(2)A	ENCIPH	ERMENT
A(2)A	COND	EMNED	A(2)A	EN	EMIES
A(2)A	COND	ENSED	A(2)A	ENT	ENTE
A(2)A	CONFER	ENCE	A(2)A(2)A		ENTENTE
A(2)A	CONF	ERRED	A(2)A		ENTER
A(2)A	CONFID	ENCE	A(2)A		ENTERING

Table D–7 (₵). List of words containing like letters repeated at various intervals (U)—Continued

A(2)A		ENTERPRISING	A(2)A	INT	ERCEPT
A(2)A(5)A		ENTERPRISE	A(2)A	INTERC	EPTED
A(2)A(6)A		ENTERTAINMENT	A(2)A(2)A	INT	ERCEPTED
A(2)A		ENVELOP	A(2)A	INTERFER	ENCE
A(2)A(3)A		ENVELOPE	A(2)A	INT	ERFERING
A(2)A		ETHER	A(2)A(1)A	INT	ERFERE
A(2)A		EXCEPT	A(2)A(1)A(2)A	INT	ERFERENCE
A(2)A		EXCESS	A(2)A	INT	ERMENT
A(2)A(4)A		EXCESSIVE	A(2)A(4)A	INT	ERMEDIATE
A(2)A		EXPECT	A(2)A	INT	ERVENING
A(2)A		EXPEDITING	A(2)A(1)A	INT	ERVENE
A(2)A		EXPEDITION	A(2)A	INT	ERVENTION
A(2)A(3)A		EXPEDITE	A(2)A	INV	ENTED
A(2)A	EXP	ELLED	A(2)A	K	EEPER
A(2)A(2)A		EXPELLED	A(2)A	L	EADER
A(2)A		EXPEND	A(2)A	L	EAVE
A(2)A	EXP	ENDED	A(2)A	L	ETTER
A(2)A(2)A		EXPENDED	A(2)A(1)A	L	ETTERED
A(2)A	EXP	ENSES	A(2)A	LIC	ENSE
A(2)A(2)A		EXPENSES	A(2)A	LI	EUTENANT
A(2)A(4)A		EXPENSIVE	A(2)A	MAN	EUVER
A(2)A	EXPERI	ENCE	A(2)A	MAT	ERIEL
A(2)A(2)A	EXP	ERIENCE	A(2)A	M	EAGER
A(2)A(2)A(2)A		EXPERIENCE	A(2)A	M	EMBER
A(2)A(3)A		EXPERIMENT	A(2)A	MESS	ENGER
A(2)A		EXTEND	A(2)A(2)A	M	ESSENGER
A(2)A	EXT	ENDED	A(2)A	N	EARER
A(2)A(2)A		EXTENDED	A(2)A	N	EAREST
A(2)A		EXTENDING	A(2)A	NEGLIG	ENCE
A(2)A		EXTENSION	A(2)A	NIN	ETEEN
A(2)A(4)A		EXTENSIVE	A(2)A	NIN	ETEENTH
A(2)A		EXTENT	A(2)A	NORTHW	ESTERN
A(2)A		EXTERIOR	A(2)A	NOV	EMBER
A(2)A		EXTERMINATION	A(2)A	OBS	ERVE
A(2)A(6)A		EXTERMINATE	A(2)A	OBS	ERVER
A(2)A	FI	ERCE	A(2)A	OFF	ENDED
A(2)A	GR	EASE	A(2)A	OFF	ENSE
A(2)A	HAV	EBEEN	A(2)A	OVERWH	ELMED
A(2)A	H	ELPER	A(2)A	PASS	ENGER
A(2)A	IMPR	ESSED	A(2)A	PRECED	ENCE
A(2)A	INCID	ENCE	A(2)A	PREFER	ENCE
A(2)A	INCOMPET	ENCE	A(2)A	PREF	ERRED
A(2)A	INCR	EASED	A(2)A	PREPAR	EDNESS
A(2)A	INDEP	ENDENT	A(2)A	PRES	ERVE
A(2)A	INF	ECTED	A(2)A	PR	ESSED
A(2)A	INFLU	ENCE	A(2)A	PROC	EEDED
A(2)A	INTELLIG	ENCE	A(2)A	PROT	ECTED

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) –Continued

A(2)A	PROT	ESTED
A(2)A	REC	EIVE
A(2)A	REC	EIVER
A(2)A	RECOMM	ENDED
A(2)A	R	ECREATION
A(2)A	R	ECREATIONAL
A(2)A	REFER	ENCE
A(2)A	REJ	ECTED
A(2)A	REL	EASE
A(2)A	R	ELIEF
A(2)A(1)A	R	ELIEVE
A(2)A	REM	EDIES
A(2)A	REM	EMBER
A(2)A	REP	EATED
A(2)A	REP	EATER
A(2)A	REP	ELLED
A(2)A(1)A	R	EPRESENT
A(2)A(1)A	R	EPRESENTATION
A(2)A(1)A(6)A	R	EPRESENTATIVE
A(2)A	R	EQUEST
A(2)A	REQU	ESTED
A(2)A(2)A	R	EQUESTED
A(2)A	RES	ERVE
A(2)A	RES	ERVES
A(2)A	R	ESPECT
A(2)A	R	ESPECTFULLY
A(2)A	R	ESPECTS
A(2)A	R	ETREAT
A(2)A	REV	ENUE
A(2)A	REV	ERSE
A(2)A	R	EVIEW
A(2)A(1)A	R	EVIEWED
A(2)A	R	EVIEWING
A(2)A(1)A	S	EALEVEL
A(2)A	S	EAMEN
A(2)A	S	ECRECY
A(2)A	S	ECRETARY
A(2)A	S	EIZE
A(2)A	SEL	ECTED
A(2)A	SENT	ENCE
A(2)A(2)A	S	ENTENCE
A(2)A	SEPT	EMBER
A(2)A(2)A	S	EPTEMBER
A(2)A	S	ERGEANT
A(2)AA	SEV	ENTEEN
A(2)AA	SEV	ENTEENTH
A(2)A	SH	ELLED
A(2)A	SOUTHW	ESTERN
A(2)A	ST	EAMER
A(2)A	SUBSIST	ENCE
A(2)A	SUCC	EEDED
A(2)A	SURR	ENDER
A(2)A(1)A	SURR	ENDERED
A(2)A	SUSP	ECTED
A(2)A	SUSP	ENDED
A(2)A	SUSP	ENSE
A(2)A(5)A	T	EMPERATURE
A(2)A(1)A	THR	EATENED
A(2)A	TRANSF	ERRED
A(2)A	TRANSV	ERSE
A(2)A	TRAV	ERSE
A(2)A	TW	ELVE
A(2)A	UNEXP	ENDED
A(2)A(2)A	UN	EXPENDED
A(2)A	V	ESSEL
A(2)A	V	ESSELS
A(2)A	W	EDNESDAY
A(2)A	W	ESTERLY
A(2)A	W	ESTERN
A(2)A	WH	ETHER
A(2)A	WITN	ESSES
A(2)A	WR	ECKED
A(2)A	Y	ESTERDAY
A(2)A	BA	GGAGE
A(2)A	DAMA	GING
A(2)A	ENGA	GING
A(2)A	FOR	GING
A(2)A		GAUGE
A(2)A		GEOGRAPHIC
A(2)A		GEOGRAPHICAL
A(2)A	LAN	GUAGE
A(2)A	NE	GLIGENT
A(2)A	NE	GLIGENCE
A(2)A	ZI	GZAG
A(2)A		HIGH
A(2)A		HIGHER
A(2)A		HIGHEST
A(2)A	T	HATHAVE
A(2)A	W	HETHER
A(2)A	W	HICH
A(2)A	ADM	ISSION
A(2)A	A	IRFIELD
A(2)A	AS	IATIC
A(2)A	ASSOC	IATION

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) –Continued

A(2)A	AV	IATION
A(2)A	BALL	ISTIC
A(2)A	BALL	ISTICS
A(2)A	BEG	INNING
A(2)A	B	INDING
A(2)A	BU	ILDING
A(2)A	CHARACTER	ISTIC
A(2)A	CO	INCIDENCE
A(2)A	COMM	ISSION
A(2)A	COMM	ISSIONER
A(2)A	COUNCIL	IATION
A(2)A	CONSCR	IPTION
A(2)A	DESCR	IPTIVE
A(2)A	DESCR	IPTION
A(2)A(1)A	D	IETITIAN
A(2)A	D	IFFICULT
A(2)A(4)A	D	IFFICULTIES
A(2)A	DISC	IPLINE
A(2)A(2)A	D	ISCIPLINE
A(2)A	D	ISMISS
A(2)A	D	ISMISSAL
A(2)A	D	ISTILL
A(2)A(3)A	D	ISTINCTION
A(2)A	DISTINGU	ISHING
A(2)A(3)A	D	ISTINGUISH
A(2)A(3)A	D	ISTINGUISHED
A(2)A(3)A(2)A	D	ISTINGUISHING
A(2)A	DR	IFTING
A(2)A	ENL	ISTING
A(2)A	F	ILLING
A(2)A	F	INDING
A(2)A	F	ISHING
A(2)A	F	ITTING
A(2)A(1)A		IGNITION
A(2)A		ILLITERATE
A(2)A(4)A		IMMIGRATION
A(2)A		INCIDENCE
A(2)A		INCIDENT
A(2)A		INDICATE
A(2)A		INDICATED
A(2)A(3)A		INDICATING
A(2)A(3)A		INDICATION
A(2)A		INDIRECT
A(2)A(1)A		INDIVIDUAL
A(2)A	INFL	ICTING
A(2)A	INS	IGNIA
A(2)A(2)A		INSIGNIA
A(2)A	INTERD	ICTION
A(2)A(3)A		INVITATION
A(2)A(3)A		IRRIGATION
A(2)A	K	ILLING
A(2)A(1)A	L	IABILITY
A(2)A	L	IFTING
A(2)A	L	IQUID
A(2)A	LOG	ISTICS
A(2)A	M	IDNIGHT
A(2)A	M	ILLIMETER
A(2)A	M	ISFIRE
A(2)A	M	ISFIRES
A(2)A	M	ISSING
A(2)A	M	ISSION
A(2)A	M	ISSIONS
A(2)A	PATR	IOTIC
A(2)A	PERM	ISSION
A(2)A	PHIL	IPPINES
A(2)A	PR	INCIPAL
A(2)A	PR	INCIPLE
A(2)A	PR	INTING
A(2)A	PR	IORITY
A(2)A	RAD	IATION
A(2)A	REF	ILLING
A(2)A	RESTR	ICTION
A(2)A	RETAL	IATION
A(2)A	REV	IEWING
A(2)A	SH	IPPING
A(2)A(1)A	S	IGNIFICANT
A(2)A(1)A	S	IGNIFICANCE
A(2)A	S	IGNIFY
A(2)A	S	INKING
A(2)A	SK	IRMISH
A(2)A	STAT	ISTICS
A(2)A	SUBM	ISSION
A(2)A	SUPER	IORITY
A(2)A	SW	IMMING
A(2)A	TRANSM	ISSION
A(2)A	VAR	IATION
A(2)A	V	ICTIM
A(2)A	W	ILLIAM
A(2)A	W	ITHIN
A(2)A	AVAI	LABLE
A(2)A	FUE	LOIL
A(2)A	PARA	LLEL
A(2)A	COM	MITMENT
A(2)A		MAIM

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) —Continued

A(2)A	MEDIU	MBOMBER	A(2)A	I	NCENDIARY
A(2)A	ABA	NDON	A(2)A	I	NCENTIVE
A(2)A	ADVA	NCING	A(2)A	INDEPE	NDENT
A(2)A	AFTER	NOON	A(2)A	I	NFANTRY
A(2)A	AN	NOUNCE	A(2)A	I	NLAND
A(2)A(4)A	AN	NOUNCEMENT	A(2)A	INSTA	NTANEOUS
A(2)AA	A	NTENNA	A(2)A	I	NTEND
A(2)A	ASSIG	NMENT	A(2)A	I	NTENSIVE
A(2)A	ASSIG	NMENTS	A(2)A	I	NTENT
A(2)A	ATTAI	NMENT	A(2)A(3)A	I	NTENTION
A(2)A	BEGI	NNING	A(2)A	INTER	NMENT
A(2)A	BI	NDING	A(2)A	I	NVENT
A(2)A	COMMA	NDANT	A(2)A	I	NVENTED
A(2)A	COMMA	NDING	A(2)A(3)A	I	NVENTION
A(2)A	CO	NCENTRATE	A(2)A	LA	NDING
A(2)A(5)A	CO	NCENTRATING	A(2)A(1)A	MAI	NTENANCE
A(2)A(6)A	CO	NCENTRATION	A(2)A	MA	NGANESE
A(2)A	CO	NDENSED	A(2)A	MA	NNING
A(2)A	CO	NFINE	A(2)A		NOON
A(2)A(3)A	CO	NFINEMENT	A(2)A	OPI	NION
A(2)A(1)A	CO	NTINENTAL	A(2)A	PAI	NTING
A(2)A(2)A	CO	NTINGENT	A(2)A	PLA	NNING
A(2)A	CONTI	NGENT	A(2)A	PO	NTON
A(2)A	CO	NTINUAL	A(2)A	PRI	NTING
A(2)A	CO	NTINUE	A(2)A	QUARA	NTINE
A(2)A	CO	NTINUOUS	A(2)A	RU	NNING
A(2)A(5)A	CO	NTINUATION	A(2)A	SE	NTENCE
A(2)A	CONVE	NIENT	A(2)A	SE	NTINEL
A(2)A(2)A	CO	NVENIENT	A(2)A	SI	NKING
A(2)A	CORRESPO	NDENCE	A(2)A	SU	NKEN
A(2)A	CORRESPO	NDING	A(2)A	U	NION
A(2)A	DEPE	NDENT	A(2)A	UNK	NOWN
A(2)A	DISCONTI	NUANCE	A(2)A	U	NTENABLE
A(2)A	DISCO	NTINUE	A(2)A(4)A	ACC	OMMODATION
A(2)A(2)A	DISCO	NTINUANCE	A(2)A	AER	ODROME
A(2)A	ECHELO	NMENT	A(2)A	B	OTTOM
A(2)A	E	NGINE	A(2)A	B	OYCOTT
A(2)A	E	ENGINEER	A(2)A	C	OMMON
A(2)A(4)A	E	NGINEERING	A(2)A	C	OMPOSED
A(2)A(5)A	E	NTANGLEMENT	A(2)A(4)A	C	OMPOSITION
A(2)A	E	NTENTE	A(2)A(5)A	C	ONFORMATION
A(2)A	ENTERTAI	NMENT	A(2)A	C	ONVOY
A(2)A	EXTE	NDING	A(2)A	C	ORPORAL
A(2)A	FI	NDING	A(2)A(4)A	C	ORPORATION
A(2)A	FLA	NKING	A(2)A	CUST	OMHOUSE
A(2)A	FORE	NOON	A(2)A	D	OCTOR
A(2)A	GOVER	NMENT	A(2)A	EN	ORMOUS

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) —Continued

A(2)A	EXPL	OSION
A(2)A	EXPL	OSIONS
A(2)A	F	OGHORN
A(2)A	F	OLLOW
A(2)A	FO	OTHOLD
A(2)A	G	ONIOMETER
A(2)A	GYR	OSCOPIC
A(2)A	L	OOKOUT
A(2)A	N	ONCOMBATANT
A(2)A		OBSOLETE
A(2)A		OCTOBER
A(2)A		OPPOSE
A(2)A		OPPOSITE
A(2)A(4)A		OPPOSITION
A(2)A	P	OISON
A(2)A	P	ONTON
A(2)AA	P	ONTOON
A(2)A	P	OSTOFFICE
A(2)A	PROM	OTION
A(2)A	REC	ONNOITER
A(2)A	REC	ONNOITERING
A(2)A	SCHO	OLHOUSE
A(2)A	TOM	ORROW
A(2)A	VICT	ORIOUS
A(2)A	AP	PROPRIATE
A(2)A	IM	PROPER
A(2)A		PREPARATION
A(2)A		PREPARE
A(2)A		PREPAREDNESS
A(2)A		PREPARING
A(2)A		PROPER
A(2)A		PROPORTION
A(2)A		PROPOSALS
A(2)A		PROPOSE
A(2)A		PUMP
A(2)A		PURPOSE
A(2)A		PURPOSES
A(2)A	AE	RODROME
A(2)A	AI	RBORNE
A(2)A	APP	ROPRIATE
A(2)A	A	RMOR
A(2)A(4)A	A	RMOREDCAR
A(2)A	A	RMORY
A(2)A	CAR	RIER
A(2)A	CO	RPORAL
A(2)A	CO	RPORATION
A(2)A	COU	RIER
A(2)A	DEPA	RTURE
A(2)A	DESE	RTER
A(2)A	DETE	RIORATE
A(2)A	E	RROR
A(2)A	EXTE	RIOR
A(2)A(4)A	EXT	RAORDINARY
A(2)A	FEB	RUARY
A(2)A	FO	RWARD
A(2)A	HA	RBOR
A(2)A	HEADQUA	RTERS
A(2)A	HYD	ROGRAPHIC
A(2)A	INTE	RFERE
A(2)A	INTE	RFERENCE
A(2)A	INTE	RFERING
A(2)A	INTE	RIOR
A(2)A	MI	RROR
A(2)A	MO	RTAR
A(2)A	MU	RDER
A(2)A	OBSE	RVER
A(2)A	O	RDER
A(2)A	O	RDERED
A(2)A	O	RDERS
A(2)A	PA	RAGRAPH
A(2)A	PE	RFORMANCE
A(2)A	P	RAIRIE
A(2)AA	P	REARRANGED
A(2)A	P	RIOR
A(2)A	P	RIORITY
A(2)A	P	ROGRAM
A(2)A	P	ROGRESS
A(2)A	P	ROGRESSIVE
A(2)A	QUA	RTER
A(2)A	QUA	RTERS
A(2)A(5)A	QUA	RTERMASTER
A(2)A		REAR
A(2)A(3)A		REARGUARD
A(2)A	RECO	RDER
A(2)A		RECREATION
A(2)A		RECREATIONAL
A(2)A		RECRUIT
A(2)A		RECRUITING
A(2)A		REORGANIZATION
A(2)A		REPRESENT
A(2)A		REPRESENTATIVE
A(2)A		REPRESENTATION
A(2)A		REPRISAL
A(2)A		REPRISALS

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) —Continued

A(2)A		RETREAT
A(2)A		RETROACTIVE
A(2)A	STA	RTER
A(2)A	SUPE	RIOR
A(2)A	SUPE	RIORITY
A(2)A	TE	RROR
A(2)A	WA	RFARE
A(2)A	ADDRE	SSES
A(2)AA	A	SPOSSIBLE
A(2)A	AS	SESSMENT
A(2)A(4)A	AS	SESSMENTS
A(2)AA	A	SSESSMENT
A(2)AA(4)A	A	SSESSMENTS
A(2)A	AS	SETS
A(2)A	A	SSIST
A(2)A	A	SSISTANT
A(2)A	A	SSISTANCE
A(2)AA	CARELES	SNESS
A(2)A	CEN	SORSHIP
A(2)A	CHA	SSIS
A(2)A	CRUI	SERS
A(2)AA	DI	SCUSS
A(2)AA	DI	SCUSSED
A(2)AA	DI	SCUSSION
A(2)A	DI	SEASE
A(2)AA	DI	SMISSAL
A(2)AA	DI	SMISS
A(2)A	DI	SPOSITION
A(2)A	EMBAS	SIES
A(2)A	GLA	SSES
A(2)A	HEAVYLO	SSES
A(2)A	IS	SUES
A(2)A	LO	SSES
A(2)A	PA	SSES
A(2)A	POS	SESSION
A(2)AA	PO	SSESSION
A(2)A	PROPO	SALS
A(2)A	REPRI	SALS
A(2)A		SESSION
A(2)A(1)A		SUBSISTENCE
A(2)A		SUBSTITUTE
A(2)A		SUBSTITUTION
A(2)A		SUNSET
A(2)AA	TRAN	SMISSION
A(2)A	VES	SELS
A(2)A	VI	SITS
A(2)A	WITNE	SSES
A(2)A	ADJU	TANT
A(2)A	ADMINIS	TRATIVE
A(2)A	ADMINIS	TRATION
A(2)A	ARBI	TRATION
A(2)A	ASSIS	TANT
A(2)A	AT	TENTION
A(2)A	CA	TASTROPHE
A(2)A	CIRCUMS	TANTIAL
A(2)A	COMBA	TANT
A(2)A	CONCEN	TRATE
A(2)A	CONCEN	TRATING
A(2)A	CONCEN	TRATION
A(2)A	CON	TACT
A(2)A	DEMONS	TRATE
A(2)A	DEMONS	TRATED
A(2)A	DEMONS	TRATION
A(2)A	DE	TECTOR
A(2)A	DE	TENTION
A(2)A	EN	TENTE
A(2)A(6)A	EN	TERTAINMENT
A(2)A	EX	TENT
A(2)A	ILLUS	TRATE
A(2)A	ILLUS	TRATION
A(2)A	IMPOR	TANT
A(2)A	INCOMPE	TENT
A(2)A	INI	TIATE
A(2)A	INS	TANT
A(2)A	INS	TANTANEOUS
A(2)A	INS	TANTLY
A(2)A	IN	TENT
A(2)A	IN	TENTION
A(2)A	NONCOMBA	TANT
A(2)A	OU	TPUT
A(2)A	PENE	TRATE
A(2)A	PENE	TRATION
A(2)A	PERSIS	TENT
A(2)A	PRO	TECT
A(2)A	PRO	TECTED
A(2)A	PRO	TECTION
A(2)A	PRO	TECTOR
A(2)A	PRO	TEST
A(2)A	PRO	TESTED
A(2)A	PRO	TESTS
A(2)A	REGIS	TRATION
A(2)A	RE	TENTION
A(2)A	SI	TUATION
A(2)A	S	TART

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) —Continued

A(2)A	S	TARTER	A(3)A	ESTIM	ATEDAT
A(2)A	STA	TISTICS	A(3)A	EX	AMINATION
A(2)A	S	TRATEGIC	A(3)A	GENER	ALALARM
A(2)A	S	TRATEGICAL	A(3)A	GENER	ALSTAFF
A(2)A	S	TRATEGY	A(3)A	HE	ADQUARTERS
A(2)A		TACTICAL	A(3)A	L	ABORATORY
A(2)A		TACTICS	A(3)A	L	ANGUAGE
A(2)A		TATOO	A(3)A	M	AINTAIN
A(2)A		TENT	A(3)A	M	AINTAINED
A(2)A(1)A		TENTATIVE	A(3)A	M	ANUFACTURE
A(2)A		TENTH	A(3)A	M	ARSHAL
A(2)A		TEXT	A(3)A	M	ARTIAL
A(2)A		THAT	A(3)A	N	ATURAL
A(2)A		THATHAVE	A(3)A	N	ATURALIZE
A(2)AA		THATTHE	A(3)A	NATUR	ALIZATION
A(2)A	TWEN	TIETH	A(3)A(3)A	N	ATURALIZATION
A(2)A	WA	TERTANK	A(3)A	N	AVIGATION
A(2)A	AGRIC	ULTURAL	A(3)A	ORG	ANIZATION
A(2)A	D	UGOUT	A(3)A	P	ANAMA
A(2)A	O	UTGUARD	A(3)A	R	AILWAY
A(2)A	O	UTPUT	A(3)A	RE	ARGUARD
A(2)A	P	URSUE	A(3)A	RECONN	AISSANCE
A(2)A	P	URSUIT	A(3)A	REORG	ANIZATION
A(2)A(6)A		UNSUCCESSFUL	A(3)A	S	ABOTAGE
A(2)A		UNSUITABLE	A(3)A	S	ANITARY
A(2)A	RE	VOLVE	A(3)A	S	ANITATION
A(2)A	RE	VOLVER	A(3)A	SPE	ARHEAD
A(2)A	AN	YWAY	A(3)A	TR	ANSPACIFIC
A(2)A		ZIGZAG	A(3)A		CAPACITY
A(3)A		ACTUALLY	A(3)A		CHURCH
A(3)A		ANIMAL	A(3)A(4)A		COINCIDENCE
A(3)A		ANNUAL	A(3)A		CONSCRIPTION
A(3)A(4)A		ANTIAIRCRAFT	A(3)A		COUNCIL
A(3)A		ANYWAY	A(3)A	DEFI	CIENCY
A(3)A		APPEAR	A(3)A	EFFI	CIENCY
A(3)A(1)A		APPEARANCE	A(3)A	ELE	CTRICITY
A(3)A		APPEARED	A(3)A	GYROS	COPIC
A(3)A		AVERAGE	A(3)A	INEFFI	CIENCY
A(3)A		AWKWARD	A(3)A	PA	CIFIC
A(3)A	C	ANADA	A(3)A	SPE	CIFIC
A(3)A	C	ARRIAGE	A(3)A	SPE	CIFICATION
A(3)A	CENTR	ALIZATION	A(3)A	TE	CHNICAL
A(3)A	CIRCUMST	ANTIAL	A(3)A	TRANSPA	CIFIC
A(3)A	DIS	APPEAR	A(3)A		DECIDE
A(3)A	DIS	APPEARED	A(3)A(1)A		DECIDED
A(3)A	E	ASTWARD	A(3)A		DECODE
A(3)A	EL	ABORATE	A(3)A		DIVIDE

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) —Continued

A(3)A		DIVIDING	A(3)A	ENV	ELOPE
A(3)A	HIN	DERED	A(3)A		ERASE
A(3)A	IN	DIVIDUAL	A(3)A		ERASER
A(3)A	MAN	DATED	A(3)A	EXP	EDITE
A(3)A	OR	DERED	A(3)A	EXP	ERIMENT
A(3)A	RE	DUCED	A(3)A		EXPRESS
A(3)A	SURREN	DERED	A(3)A(1)A		EXTREME
A(3)A	WE	DNESDAY	A(3)A	FUS	ELAGE
A(3)A	WIN	DWARD	A(3)A	G	EORGE
A(3)A	ASS	EMBLE	A(3)A	GOV	ERNMENT
A(3)A	ASS	ESSMENT	A(3)A	GR	ENADE
A(3)A	ASS	ESSMENTS	A(3)A	H	EAVIER
A(3)A	ATT	EMPTED	A(3)A	ILLIT	ERATE
A(3)A	AV	ERAGE	A(3)A	IMP	EDIMENTA
A(3)AA(1)A	B	EENNEEDED	A(3)A	INS	ECURE
A(3)A(1)A	BE	ENNEEDED	A(3)A	INT	ERNMENT
A(3)A	B	EETLE	A(3)A	INT	ERPRETATION
A(3)A	B	EFORE	A(3)A(1)A	INT	ERPRETER
A(3)A	B	ETWEEN	A(3)A	INT	ERVIEW
A(3)A	CAREL	ESSNESS	A(3)A	L	EAGUE
A(3)A	C	EMETERY	A(3)A	OP	ERATE
A(3)A	COMPL	ETENESS	A(3)A(2)A	OV	ERWHELMED
A(3)A	CONC	EALMENT	A(3)A	PAR	ENTHESIS
A(3)A	COOP	ERATE	A(3)A(1)A	PAR	ENTHESES
A(3)A	CORR	ECTNESS	A(3)A	PR	ECEDE
A(3)A	D	ECIDE	A(3)A(2)A	PR	ECEDENCE
A(3)A	D	ECIDED	A(3)A(2)A	PR	EFERENCE
A(3)A	D	ECODE	A(3)A	PR	EPARE
A(3)A	D	ECREE	A(3)A(2)A	PR	EPAREDNESS
A(3)A	D	EGREE	A(3)A	PR	ESIDENT
A(3)A	D	ELAYED	A(3)A	PR	ESIDENTIAL
A(3)A	D	ELIVER	A(3)A	PROC	EDURE
A(3)A	DEV	ELOPE	A(3)A	R	EACHED
A(3)A	DEV	ELOPED	A(3)A	R	ECOVER
A(3)A	D	EVICE	A(3)A	R	EDUCE
A(3)A	D	EVISE	A(3)A	R	EDUCED
A(3)A		EASTERLY	A(3)A(2)A	R	EFERENCE
A(3)A		EASTERN	A(3)A	R	EFUGE
A(3)A	ECH	ELONED	A(3)AA	R	EFUGEE
A(3)A		EITHER	A(3)A	R	EFUSE
A(3)A		ELEMENT	A(3)A	R	EGIMENTAL
A(3)A		ELEMENTARY	A(3)A	R	EGIMENT
A(3)A	EL	EVATE	A(3)A	R	ESCUE
A(3)A		ELEVEN	A(3)A	R	ESUME
A(3)A		ENTRENCH	A(3)A	R	ETIRE
A(3)A(3)A		ENTRENCHED	A(3)A	SCH	EDULE
A(3)A	ENTR	ENCHED	A(3)A	S	ECURE

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) —Continued

A(3)A	S	ETTLE	A(3)A	D	ISTRIBUTE
A(3)A	SEV	ENTEEN	A(3)A	DISTR	IBUTING
A(3)A	SEV	ENTEENTH	A(3)A	DISTR	IBUTION
A(3)A	S	EVERE	A(3)A(3)A	D	ISTRIBUTING
A(3)AA	SMOK	ESCREEN	A(3)A(3)A	D	ISTRIBUTION
A(3)A	SP	EARHEAD	A(3)A	D	ISTRICT
A(3)A	THER	EFORE	A(3)A	D	ISTRICTS
A(3)A	TW	ENTIETH	A(3)A	D	IVIDING
A(3)A	W	EATHER	A(3)A	D	IVISION
A(3)A		GARAGE	A(3)A	D	IVISIONS
A(3)A		GEORGE	A(3)A	DOM	INATION
A(3)A		GOING	A(3)A	ENC	IRCLING
A(3)A	C	HURCH	A(3)A	EST	IMATION
A(3)A	FLAS	HLIGHT	A(3)A	EXAM	INATION
A(3)A	P	HOSPHOROUS	A(3)A	EXH	IBITION
A(3)A	SC	HOOLHOUSE	A(3)A	EXTERM	INATION
A(3)A	SEARC	HLIGHTS	A(3)A	EXT	INGUISH
A(3)A	T	HATTHE	A(3)A	FAC	ILITIES
A(3)A	T	HOUGH	A(3)A	F	IGHTING
A(3)A	ACT	IVITIES	A(3)A	HOST	ILITIES
A(3)A	ANTIC	IPATION	A(3)A	IDENTIF	ICATION
A(3)A	APPL	ICATION	A(3)A	ILLUM	INATING
A(3)A	ART	IFICIAL	A(3)A	ILLUM	INATION
A(3)A	AUD	IBILITY	A(3)A(1)A		INCLINING
A(3)A	BR	IGADIER	A(3)A	IND	ICATING
A(3)A	CENTRAL	IZATION	A(3)A	IND	ICATION
A(3)A	C	IRCUIT	A(3)A		INFLICT
A(3)A	C	IRCUITOUS	A(3)A(2)A		INFLICTING
A(3)A	C	ITATION	A(3)A		INITIATE
A(3)A	CLASSIF	ICATION	A(3)A		INQUIRE
A(3)A	COMMUN	ICATION	A(3)A		INQUIRY
A(3)A	CONST	ITUTING	A(3)A	INSP	IRATION
A(3)A	CONST	ITUTION	A(3)A(3)A		INSPIRATION
A(3)A	COORD	INATION	A(3)A		INSPIRE
A(3)A	CR	ITICISE	A(3)A	INST	ITUTION
A(3)A	CR	ITICISM	A(3)A(3)A		INSTITUTION
A(3)A	DED	ICATION	A(3)A	INVEST	IGATION
A(3)A	DEF	INITION	A(3)A	INVEST	IGATIONS
A(3)A	DEMOBIL	IZATION	A(3)A	INV	ITATION
A(3)A	DETERM	INATION	A(3)A	IRR	IGATIONS
A(3)A	D	IMINISH	A(3)A		ISSUING
A(3)A	D	IRIGIBLE	A(3)A	LIM	ITATION
A(3)A	DISSEM	INATION	A(3)A	L	IMITING
A(3)A	DIST	INCTION	A(3)A	MA	INTAIN
A(3)A	DIST	INGUISH	A(3)A	MA	INTAINED
A(3)A	DIST	INGUISHED	A(3)A	M	ILITIA
A(3)A(2)A	DIST	INGUISHING	A(3)A	MOBIL	IZATION

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U)—Continued

A(3)A	NATURAL	IZATION	A(3)A	E	NCOUNTERED
A(3)A	NAV	IGATION	A(3)A	E	NTRENCH
A(3)A	ORGAN	IZATION	A(3)A	E	NTRENCHED
A(3)A	PRELIM	INARIES	A(3)A	EXPA	NSION
A(3)A	QUALIF	ICATION	A(3)A	EXTE	NSION
A(3)A	RECONNO	ITERING	A(3)A	ILLUMI	NATING
A(3)A	REORGAN	IZATION	A(3)A	I	NDEMNITY
A(3)A	REQU	ISITION	A(3)A	I	NSIGNIA
A(3)A	RESPONS	IBILITY	A(3)A	I	NSTANT
A(3)A	SAN	ITATION	A(3)A	I	NSTANTLY
A(3)A	SEM	IRIGID	A(3)A(2)A	I	NSTANTANEOUS
A(3)A	S	IGHTING	A(3)A	INTE	NTION
A(3)A	SIM	ILARITY	A(3)A	I	NTERNAL
A(3)A	SPECIF	ICATION	A(3)A(4)A	I	NTERNATIONAL
A(3)A	SUBST	ITUTION	A(3)A(2)A	I	NTERNMENT
A(3)A(1)A	SU	ITABILITY	A(3)A	INTERVE	NTION
A(3)A	VERIF	ICATION	A(3)A	I	NTRENCH
A(3)A	VETER	INARIAN	A(3)A	INVE	NTION
A(3)A	V	ICINITY	A(3)A	LAU	NCHING
A(3)A	VIS	IBILITY	A(3)A	MACHI	NEGUN
A(3)A(1)A	V	ISIBILITY	A(3)A	MAI	NTAIN
A(3)A	CO	LONEL	A(3)A	MAI	NTAINED
A(3)A	COMP	LETELY	A(3)A	MOU	NTAIN
A(3)A	F	LASHLIGHT	A(3)A		NOTING
A(3)A	IL	LEGAL	A(3)A	O	NEHUNDRED
A(3)A		LEVEL	A(3)A	PO	NTOON
A(3)A		LITTLE	A(3)A	REAPPOI	NTMENT
A(3)A		LOCAL	A(3)A	RETE	NTION
A(3)A	SEA	LEVEL	A(3)A	SEVE	NTEEN
A(3)A	A	MUSEMENT	A(3)A	SEVE	NTEENTH
A(3)A	CO	MMITMENT	A(3)A	SUSPE	NSION
A(3)A(1)A		MAXIMUM	A(3)A	U	NIDENTIFIED
A(3)A(1)A		MINIMUM	A(3)A	AIRC	ONTROL
A(3)A		MOVEMENT	A(3)A	AN	ONYMOUS
A(3)A	ALTER	NATING	A(3)A	CHR	ONOLOGICAL
A(3)A(4)A	A	NNOUNCEMENT	A(3)AA	C	ODEBOOK
A(3)A	A	NTENNA	A(3)A	C	ONTROL
A(3)A	APPOI	NTMENT	A(3)A	C	ONTROVERSY
A(3)A	ASCE	NSION	A(3)A	CR	OSSROADS
A(3)A	ATTE	NTION	A(3)A	FIREC	ONTROL
A(3)A(1)A	CO	NCERNING	A(3)A	F	OOTHOLD
A(3)A	CO	NDEMN	A(3)AA	F	ORENOON
A(3)A	CO	NDEMNED	A(3)A	H	ORIZON
A(3)A	CONFI	NEMENT	A(3)A	LAB	ORATORY
A(3)A	CO	NTAIN	A(3)A	L	OCOMOTIVE
A(3)A	DETE	NTION	A(3)A	METE	OROLOGICAL
A(3)A	DIME	NSION	A(3)A	M	ONOPOLY

Table D–7 ~~(C)~~. List of words containing like letters repeated at various intervals (U)—Continued

A(3)A		OUTBOARD
A(3)A		OUTPOST
A(3)A		OUTPOSTS
A(3)A	PH	OSPHORUS
A(3)A	P	ONTOON
A(3)A	P	OSTPONE
A(3)A	PROP	ORTION
A(3)A	PR	OTOCOL
A(3)A	A	PPROPRIATE
A(3)A		PASSPORT
A(3)A		PHOSPHORUS
A(3)A		POSTPONE
A(3)A		PROMPT
A(3)A	TROO	PSHIP
A(3)A	TROO	PSHIPS
A(3)A	A	RBITRATION
A(3)A	B	RIBERY
A(3)A	CA	RRIER
A(3)A	CONT	ROVERSY
A(3)A	COR	RIDOR
A(3)A	C	ROSSROADS
A(3)A	DEST	ROYERS
A(3)A	DEST	ROYER
A(3)A	E	RASER
A(3)A	FA	RTHER
A(3)A	FU	RTHER
A(3)A	IMP	ROPER
A(3)A	INTERP	RETER
A(3)A	LABO	RATORY
A(3)A	NO	RTHERN
A(3)A	NO	RTHERLY
A(3)A	OPE	RATOR
A(3)A	P	REARRANGED
A(3)A	P	REFER
A(3)A	P	REFERENCE
A(3)AA	P	REFERRED
A(3)A	P	REPARATION
A(3)A	P	REPARE
A(3)A	P	REPAREDNESS
A(3)A	P	REPARING
A(3)A	P	RESCRIBED
A(3)A	P	RESERVATION
A(3)A	P	RESERVE
A(3)A	P	RIMARY
A(3)A	P	ROPER
A(3)A	P	ROPORTION
A(3)A		RAILROAD
A(3)A	REA	RGUARD
A(3)A		RECORD
A(3)A(2)A		RECORDER
A(3)A		REDCROSS
A(3)A		REFER
A(3)A		REFERENCE
A(3)A		REGARDING
A(3)A		REPORT
A(3)A		REPORTED
A(3)A		RESERVATION
A(3)A		RESERVE
A(3)A		RESERVES
A(3)A		RESTRAINT
A(3)A		RESTRICTED
A(3)A		RESTRICTION
A(3)A		RETIRE
A(3)A		RETIRING
A(3)A		RETURN
A(3)A		RETURNED
A(3)A		RETURNING
A(3)A		REVERSE
A(3)A		RIGOROUS
A(3)A		RIVER
A(3)A		ROGER
A(3)A	SEC	RETARY
A(3)A	TEMPE	RATURE
A(3)A	TER	RITORY
A(3)A	THE	REFORE
A(3)A	T	RAVERSE
A(3)A	VETE	RINARIAN
A(3)A	A	SCENSION
A(3)A	A	SPOSSIBLE
A(3)A	A	SSESSMENT
A(3)A(4)A	A	SSESSMENTS
A(3)A	A	SSETS
A(3)A	BALLI	STICS
A(3)A	BATTLE	SHIPS
A(3)AA	BU	SINESS
A(3)AA	CARELE	SSNESS
A(3)A	CARELES	SNESS
A(3)A	COLLI	SIONS
A(3)A	DI	SCUSS
A(3)A	DI	SCUSSED
A(3)A	DI	SCUSSION
A(3)A	DI	SMISSAL
A(3)A	DI	SMISS
A(3)A	DI	SPERSE

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) —Continued

A(3)A	DI	SPERSED
A(3)A	DI	SPERSION
A(3)AA	DI	STRESS
A(3)AA	DI	STRESSED
A(3)A	DIVI	SIONS
A(3)A	EMBA	SSIES
A(3)A	EXPLO	SIONS
A(3)A	I	SSUES
A(3)A	LOGI	STICS
A(3)A	MARK	SMANSHIP
A(3)A	MES	SAGES
A(3)A	MIS	SIONS
A(3)A	PO	SSESSION
A(3)A	PROVI	SIONS
A(3)A	RE	SPONSIBLE
A(3)A	RE	SPONSIBILITY
A(3)A		SATISFACTORY
A(3)A		SATISFY
A(3)A		SHIPS
A(3)A	STATI	STICS
A(3)AA		STRESS
A(3)A	SU	SPENSE
A(3)A	SU	SPENSION
A(3)A	TRAN	SMISSION
A(3)A	TRAN	SVERSE
A(3)A	TROOP	SHIPS
A(3)AA	U	SELESS
A(3)A	VE	SSELS
A(3)A	WAR	SHIPS
A(3)A	AC	TIVITY
A(3)A	AC	TIVITIES
A(3)A	ALLO	TMENT
A(3)A	AN	TEDATING
A(3)A	APPOIN	TMENT
A(3)A	A	TLANTIC
A(3)A	AT	TEMPT
A(3)A	AT	TEMPTED
A(3)A	A	TTENTION
A(3)A	AU	TOMATIC
A(3)A	COMMI	TMENT
A(3)A	COMPAR	TMENT
A(3)A	CONS	TITUTE
A(3)A	CONS	TITUTION
A(3)A	CONS	TRUCTION
A(3)A	CON	TRACT
A(3)AA	COUN	TERATTACK
A(3)A	DEPAR	TMENT
A(3)A	DEPAR	TMENTAL
A(3)A	DES	TITUTE
A(3)A	DES	TRUCTION
A(3)A	DE	TONATE
A(3)A	DE	TONATED
A(3)A	DE	TONATION
A(3)A	DIS	TINCTION
A(3)A	DIS	TRICT
A(3)A	DIS	TRICTS
A(3)A	EIGH	TEENTH
A(3)A	ENLIS	TMENT
A(3)A	ES	TIMATE
A(3)A	ES	TIMATION
A(3)A	ESTIMA	TEDAT
A(3)A	ES	TIMATES
A(3)A(3)A	ES	TIMATEDAT
A(3)A	EX	TRACT
A(3)A	FA	TALITY
A(3)A	FIF	TEENTH
A(3)A	FOUR	TEENTH
A(3)A	HOS	TILITY
A(3)A	HOS	TILITIES
A(3)A	ILLI	TERATE
A(3)A	INS	TITUTION
A(3)A	INS	TRUCT
A(3)A	INS	TRUCTION
A(3)A	INS	TRUCTIONS
A(3)A	INS	TRUCTOR
A(3)A	INVES	TIGATE
A(3)A	INVES	TIGATION
A(3)A	INVES	TIGATIONS
A(3)A	NINE	TEENTH
A(3)A	OBS	TRUCTIONS
A(3)A	OU	TPOST
A(3)A	OU	TPOSTS
A(3)A	PA	TRIOTIC
A(3)A	REAPPOIN	TMENT
A(3)A	RECONS	TRUCTION
A(3)A	REENLIS	TMENT
A(3)A	RES	TRICTED
A(3)A	RES	TRICTION
A(3)A	RE	TREAT
A(3)A	SEVEN	TEENTH
A(3)A	SIX	TEENTH
A(3)A	S	TREET
A(3)A	SUBS	TITUTE
A(3)A	SUBS	TITUTION

Table D–7 (Ȼ). List of words containing like letters repeated at various intervals (U) —Continued

A(3)A		TAXATION	A(4)A	GEOGR	APHICAL
A(3)A		THATTHE	A(4)A	IMPR	ACTICABLE
A(3)A		THIRTEEN	A(4)A	IN	AUGURATION
A(3)A	THIR	TEENTH	A(4)A	INTERN	ATIONAL
A(3)A(3)A		THIRTEENTH	A(4)A	M	ARKSMANSHIP
A(3)A		THIRTY	A(4)A	M	ATERIAL
A(3)A		TRACT	A(4)A	N	ATIONAL
A(3)A		TRACTOR	A(4)A	N	ATIONALISM
A(3)A	TRANSA	TLANTIC	A(4)A	N	ATIONALITY
A(3)A(2)A		TWENTIETH	A(4)A	N	AUTICAL
A(3)A		TWENTY	A(4)A	NAV	ALATTACK
A(3)A		TWENTYFIVE	A(4)A	N	AVALBASE
A(3)A(1)A	UNI	TEDSTATES	A(4)A	N	AVALBATTLE
A(3)A	U	TILITY	A(4)A	P	ARAGRAPH
A(3)A	WARDEPAR	TMENT	A(4)A	P	ARALLAX
A(3)A	WI	THOUT	A(4)A	PR	ACTICAL
A(3)A	B	UREAU	A(4)A	R	AILHEAD
A(3)A	CHA	UFFEUR	A(4)A	R	AILROAD
A(3)A	CIRC	UITOUS	A(4)A	RECRE	ATIONAL
A(3)A	COMM	UNIQUE	A(4)A	S	ATISFACTORY
A(3)A	S	URPLUS	A(4)A	S	ATURDAY
A(3)A	S	URROUND	A(4)A	T	ACTICAL
A(3)A		UNUSUAL	A(4)A	W	ARDEPARMENT
A(3)A		WESTWARD	A(4)A	W	ATERTANK
A(3)A		WINDWARD	A(4)A		BLOCKBUSTER
A(4)A		ADJUTANT	A(4)A		CHARACTER
A(4)A		AERONAUTICS	A(4)A(7)A		CHARACTERISTIC
A(4)A		AIRCRAFT	A(4)A		CHEMICAL
A(4)A		AIRPLANE	A(4)A		CLERICAL
A(4)A		ALASKA	A(4)A	COIN	CIDENCE
A(4)A		ALLOCATION	A(4)A		COLLECT
A(4)A		ALLOWANCE	A(4)A		COLLECTION
A(4)A		ALMANAC	A(4)A		CONDUCT
A(4)A		AMBULANCE	A(4)A		CONNECTING
A(4)A		ANTEDATING	A(4)A		CONNECTION
A(4)A	ANTI	AIRCRAFT	A(4)A		CONTACT
A(4)A		ANTITANK	A(4)A		CORRECTED
A(4)A		APPARATUS	A(4)A		CORRECTION
A(4)A		APPROACH	A(4)A		CORRECTNESS
A(4)A		ARABIA	A(4)A		CORRECT
A(4)A		ARRIVAL	A(4)A		CRITIC
A(4)A		ASSURANCE	A(4)A		CRITICAL
A(4)A		AUTOMATIC	A(4)A		CRITICISE
A(4)A		AVAILABLE	A(4)A	IN	CIDENCE
A(4)A	BE	ACHHEAD	A(4)A	ME	CHANIC
A(4)A	C	AUSEWAY	A(4)A	PRE	CEDENCE
A(4)A	CO	ASTGUARD	A(4)A	RE	CEPTACLE

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) –Continued

A(4)A		CRITICISM
A(4)A	CON	DEMNED
A(4)A	CON	DENSED
A(4)A		DEFEND
A(4)A		DEFENDER
A(4)A(1)A		DEFENDED
A(4)A(1)A		DEMANDED
A(4)A		DEPEND
A(4)A		DEPENDABLE
A(4)A		DEPENDABILITY
A(4)A		DEPENDENT
A(4)A		DISLODGE
A(4)A		DOWNED
A(4)A	IN	DEPENDENT
A(4)A	ALT	ERNATE
A(4)A	ASS	EMBLIES
A(4)A	B	EACHHEAD
A(4)A	B	ECAUSE
A(4)A(1)A	B	EENNEEDED
A(4)A(1)A	B	ELLIGERENT
A(4)A	B	ESIEGED
A(4)A	C	ENTERED
A(4)A	COMM	ENCEMENT
A(4)A	COMP	ENSATE
A(4)A	CONF	ERENCE
A(4)A	CONSID	ERABLE
A(4)A	D	ECEMBER
A(4)A	D	ECIPHER
A(4)A(1)A	D	ECIPHERED
A(4)A(2)A	D	ECIPHERMENT
A(4)A	D	ECLARE
A(4)A	D	ECLARED
A(4)A	D	EFEATED
A(4)A	DEF	ECTIVE
A(4)A	D	EFENDER
A(4)A	D	EFENDED
A(4)A	D	EFENSE
A(4)A	D	EFENSES
A(4)A	DEF	ENSIVE
A(4)A	D	EFERRED
A(4)A	D	EFICIENT
A(4)A	D	EFICIENCY
A(4)A	D	EMANDED
A(4)A	D	EPARTED
A(4)A	D	EPENDENT
A(4)A	D	EPLOYED
A(4)A	D	EPORTED
A(4)A	D	ESERTED
A(4)A	D	ESERTER
A(4)A	D	ETACHED
A(4)A	DET	ERMINE
A(4)A	DET	ERMINED
A(4)A	DEV	ELOPMENT
A(4)A	DIFF	ERENCE
A(4)A	DIV	EBOMBER
A(4)A	ECH	ELONMENT
A(4)A	EFF	ECTIVE
A(4)AA		EIGHTEEN
A(4)AA		EIGHTEENTH
A(4)A	ELS	EWHERE
A(4)A		EMERGENCY
A(4)A		ENCODE
A(4)A		ENCODED
A(4)A		ENEMIES
A(4)A		ENGAGE
A(4)A(1)A		ENGAGEMENT
A(4)A		ENGINE
A(4)AA		ENGINEER
A(4)AA		ENGINEERING
A(4)A		ENTIRE
A(4)A		EUROPE
A(4)A		EUROPEAN
A(4)A	EXC	ESSIVE
A(4)A		EXCITE
A(4)A(1)A		EXCITEMENT
A(4)A	EX	ERCISE
A(4)A	EX	ERCISES
A(4)A	EXP	ENSIVE
A(4)A	EXT	ENSIVE
A(4)A	FL	EXIBLE
A(4)A	IMM	EDIATE
A(4)A	IMPR	ESSIVE
A(4)A	INC	ENTIVE
A(4)A	INCOMP	ETENCE
A(4)A	IND	EPENDENT
A(4)A	INT	ELLIGENT
A(4)A(2)A	INT	ELLIGENCE
A(4)A	INT	ENSIVE
A(4)A	INTERF	ERENCE
A(4)A	INT	ERFERE
A(4)A(2)A	INT	ERFERENCE
A(4)A	INTERM	EDIATE
A(4)A	INT	ERPOSE
A(4)A	INT	ERVENE

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) –Continued

A(4)A	L	ECTURE
A(4)A	L	ETTERED
A(4)A	MAINT	ENANCE
A(4)A(1)A	M	EASUREMENT
A(4)A(1)A	M	EASUREMENTS
A(4)A	M	ESSAGE
A(4)A	M	ESSAGES
A(4)A	MISC	ELLANEOUS
A(4)A	N	EGLIGENT
A(4)A(2)A	N	EGLIGENCE
A(4)A	OBJ	ECTIVE
A(4)A	OFF	ENSIVE
A(4)A	PEN	ETRATE
A(4)A	P	ERMANENT
A(4)A	PREC	EDENCE
A(4)A	PREF	ERENCE
A(4)A	PR	EFERRED
A(4)A	PR	ESERVE
A(4)A	PR	ESSURE
A(4)A	PROGR	ESSIVE
A(4)A	RANG	EFINDER
A(4)A	R	EADINESS
A(4)A	R	ECEIVE
A(4)A	R	ECEIVER
A(4)A	R	ECOMMEND
A(4)A	R	ECOMMENDATION
A(4)A(2)A	R	ECOMMENDED
A(4)A	R	ECORDER
A(4)A	REF	ERENCE
A(4)A	R	EFUGEE
A(4)A	R	EGISTER
A(4)A	R	EJECTED
A(4)A	R	ELEASE
A(4)A	R	ELIEVE
A(4)A	R	EMEDIES
A(4)A	R	EMEMBER
A(4)A	R	EPAIRED
A(4)A	R	EPEATED
A(4)A	R	EPEATER
A(4)A	R	EPELLED
A(4)A	R	EPLACE
A(4)A(1)A	R	EPLACEMENT
A(4)A	R	EPORTED
A(4)A	R	EPRESENT
A(4)A	R	EPRESENTATION
A(4)A(6)A	R	EPRESENTATIVE
A(4)A	R	EPULSED
A(4)A	R	EQUIRE
A(4)A(1)A	R	EQUIREMENT
A(4)A	R	ESERVE
A(4)A	R	ESERVES
A(4)A	R	ESTORED
A(4)A	R	ETURNED
A(4)A	R	EVENUE
A(4)A	R	EVERSE
A(4)A	R	EVIEWED
A(4)A	R	EVOLVE
A(4)A	R	EVOLVER
A(4)A	S	EALEVEL
A(4)A	S	ELECTED
A(4)A	S	ENTINEL
A(4)A	S	ERVICE
A(4)AA	S	EVENTEEN
A(4)AA	S	EVENTEENTH
A(4)A	SMOK	ESCREEN
A(4)A	SUCC	ESSIVE
A(4)A	SURR	ENDERED
A(4)A	TEL	EPHONE
A(4)A(1)A	TH	ERMOMETER
A(4)A	THR	EATENED
A(4)A	UNT	ENABLE
A(4)A	V	EHICLES
A(4)A		FORTIFIED
A(4)A	EN	GAGING
A(4)A	FI	GHTING
A(4)A	SI	GHTING
A(4)A	BREAKT	HROUGH
A(4)A	S	HARPSHOOTER
A(4)A	T	HROUGH
A(4)A	ARB	ITRATION
A(4)A	CONC	ILIATION
A(4)A	CONF	IDENTIAL
A(4)A	CONF	IRMATION
A(4)A	CONF	ISCATION
A(4)A	CONT	INUATION
A(4)A	DES	IGNATION
A(4)A	D	IETITIAN
A(4)A	DIFF	ICULTIES
A(4)A	D	IMENSION
A(4)A	D	IRECTION
A(4)A(1)A	D	ISPOSITION
A(4)A	D	ISSEMINATED
A(4)A(3)A	D	ISSEMINATION
A(4)A	ENG	INEERING

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) –Continued

A(4)A		IDENTICAL
A(4)A		IDENTIFY
A(4)A(1)A(3)A		IDENTIFICATION
A(4)A		IGNITION
A(4)A		ILLUMINATE
A(4)A(3)A		ILLUMINATING
A(4)A(3)A		ILLUMINATION
A(4)A		IMMEDIATE
A(4)A	IMM	IGRATION
A(4)A		IMPEDIMENTA
A(4)A		INDIVIDUAL
A(4)A(1)A		INEFFICIENCY
A(4)A		INHABITED
A(4)A		INTERIOR
A(4)A		INVADING
A(4)A		INVASION
A(4)A	LEG	ISLATION
A(4)A	L	IABILITY
A(4)A	NAT	IONALISM
A(4)A	NAT	IONALITY
A(4)A	PH	ILIPPINES
A(4)A	PRES	IDENTIAL
A(4)A	RES	IGNATION
A(4)A	S	IGNIFICANT
A(4)A	S	IGNIFICANCE
A(4)A	S	ITUATION
A(4)A(1)A	UN	IDENTIFIED
A(4)A	V	ICTORIOUS
A(4)A	AGRICU	LTURAL
A(4)A	BATT	LEFIELD
A(4)A	E	LIGIBLE
A(4)A	F	LEXIBLE
A(4)A	I	LLEGAL
A(4)A		LEGISLATION
A(4)A		LIABILITY
A(4)A	NAVA	LBATTLE
A(4)A	ATO	MICBOMB
A(4)A	BO	MBARDMENT
A(4)A	COM	MENCEMENT
A(4)A	CO	MPARTMENT
A(4)A	E	MPLOYMENT
A(4)A	I	MPEDIMENTA
A(4)A		MARKSMANSHIP
A(4)A		MEDIUM
A(4)A(2)A		MEDIUMBOMBER
A(4)A		MILLIMETER
A(4)A	AMMU	NITION
A(4)A	ANNOU	NCEMENT
A(4)A	A	NTITANK
A(4)A	ARRA	NGEMENT
A(4)A	CE	NTERING
A(4)A	COI	NCIDENCE
A(4)A	COMME	NCEMENT
A(4)A	CO	NFERENCE
A(4)A	CO	NFIDENCE
A(4)A	CO	NFIDENT
A(4)A	CO	NFIDENTIAL
A(4)A	CON	NECTING
A(4)A	CO	NTINENTAL
A(4)A	COORDI	NATION
A(4)A	DEFI	NITION
A(4)A	DESIG	NATION
A(4)A	DETERMI	NATION
A(4)A	DETO	NATION
A(4)A	DISSEMI	NATION
A(4)A	DISTI	NCTION
A(4)A	DOMI	NATION
A(4)A	E	NDURANCE
A(4)A	E	NGAGING
A(4)A	ENGI	NEERING
A(4)A	E	NTERING
A(4)A	E	NTRAIN
A(4)A	E	NTRAINED
A(4)A	EXAMI	NATION
A(4)A	EXPLA	NATION
A(4)A	EXTERMI	NATION
A(4)A	IG	NITION
A(4)A	ILLUMI	NATION
A(4)A	I	NCIDENT
A(4)A	I	NCIDENCE
A(4)A(2)A	I	NDEPENDENT
A(4)A	I	NFLUENCE
A(4)A	INTER	NATIONAL
A(4)A	I	NVADING
A(4)A	JU	NCTION
A(4)A	MAI	NTENANCE
A(4)A	MU	NITIONS
A(4)A		NATIONALITY
A(4)A		NATIONAL
A(4)A		NATIONALISM
A(4)A	NI	NETEEN
A(4)A	NI	NETEENTH
A(4)A		NOTHING
A(4)A	RA	NGEFINDER

Table D–7 (¢). List of words containing like letters repeated at various intervals (U) –Continued

A(4)A	RECOG	NITION
A(4)A	RESIG	NATION
A(4)A	ROADJU	NCTION
A(4)A	SIG	NALLING
A(4)A	SY	NCHRONIZE
A(4)A	U	NEXPENDED
A(4)A	U	NKNOWN
A(4)A	VETERI	NARIAN
A(4)A	ACCOMM	ODATION
A(4)A	ALL	OCATION
A(4)A	AT	OMICBOMB
A(4)A	C	ODEBOOK
A(4)A	COMP	OSITION
A(4)A	CORP	ORATION
A(4)A	C	ORRIDOR
A(4)A	DEC	ORATION
A(4)A	DET	ONATION
A(4)A	DISP	OSITION
A(4)A	F	ORENOON
A(4)A	INTR	ODUCTORY
A(4)A	L	OCATION
A(4)A		OPINION
A(4)A	OPP	OSITION
A(4)A		OVERCOMING
A(4)A	P	OSITION
A(4)A	P	OSITIONS
A(4)A	PR	OJECTOR
A(4)A	PR	OMOTION
A(4)A	PR	OTECTOR
A(4)A	PR	OVISION
A(4)A	PR	OVISIONS
A(4)A	REV	OLUTION
A(4)A	REV	OLUTIONARY
A(4)A	T	OBACCO
A(4)A	T	OMORROW
A(4)A	T	ORPEDO
A(4)AA		PHILIPPINES
A(4)A	TO	POGRAPHIC
A(4)A	AI	RCONTROL
A(4)A	ARMO	REDCAR
A(4)A	CHA	RACTER
A(4)A	CHA	RACTERISTIC
A(4)A	CI	RCULAR
A(4)A	CO	RRIDOR
A(4)A	C	RUISER
A(4)A	C	RUISERS
A(4)A	DI	RECTOR
A(4)A	EXTRAO	RDINARY
A(4)A	FI	REALARM
A(4)A	INST	RUCTOR
A(4)A	NO	RTHWARD
A(4)A	P	REFERRED
A(4)A	P	RESSURE
A(4)A		REPAIR
A(4)A		REPAIRED
A(4)A		REQUIRE
A(4)A		REQUIREMENT
A(4)A		REQUIRING
A(4)A		RESEARCH
A(4)A		RESOURCES
A(4)A		RESTORED
A(4)A		RUBBER
A(4)A		RUNNER
A(4)A	SUR	RENDER
A(4)A	SUR	RENDERED
A(4)A	TE	RRITORY
A(4)A	T	RACTOR
A(4)A	T	RAILERS
A(4)A	T	RAWLER
A(4)A	T	RIGGER
A(4)A	WA	RDEPARTMENT
A(4)A	ASSES	SMENTS
A(4)A	AS	SOONAS
A(4)A	BU	SINESS
A(4)A	CARELE	SSNESS
A(4)A	CROS	SROADS
A(4)A	DI	STRESS
A(4)A	DI	STRESSED
A(4)A	I	SLANDS
A(4)A	ME	SSAGES
A(4)A	MI	SFIRES
A(4)A	MI	SSIONS
A(4)A	OUT	SKIRTS
A(4)A	PRI	SONERS
A(4)A	RE	SERVES
A(4)A	RE	SPECTS
A(4)A		SHARPSHOOTER
A(4)A		SHELLS
A(4)A		SMOKESCREEN
A(4)A		SPOOLS
A(4)A		SPOONS
A(4)A		STATES
A(4)A(3)A		STATISTICS
A(4)A		STATUS

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) —Continued

A(4)A		STRESS	A(4)A		TARGET
A(4)A		STRIPS	A(4)A		TENTATIVE
A(4)AA		SUBMISSION	A(4)A		TERRITORY
A(4)A		SUBSISTENCE	A(4)A		THREAT
A(4)AA		SUCCESSIVE	A(4)A		THREATENED
A(4)AA		SUCCESS	A(4)A		TRADITIONAL
A(4)AA		SUCCESSFUL	A(4)A		TURRET
A(4)AA		SUCCESSFULLY	A(4)A		TWELFTH
A(4)A		SUGGEST	A(4)A	L	UMINOUS
A(4)A		SUNRISE	A(4)A	MAN	UFACTURE
A(4)A		SUPPOSE	A(5)A		ACCEPTANCE
A(4)A	TRAN	SPORTS	A(5)A		ACCEPTABLE
A(4)A	UNITED	STATES	A(5)A		ACCOMPANY
A(4)AA	UN	SUCCESSFUL	A(5)A		ACCORDANCE
A(4)A	U	SELESS	A(5)A		ADVANTAGEOUS
A(4)A	AL	TERNATING	A(5)A		ADVANTAGE
A(4)A	AL	TERNATE	A(5)A		AEROPLANE
A(4)A	A	TTEMPT	A(5)A		ALLEGIANCE
A(4)A	A	TTEMPTED	A(5)A		ALTERNATING
A(4)A	CHARAC	TERISTIC	A(5)A		ALTERNATE
A(4)A	CON	TINENTAL	A(5)A		AMBASSADOR
A(4)A	CON	TINUATION	A(5)A		AMERICAN
A(4)A	COUN	TERATTACK	A(5)A		ANTENNA
A(4)A	DIS	TRIBUTE	A(5)A		APPEARANCE
A(4)A	DIS	TRIBUTION	A(5)A		APPLICATION
A(4)A	DIS	TRIBUTING	A(5)A		APPROVAL
A(4)A	ELEC	TRICITY	A(5)A		ARBITRARY
A(4)A	EXCI	TEMENT	A(5)A		ARBITRATION
A(4)A	INS	TALLATIONS	A(5)A		ASSISTANT
A(4)A	IN	TEGRITY	A(5)A		ASSISTANCE
A(4)A	IN	TEREST	A(5)A		ASSOCIATE
A(4)A	IN	TERESTING	A(5)A		ASSOCIATION
A(4)A	IN	TERNATIONAL	A(5)A		ASSOONAS
A(4)A	LIEU	TENANT	A(5)A	C	ABLEGRAM
A(4)A	NOR	THEAST	A(5)A	C	AMOUFLAGE
A(4)A	NOR	THWEST	A(5)A	C	ANCELLATION
A(4)A	NOR	THWESTERN	A(5)A	DIS	APPEARANCE
A(4)A	OU	TSKIRTS	A(5)A	EXTR	AORDINARY
A(4)A	REINSTA	TEMENT	A(5)A	M	AINTENANCE
A(4)A	RES	TRAINT	A(5)A	QU	ALIFICATION
A(4)A	RE	TALIATION	A(5)A	QU	ARTERMASTER
A(4)A	RE	TROACTIVE	A(5)A	R	ADIOGRAM
A(4)A	SOU	THEAST	A(5)A	R	ADIOSTATION
A(4)A	SOU	THWEST	A(5)A	STR	ATEGICAL
A(4)A	SOU	THWESTERN	A(5)A	TR	ANSATLANTIC
A(4)A	STA	TEMENT	A(5)A	AC	CEPTANCE
A(4)A	S	TATISTICS	A(5)A	AC	CORDANCE

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) –Continued

A(5)A		CHRONICLE	A(5)A	DISCR	EPANCIES
A(5)A		COEFFICIENT	A(5)A	DISS	EMINATED
A(5)A		COMMENCE	A(5)A		EFFECTED
A(5)A		COMMENCEMENT	A(5)A		EFFICIENT
A(5)A		COMMERCE	A(5)A		EFFICIENCY
A(5)A		CONFISCATION	A(5)A		EIGHTEEN
A(5)A		CONFLICT	A(5)A		EIGHTEENTH
A(5)A		CONTACT	A(5)A		ELEVATE
A(5)A	DIS	CREPANCIES	A(5)A(1)A		ELSEWHERE
A(5)A	DIS	CREPANCY	A(5)A(1)A		EMPLACEMENT
A(5)A	E	CONOMIC	A(5)AA		EMPLOYEE
A(5)A	AD	DRESSED	A(5)A		EMPLOYER
A(5)A	A	DVANCED	A(5)A(2)A		ENCIPHERMENT
A(5)A	BRI	DGEHEAD	A(5)A(1)A		ENCIPHERED
A(5)A		DAMAGED	A(5)A		ENCIPHER
A(5)A		DECIDED	A(5)A(1)A		ENFORCEMENT
A(5)A		DELAYED	A(5)A		ENFORCE
A(5)A		DROPPED	A(5)A		ENGINEER
A(5)A	IN	DICATED	A(5)A		ENGINEERING
A(5)A	ACC	EPTANCE	A(5)A		ENLISTED
A(5)A	ACC	EPTABLE	A(5)A		ENROLLED
A(5)A	ALL	EGIANCE	A(5)A		ENTENTE
A(5)A	APP	EARANCE	A(5)A	ENT	ERPRISE
A(5)A	CAR	ELESSNESS	A(5)A		EQUIPMENT
A(5)A	CL	EARANCE	A(5)A		ESCORTED
A(5)A	CO	EFFICIENT	A(5)A		EXCLUDE
A(5)A	CONC	ENTRATE	A(5)A	EX	ECUTIVE
A(5)A(2)A	CORR	ESPONDENCE	A(5)A		EXPANDED
A(5)A	D	ECREASE	A(5)A		EXPELLED
A(5)A	D	ECREASED	A(5)A		EXPENDED
A(5)A	D	EDICATE	A(5)A		EXPENSES
A(5)A	D	EFINITE	A(5)A	EXP	ERIENCE
A(5)A	D	EPARTMENT	A(5)A(2)A		EXPERIENCE
A(5)A	D	EPARTMENTAL	A(5)A		EXTENDED
A(5)A	DEP	ENDABLE	A(5)A		EXTREME
A(5)A	D	EPLOYMENT	A(5)A	FIGHT	ERPLANE
A(5)A	D	ESCRIBE	A(5)A	IN	EFFICIENCY
A(5)A	D	ESCRIBED	A(5)A	INT	ERCEPTED
A(5)A	D	ESTROYERS	A(5)A	INT	ERPRETER
A(5)A	D	ESTROYED	A(5)A	INT	ERRUPTED
A(5)A	D	ESTROYER	A(5)A	J	ETPLANE
A(5)A	D	ETACHMENT	A(5)A	M	EDICINE
A(5)A	D	ETONATE	A(5)A	M	ESSENGER
A(5)A	D	ETONATED	A(5)A	N	EWSPAPER
A(5)A	D	ETRAINED	A(5)A	N	EWSPAPERS
A(5)A	D	EVELOPED	A(5)A	ON	EHUNDRED
A(5)A	DISAPP	EARANCE	A(5)A	PAR	ENTHESES

Table D–7 ~~(C)~~. List of words containing like letters repeated at various intervals (U) —Continued

A(5)A	P	ERSISTENT	A(5)A		INCENTIVE
A(5)A	P	ERSONNEL	A(5)A		INCLINING
A(5)A	PR	EMATURE	A(5)A		INCLUDING
A(5)A	PR	ESCRIBED	A(5)A		INCLUSIVE
A(5)A	QUART	ERMASTER	A(5)A		INDEMNITY
A(5)A	REC	EPTACLE	A(5)A		INFLATION
A(5)A(1)A	RE	ENFORCEMENT	A(5)A		INSIGNIA
A(5)A	RE	ENFORCE	A(5)A		INTEGRITY
A(5)A	RE	ENLISTED	A(5)A		INTELLIGENCE
A(5)A	R	EMAINDER	A(5)A		INTELLIGENT
A(5)A	R	EQUESTED	A(5)A		INTENSIVE
A(5)A	R	ESOURCES	A(5)A		INTENTION
A(5)A	S	EABORNE	A(5)A(2)A		INTERDICTION
A(5)A	S	EAPLANES	A(5)A		INTERDICT
A(5)A	S	ENTENCE	A(5)A		INTERVIEW
A(5)A	S	EPARATE	A(5)A		INVENTION
A(5)A	S	EPTEMBER	A(5)A(3)A		INVESTIGATION
A(5)A	S	EVENTEEN	A(5)A(3)A		INVESTIGATIONS
A(5)A	S	EVENTEENTH	A(5)A		INVESTIGATE
A(5)A	SH	ELLFIRE	A(5)A	L	IMITATION
A(5)A	TEMP	ERATURE	A(5)A	MOB	ILIZATION
A(5)A	T	ERRIBLE	A(5)A	PREL	IMINARIES
A(5)A	TH	EREFORE	A(5)A	QUAL	IFICATION
A(5)A	UN	EXPENDED	A(5)A	RAD	IOSTATION
A(5)A	UNID	ENTIFIED	A(5)A	REG	ISTRATION
A(5)A	UNIT	EDSTATES	A(5)A	S	IGNALLING
A(5)A	WARD	EPARTMENT	A(5)A	S	IMILARITY
A(5)A	BE	GINNING	A(5)A	SPEC	IFICATION
A(5)A		GASSING	A(5)A	SU	ITABILITY
A(5)A		GETTING	A(5)A	VER	IFICATION
A(5)A	RE	GARDING	A(5)A	V	ISIBILITY
A(5)A	EIG	HTEENTH	A(5)A	CHRONO	LOGICAL
A(5)A	ADMIN	ISTRATIVE	A(5)A	C	LERICAL
A(5)A	ADMIN	ISTRATION	A(5)A	INF	LAMMABLE
A(5)A	ANT	ICIPATION	A(5)A		LOGICAL
A(5)A	CLASS	IFICATION	A(5)A	METEORO	LOGICAL
A(5)A	CONS	IDERATION	A(5)A	PO	LITICAL
A(5)A	DEMOB	ILIZATION	A(5)A	CO	MMENCEMENT
A(5)A	D	ISCIPLINE	A(5)A	E	MPLACEMENT
A(5)A	D	ISCONTINUE	A(5)A	I	MPROVEMENT
A(5)A	D	ISCONTINUANCE	A(5)A		MANAGEMENT
A(5)A	D	ISCUSSION	A(5)A		MARITIME
A(5)A	D	ISPERSION	A(5)A		MAXIMUM
A(5)A	IDENT	IFICATION	A(5)A		MINIMUM
A(5)A		IMPASSIBLE	A(5)A	REI	MBURSEMENT
A(5)A		IMPOSSIBLE	A(5)A	COMME	NDATION
A(5)A		INCENDIARY	A(5)A	COMPE	NSATION

Table D–7 ~~(C)~~. List of words containing like letters repeated at various intervals (U) –Continued

A(5)A	CONCE	NTRATING	A(5)A		PRINCIPAL
A(5)A	CO	NCERNING	A(5)A		PRINCIPLE
A(5)A	CO	NDITION	A(5)A	AI	RSUPPORT
A(5)A	CO	NNECTING	A(5)A	A	RBITRARY
A(5)A	CON	NECTION	A(5)A	A	RTILLERY
A(5)A	CO	NTINGENT	A(5)A	BA	ROMETER
A(5)A	CONTI	NUATION	A(5)A	B	REAKTHROUGH
A(5)A	CO	NTRABAND	A(5)A	FI	RECONTROL
A(5)A	CO	NVENIENT	A(5)A	GENE	RALALARM
A(5)A	DISCO	NTINUANCE	A(5)A	GY	ROMETER
A(5)A	E	NEMYTANKS	A(5)A	HYD	ROMETER
A(5)A	E	NLISTING	A(5)A	HYG	ROMETER
A(5)A	ENTA	NGLEMENT	A(5)A	INTE	RPRETER
A(5)A	FOU	NDATION	A(5)A	IR	REGULAR
A(5)A	I	NCLINING	A(5)A	IR	REGULARITIES
A(5)A	I	NCLUDING	A(5)A	IR	REGULARITY
A(5)A	I	NTERMENT	A(5)A	P	REMATURE
A(5)A(3)A	I	NTERVENTION	A(5)A	P	RISONER
A(5)A(1)A	I	NTERVENING	A(5)A	P	RISONERS
A(5)A	I	NTERVENE	A(5)A	P	ROCEDURE
A(5)A	I	NVASION	A(5)A	PSYCH	ROMETER
A(5)A	MA	NAGEMENT	A(5)A	QUARTE	RMASTER
A(5)A	RECOMME	NDATION	A(5)A		RADIOGRAM
A(5)A	RECON	NAISSANCE	A(5)A		RECOVER
A(5)A	REPRESE	NTATION	A(5)A		REENFORCE
A(5)A	SIG	NIFICANCE	A(5)A		REENFORCEMENT
A(5)A	SIG	NIFICANT	A(5)A		REGISTRATION
A(5)A	TRA	NSATLANTIC	A(5)A		REGULAR
A(5)A	ASS	OCIATION	A(5)A		REIMBURSEMENT
A(5)A	C	OALITION	A(5)A		REINFORCE
A(5)A	C	OLLISION	A(5)A		REINFORCEMENT
A(5)A	C	OLLISIONS	A(5)A	ST	RAGGLER
A(5)A	C	ONDITION	A(5)A	SU	RRENDER
A(5)A	CONF	ORMATION	A(5)A	SU	RRENDERED
A(5)A	C	ONTINUOUS	A(5)AA	T	RANSFERRED
A(5)A	C	ORRESPONDENCE	A(5)AA	T	RANSFERRING
A(5)A	C	ORRESPONDING	A(5)A	T	RANSFER
A(5)A	F	ORMATION	A(5)A	T	RANSPORT
A(5)A	INF	ORMATION	A(5)A	T	RANSPORTATION
A(5)A	INTR	ODUCTION	A(5)A	T	RANSPORTS
A(5)A		OPERATOR	A(5)A	T	RANSVERSE
A(5)A	PR	OPORTION	A(5)A	ASSE	SSMENTS
A(5)A	PR	OTECTION	A(5)A	A	SSOONAS
A(5)A	RADI	OSTATION	A(5)A	CIRCUM	STANCES
A(5)A	REC	OGNITION	A(5)A	CRO	SSROADS
A(5)A	TRANSP	ORTATION	A(5)A	DI	STRICTS
A(5)A		PHILIPPINES	A(5)A	E	STABLISH

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) –Continued

A(5)A	E	STABLISHED	A(5)A	S	UBSTITUTE
A(5)A	E	STABLISHMENT	A(5)A	S	UBSTITUTION
A(5)A	NEW	SPAPERS	A(6)A		ANTICIPATE
A(5)A	PHO	SPHORUS	A(6)A		ANTICIPATION
A(5)A	PO	SITIONS	A(6)A	CL	ASSIFICATION
A(5)A	RE	SOURCES	A(6)A	DEP	ARTMENTAL
A(5)A		SAILORS	A(6)A	TR	ADITIONAL
A(5)A		SECTORS	A(6)A	TR	ANSPORTATION
A(5)A		SERIOUSLY	A(6)A	A	CCEPTANCE
A(5)A		SKIRMISH	A(6)A	A	CCORDANCE
A(5)A		SUBMISSION	A(6)A		CERTIFICATE
A(5)A		SUCCESSIVE	A(6)A	CIR	CUMSTANCES
A(5)A		SUCCESS	A(6)A		CLEARANCE
A(5)A		SUCCESSFUL	A(6)A		COMMUNICATE
A(5)A		SUCCESSFULLY	A(6)A		COMMUNICATION
A(5)A		SURPLUS	A(6)A		CONSTRUCTION
A(5)A		SURPRISE	A(6)A	RE	CONSTRUCTION
A(5)A		SUSPENSE	A(6)A	A	DDRESSED
A(5)A		SUSPENSION	A(6)A		DECLARED
A(5)A	UN	SUCCESSFUL	A(6)A		DEFEATED
A(5)A	AN	TICIPATE	A(6)A		DEFENDED
A(5)A	AN	TICIPATION	A(6)A		DEFERRED
A(5)A	CER	TIFICATE	A(6)A		DEMANDED
A(5)A	CON	TINGENT	A(6)A		DEPARTED
A(5)A	IDEN	TIFICATION	A(6)A		DEPLOYED
A(5)A	INS	TRUMENT	A(6)A		DEPORTED
A(5)A	INS	TRUMENTS	A(6)A		DESERTED
A(5)A	IN	TERCEPT	A(6)A		DETACHED
A(5)A	IN	TERCEPTED	A(6)A		DICTATED
A(5)A	IN	TERDICT	A(6)A		DISARMED
A(5)A	IN	TERDICTION	A(6)A	UN	DERSTAND
A(5)A	IN	TERMENT	A(6)A	UN	DERSTOOD
A(5)A(1)A	IN	TERPRETATION	A(6)A	A	ERODROME
A(5)A	IN	TERPRETER	A(6)A	A	EROPLANE
A(5)A	IN	TERRUPT	A(6)A	B	EENNEEDED
A(5)A	IN	TERRUPTED	A(6)A	B	ELLIGERENT
A(5)A	IN	TERRUPTION	A(6)A	D	ECIPHERED
A(5)A	IN	TERVENTION	A(6)A	D	EFECTIVE
A(5)A	IN	TRODUCTION	A(6)A	D	EFENSIVE
A(5)A	IN	TRODUCTORY	A(6)A	D	EPARTURE
A(5)A	QUAR	TERMASTER	A(6)A	D	ESIGNATE
A(5)A	SA	TISFACTORY	A(6)A	D	ESIGNATED
A(5)A	SUI	TABILITY	A(6)A	D	ESPATCHES
A(5)A		TONIGHT	A(6)A	D	ESPATCHED
A(5)A		TRAJECTORY	A(6)A	D	ESTITUTE
A(5)A(3)A		TRANSATLANTIC	A(6)A	DET	ERIORATE
A(5)A	UNI	TEDSTATES	A(6)A	D	ETERMINE

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) —Continued

A(6)A	D	ETERMINED	A(6)A	R	EENFORCE
A(6)A	D	EVELOPMENT	A(6)A(1)A	R	EENFORCEMENT
A(6)A		ECHELONED	A(6)A	R	EENLISTED
A(6)A		ELIGIBLE	A(6)A	RE	ENLISTMENT
A(6)A		EMBASSIES	A(6)A	R	EFERENCE
A(6)A		EMPLOYEE	A(6)A(1)A	R	EIMBURSEMENT
A(6)A		EMPLOYMENT	A(6)A(1)A	R	EINFORCEMENT
A(6)A		ENCIRCLE	A(6)A	R	EINFORCE
A(6)A(1)A		ENCOUNTERED	A(6)A(1)A	R	EINSTATEMENT
A(6)A	EN	EMYPLANES	A(6)A	R	EINSTATE
A(6)A		ENFILADE	A(6)A	R	EPLACEMENT
A(6)A		ENGAGEMENT	A(6)A	REPRES	ENTATIVE
A(6)A		ENLISTMENT	A(6)A	R	EQUIREMENT
A(6)A		ENROLLMENT	A(6)A	R	ESTRICTED
A(6)A(1)A		ENTANGLEMENT	A(6)A	SEV	ENTYFIVE
A(6)A	ENT	ERTAINMENT	A(6)A	T	ECHNIQUE
A(6)A		ENTRAINED	A(6)A	T	ELEPHONE
A(6)A		ENVELOPE	A(6)A	T	ENTATIVE
A(6)A		EQUALIZE	A(6)A	TH	ERMOMETER
A(6)A		EQUIPAGE	A(6)A	TW	ENTYFIVE
A(6)A		EQUIVALENT	A(6)A	DISTIN	GUISHING
A(6)A		ESTIMATE	A(6)A		GROUPING
A(6)A		ESTIMATEDAT	A(6)A		GUARDING
A(6)A		ESTIMATES	A(6)A	SI	GNALLING
A(6)A		EVACUATE	A(6)A	C	IRCULATION
A(6)A		EXCAVATE	A(6)A	D	IPLOMATIC
A(6)A		EXCHANGE	A(6)A	D	ISORGANIZED
A(6)A		EXCITEMENT	A(6)A	D	ISPOSITION
A(6)A		EXERCISE	A(6)A	D	ISTINCTION
A(6)A		EXERCISES	A(6)A	D	ISTINGUISH
A(6)A		EXHIBITED	A(6)A	D	ISTINGUISHED
A(6)A		EXPEDITE	A(6)A(2)A	D	ISTINGUISHING
A(6)A		EXPERIMENT	A(6)A	DIST	INGUISHING
A(6)A	EXT	ERMINATE	A(6)A	F	INGERPRINT
A(6)A	INDET	ERMINATE	A(6)A(3)A		IDENTIFICATION
A(6)A	INV	ESTIGATE	A(6)A		IMPRACTICABLE
A(6)A	M	EASUREMENT	A(6)A		IMPRESSION
A(6)A	M	EASUREMENTS	A(6)A		IMPRESSIVE
A(6)A	M	ECHANIZED	A(6)A		INDICATING
A(6)A	NEC	ESSITATE	A(6)A		INDICATION
A(6)A	OV	ERWHELMED	A(6)A		INEFFICIENCY
A(6)A	P	ENETRATE	A(6)A		INFLICTING
A(6)A	PR	EARRANGED	A(6)A		INSECURITY
A(6)A	PR	ECEDENCE	A(6)A		INSPECTION
A(6)A	PR	EFERENCE	A(6)A		INVITATION
A(6)A	PR	EPAREDNESS	A(6)A		IRRIGATION
A(6)A	R	ECOGNIZE	A(6)A	UN	IDENTIFIED

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) –Continued

A(6)A	W	ITHDRAWING	A(6)A	C	ONCESSION
A(6)A		MEASUREMENT	A(6)A	C	ONCLUSION
A(6)A		MEASUREMENTS	A(6)A	C	ONFESSION
A(6)A	ME	MORANDUM	A(6)A	C	ONNECTION
A(6)A	A	NTEDATING	A(6)A	CO	OPERATION
A(6)A	COMMU	NICATION	A(6)A	C	ORRECTION
A(6)A	CO	NCEALMENT	A(6)A	D	OMINATION
A(6)A	CONCE	NTRATION	A(6)A	F	OUNDATION
A(6)A	CO	NCESSION	A(6)A		OBJECTION
A(6)A	CO	NCLUSION	A(6)A		OPERATION
A(6)A	CO	NFESSION	A(6)A	P	OPULATION
A(6)A	CO	NFINEMENT	A(6)A	P	OSSESSION
A(6)A	CO	NNECTION	A(6)A		PARAGRAPH
A(6)A	DISTI	NGUISHING	A(6)A	AG	RICULTURAL
A(6)A	E	NCIRCLING	A(6)A	B	RIGADIER
A(6)A	E	NEMYPLANES	A(6)A	INT	RODUCTORY
A(6)A	E	NLISTMENT	A(6)A	I	RREGULAR
A(6)A	E	NROLLMENT	A(6)A	I	RREGULARITIES
A(6)A(2)A	E	NTERTAINMENT	A(6)A	I	RREGULARITY
A(6)A	E	NTRUCKING	A(6)A	P	ROJECTOR
A(6)A	FI	NGERPRINT	A(6)A	P	ROTECTOR
A(6)A	I	NDICATING	A(6)A		REARGUARD
A(6)A	I	NFLATION	A(6)A		RECEIVER
A(6)A	I	NFLICTING	A(6)A		RECONSTRUCTION
A(6)A	I	NSTANTANEOUS	A(6)A		RECORDER
A(6)A	I	NSTRUMENT	A(6)A		REGISTER
A(6)A	I	NSTRUMENTS	A(6)A		REJECTOR
A(6)A	I	NTENTION	A(6)A		REMEMBER
A(6)A	I	NTERNMENT	A(6)A		REPEATER
A(6)A	I	NVENTION	A(6)A		REVOLVER
A(6)A		NEGLIGENT	A(6)A	THE	RMOMETER
A(6)A		NEGLIGENCE	A(6)A	T	RAJECTORY
A(6)A		NINETEEN	A(6)A	T	RANSFERRED
A(6)A		NINETEENTH	A(6)A	T	RANSFERRING
A(6)A		NORTHERN	A(6)A	AS	SEMBLIES
A(6)A		NUMBERING	A(6)A	CA	SUALTIES
A(6)A	ORGA	NIZATION	A(6)A	CU	STOMHOUSE
A(6)A	RECO	NNAISSANCE	A(6)A	DE	SPATCHES
A(6)A	RECON	NOITERING	A(6)A	DE	STROYERS
A(6)A	REE	NLISTMENT	A(6)A	DI	SPATCHES
A(6)A	REORGA	NIZATION	A(6)A	DI	STINGUISH
A(6)A	SA	NITATION	A(6)A	DI	STINGUISHED
A(6)A	TRA	NSFERRING	A(6)A	DI	STINGUISHING
A(6)A	U	NDERSTAND	A(6)A	E	STIMATES
A(6)A	C	OLLECTION	A(6)A		SOLDIERS
A(6)A	C	OMMISSION	A(6)A		SOUTHEAST
A(6)A	C	OMMISSIONER	A(6)A		SOUTHWEST

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) —Continued

A(6)A		SOUTHWESTERN	A(7)A		DECREASED
A(6)A		STATIONS	A(7)A		DESCRIBED
A(6)A		SUPPLIES	A(7)A		DESTROYED
A(6)A	SU	SPICIONS	A(7)A		DETONATED
A(6)A	SU	SPICIOUS	A(7)A		DETRAINED
A(6)A	AT	TACHMENT	A(7)A		DEVELOPED
A(6)A.	AT	TAINMENT	A(7)A		DISCUSSED
A(6)A	CEN	TRALIZATION	A(7)A		DISPERSED
A(6)A	DE	TACHMENT	A(7)A		DOMINATED
A(6)A	DE	TERIORATE	A(7)A	UNI	DENTIFIED
A(6)A	DE	TERMINATION	A(7)A	C	ENTRALIZE
A(6)A	ENTER	TAINMENT	A(7)A	DEC	ENTRALIZE
A(6)A	EX	TERMINATE	A(7)A	DEC	ENTRALIZED
A(6)A	EX	TERMINATION	A(7)A	D	ENCIPHERMENT
A(6)A	INDE	TERMINATE	A(7)A	D	EMOBILIZE
A(6)A	IN	TERNMENT	A(7)A	D	EPENDABLE
A(6)A	NA	TIONALITY	A(7)A		ECHELONMENT
A(6)A	REINS	TATEMENT	A(7)A		EFFECTIVE
A(6)A	S	TATEMENT	A(7)A		ELABORATE
A(6)A		TEMPERATURE	A(7)A		EMPLACEMENT
A(6)A		TWENTIETH	A(7)A		ENCIPHERED
A(6)A	C	USTOMHOUSE	A(7)A		ENDURANCE
A(6)A	SIM	ULTANEOUS	A(7)A		ENFORCEMENT
A(6)A	S	UCCESSFUL	A(7)A		ENTRENCHED
A(6)A	S	UCCESSFULLY	A(7)A		EXCESSIVE
A(6)A	S	USPICIOUS	A(7)A		EXCLUSIVE
A(6)A	UNS	UCCESSFUL	A(7)A		EXECUTIVE
A(6)A	SE	VENTYFIVE	A(7)A		EXPANSIVE
A(6)A		WITHDRAW	A(7)A		EXPENSIVE
A(6)A		WITHDRAWAL	A(7)A		EXPLOSIVE
A(6)A		WITHDRAWING	A(7)A		EXTENSIVE
A(6)A		WITHDREW	A(7)A	H	EADQUARTERS
A(7)A		ACCIDENTAL	A(7)A	H	EAVYBOMBER
A(7)A		ACCOMMODATION	A(7)A	H	EAVYLOSSES
A(7)A		ADDITIONAL	A(7)A	INT	ELLIGENCE
A(7)A		APPROPRIATE	A(7)A	INT	ERMEDIATE
A(7)A		APPROXIMATE	A(7)A	N	EGLIGENCE
A(7)A		ARMOREDCAR	A(7)A	R	EAPPOINTED
A(7)A		ARTIFICIAL	A(7)A	R	ECEPTACLE
A(7)A	N	ATURALIZATION	A(7)A	R	ECOMMENDED
A(7)A	CHARA	CTERISTIC	A(7)A	R	ECONNOITER
A(7)A		CLASSIFICATION	A(7)A	R	ECONNOITERING
A(7)A		CONFERENCE	A(7)A	RE	ENFORCEMENT
A(7)A		CONFIDENCE	A(7)A	R	EENLISTMENT
A(7)A		CONSPIRACY	A(7)A	R	ESISTANCE
A(7)A		CONVALESCENT	A(7)A	EN	GINEERING
A(7)A	IN	COMPETENCE	A(7)A	P	HOTOGRAPHY

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) —Continued

A(7)A	T	HIRTEENTH
A(7)A	ADM	INISTRATIVE
A(7)A	ADM	INISTRATION
A(7)A	D	IFFICULTIES
A(7)A	D	ISTRIBUTING
A(7)A	D	ISTRIBUTION
A(7)A		IMMIGRATION
A(7)A		INDETERMINATE
A(7)A		INFORMATION
A(7)A		INSPIRATION
A(7)A		INSTITUTION
A(7)A		INSTRUCTION
A(7)A		INSTRUCTIONS
A(7)A		INTERESTING
A(7)A		INTERFERING
A(7)A		INTERMEDIATE
A(7)A		INTERNATIONAL
A(7)A		INTERVENING
A(7)A		MECHANISM
A(7)A		MEDIUMBOMBER
A(7)A	AN	NOUNCEMENT
A(7)A	CO	NGRESSIONAL
A(7)A	CO	NSTITUTING
A(7)A	CO	NSUMPTION
A(7)A	CO	NVALESCENT
A(7)A	DEMO	NSTRATION
A(7)A	E	NFORCEMENT
A(7)A	E	NGINEERING
A(7)A	I	NCOMPETENT
A(7)A	I	NCOMPETENCE
A(7)A	I	NDEPENDENT
A(7)A	I	NDETERMINATE
A(7)A	I	NDICATION
A(7)A	I	NEFFICIENCY
A(7)A	I	NSPECTION
A(7)A	I	NTELLIGENCE
A(7)A	I	NTELLIGENT
A(7)A	I	NTERESTING
A(7)A	I	NTERFERENCE
A(7)A	I	NTERFERING
A(7)A	I	NTERVENING
A(7)A	I	NVITATION
A(7)A	NO	NCOMBATANT
A(7)A	PE	NETRATION
A(7)A	RECO	NNOITERING
A(7)A	REE	NFORCEMENT
A(7)A	REI	NFORCEMENT
A(7)A	REI	NSTATEMENT
A(7)A	TRA	NSMISSION
A(7)A	ACC	OMMODATION
A(7)A	C	OMPETITION
A(7)A	C	OMPOSITION
A(7)A	C	OMPUTATION
A(7)A	C	ONGRESSIONAL
A(7)A	C	ONSUMPTION
A(7)A	C	OOPERATION
A(7)A	CO	ORDINATION
A(7)A	C	ORPORATION
A(7)A	DEM	ONSTRATION
A(7)A		OCCUPATION
A(7)A		OPPOSITION
A(7)A	PR	OCLAMATION
A(7)A		PHOTOGRAPHY
A(7)A	A	RMOREDCAR
A(7)A	EXT	RAORDINARY
A(7)A	NO	RTHWESTERN
A(7)A	P	RELIMINARIES
A(7)A	P	RELIMINARY
A(7)A		REMAINDER
A(7)A	SHA	RPSHOOTER
A(7)A	A	SSEMBLIES
A(7)A	AS	SESSMENTS
A(7)A	AS	SIGNMENTS
A(7)A	HO	STILITIES
A(7)A	IN	STRUMENTS
A(7)A	MEA	SUREMENTS
A(7)A		SEAPLANES
A(7)A		STANDARDS
A(7)A	A	TTACHMENT
A(7)A	A	TTAINMENT
A(7)A	ES	TIMATEDAT
A(7)A	IN	TELLIGENT
A(7)A	IN	TERMEDIATE
A(7)A	IN	TERPRETATION
A(7)A	NA	TURALIZATION
A(7)A		THERMOMETER
A(7)A		THIRTEENTH
A(7)A(1)A		TRANSPORTATION
A(7)A		TRANSPORT
A(7)A		TRANSPORTS
A(7)A		YESTERDAY
A(8)A		ADMINISTRATIVE
A(8)A		ADMINISTRATION
A(8)A		ANTIAIRCRAFT

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) —Continued

A(8)A		COINCIDENCE
A(8)A	DIS	CONTINUANCE
A(8)A		DECIPHERED
A(8)A		DESIGNATED
A(8)A		DESPATCHED
A(8)A		DETERMINED
A(8)A		DISPATCHED
A(8)A		DISTRESSED
A(8)A	C	ERTIFICATE
A(8)A	CORR	ESPONDENCE
A(8)A	D	EMONSTRATE
A(8)A	D	EMONSTRATED
A(8)A	D	ESCRIPTIVE
A(8)A	D	ETERIORATE
A(8)A		ENCIPHERMENT
A(8)A		ENCOUNTERED
A(8)A		ENEMYPLANES
A(8)A		ENTANGLEMENT
A(8)A		ENTERPRISE
A(8)A		ESTABLISHED
A(8)A	IND	ETERMINATE
A(8)A	IRR	EGULARITIES
A(8)A	M	EDIUMBOMBER
A(8)A	N	ECESSITATE
A(8)A	P	ERFORMANCE
A(8)A	PR	ELIMINARIES
A(8)A	R	EAPPOINTMENT
A(8)A	R	EENFORCEMENT
A(8)A	R	EIMBURSEMENT
A(8)A	R	EINFORCEMENT
A(8)A	R	EINSTATEMENT
A(8)A	REPR	ESENTATIVE
A(8)A	R	ESPONSIBLE
A(8)A	R	ETROACTIVE
A(8)A	S	EVENTYFIVE
A(8)A	T	EMPERATURE
A(8)A		HYDROGRAPHIC
A(8)A	D	ISCREPANCIES
A(8)A		ILLUSTRATION
A(8)A		INAUGURATION
A(8)A		INSTALLATIONS
A(8)A		INTERDICTION
A(8)A		INTERRUPTION
A(8)A		INTERVENTION
A(8)A		INTRODUCTION
A(8)A(1)A		IRREGULARITIES
A(8)A		IRREGULARITY
A(8)A		MEMORANDUM
A(8)A	ADMI	NISTRATION
A(8)A	A	NNOUNCEMENT
A(8)A	CA	NCELLATION
A(8)A	CO	NCENTRATING
A(8)A	CO	NCILLIATION
A(8)A	CO	NFIRMATION
A(8)A	CO	NFISCATION
A(8)A	CO	NFORMATION
A(8)A	CO	NSCRIPTION
A(8)A	CO	NSTITUTION
A(8)A	CO	NSTRUCTION
A(8)A	CO	NTINUATION
A(8)A	CO	NVERSATION
A(8)A	E	NCIPHERMENT
A(8)A	E	NTANGLEMENT
A(8)A	E	NTERPRISING
A(8)A	I	NFORMATION
A(8)A	I	NSPIRATION
A(8)A	I	NSTITUTION
A(8)A	I	NSTRUCTION
A(8)A	I	NSTRUCTIONS
A(8)A	I	NTERNATIONAL
A(8)A		NAVIGATION
A(8)A	RECO	NSTRUCTION
A(8)A	C	OMMENDATION
A(8)A	C	OMPENSATION
A(8)A	C	ONCILIATION
A(8)A	C	ONFIRMATION
A(8)A	C	ONFISCATION
A(8)A	C	ONFORMATION
A(8)A	C	ONSCRIPTION
A(8)A	C	ONSTITUTION
A(8)A	C	ONSTRUCTION
A(8)A	C	ONTINUATION
A(8)A	C	ONVERSATION
A(8)A	DEM	OBILIZATION
A(8)A	M	OBILIZATION
A(8)A		OBSERVATION
A(8)A		OBSTRUCTIONS
A(8)A	REC	OMMENDATION
A(8)A	REC	ONSTRUCTION
A(8)A	R	OADJUNCTION
A(8)A	QUA	RTERMASTER
A(8)A	A	SSESSMENTS
A(8)A	A	SSIGNMENTS
A(8)A	IN	STRUCTIONS

Table D–7 (~~C~~). List of words containing like letters repeated at various intervals (U) –Continued

A(8)A	INVE	STIGATIONS
A(8)A	OB	STRUCTIONS
A(8)A	REPRE	SENTATIONS
A(8)A		SCHOOLHOUSE
A(8)A		SUBMARINES
A(8)A		SUSPICIONS
A(8)A		SUSPICIOUS
A(8)A	AN	TIAIRCRAFT
A(8)A	EN	TANGLEMENT
A(9)A		AGRICULTURAL
A(9)A		CHRONOLOGICAL
A(9)A		CIRCUMSTANCES
A(9)A	RE	CONNAISSANCE
A(9)A		DISAPPEARED
A(9)A		DISINFECTED
A(9)A	D	ECENTRALIZE
A(9)A	D	ECENTRALIZED
A(9)A		ENTERTAINMENT
A(9)A		ESTABLISHMENT
A(9)A		EXTERMINATE
A(9)A	C	IRCUMSTANTIAL
A(9)A		INVESTIGATION
A(9)A		INVESTIGATIONS
A(9)A	A	NTICIPATION
A(9)A	CO	NCENTRATION
A(9)A	CO	NSIDERATION
A(9)A	E	NTERTAINMENT
A(9)A	IDE	NTIFICATION
A(9)A	I	NAUGURATION
A(9)A	I	NSTALLATIONS
A(9)A	I	NTERDICTION
A(9)A	I	NTERRUPTION
A(9)A	I	NTERVENTION
A(9)A	I	NTRODUCTION
A(9)A		NONCOMBATANT
A(9)A	TRA	NSPORTATION
A(9)A	C	OMMUNICATION
A(9)A	C	ONCENTRATION
A(9)A	C	ONSIDERATION
A(9)A		ORGANIZATION
A(9)A	RE	ORGANIZATION
A(9)A		RANGEFINDER
A(9)A		RECONNOITER
A(9)A		RECONNOITERING
A(9)A	DI	SCREPANCIES
A(9)A	IN	STALLATIONS
A(9)A	IN	STANTANEOUS
A(9)A	MI	SCELLANEOUS
A(9)A	EN	TERTAINMENT
A(9)A	ES	TABLISHMENT
A(9)A		TRANSATLANTIC
A(9)A		TRANSPORTATION
A(9)A		UNSUCCESSFUL
A(10)A		COUNTERATTACK
A(10)A		DEMONSTRATED
A(10)A		DISORGANIZED
A(10)A		DISSEMINATED
A(10)A		INTERPRETATION
A(10)A		IRREGULARITIES
A(10)A	CE	NTRALIZATION
A(10)A	I	NVESTIGATION
A(10)A	I	NVESTIGATIONS
A(10)A		NORTHWESTERN
A(10)A		REVOLUTIONARY
A(10)A		SEARCHLIGHTS
A(10)A		SIMULTANEOUS
A(11)A		CORRESPONDENCE
A(11)A		DECENTRALIZED
A(11)A		DISTINGUISHED
A(11)A	R	ECONNAISSANCE
A(11)A	I	NTERPRETATION
A(12)A		NATURALIZATION

APPENDIX E (~~C~~)
USEFUL TABLES

Table E–1 (~~C~~). Expected number of repetitions, polyalphabetic ciphers (U)

Number of letters	Expected number of diagraphs occurring exactly x times								
	E(2)	E(3)	E(4)	E(5)	E(6)	E(7)	E(8)	E(9)	E(10)
100	6.21	0.298	0.011						
200	21.8	2.12	0.154	0.009					
300	42.5	6.23	0.683	0.060	0.004				
400	65.3	12.8	1.87	0.220	0.022	0.002			
500	88.1	21.6	3.97	0.582	0.071	0.008			
600	110	32.3	7.11	1.25	0.184	0.023	0.003		
700	129	44.3	11.4	2.35	0.403	0.059	0.008	0.001	
800	145	57.1	16.8	3.96	0.777	0.130	0.019	0.003	
900	158	70.1	23.2	6.16	1.36	0.257	0.043	0.006	0.001
1000	169	83.0	30.6	9.03	2.21	0.466	0.085	0.014	0.002

Number of letters	Expected number of trigraphs		
	E(2)	E(3)	E(4)
100	0.269	0.001	
200	1.10	0.004	
300	2.48	0.014	
400	4.40	0.033	
500	6.85	0.064	
600	9.81	0.111	0.001
700	13.3	0.175	0.002
800	17.3	0.261	0.003
900	21.8	0.371	0.005
1000	26.8	0.505	0.008

Number of letters	Tetragraphs	
	E(2)	E(3)
100	0.010	
200	0.043	
300	0.096	
400	0.171	
500	0.270	
600	0.389	
700	0.530	
800	0.693	
900	0.877	
1000	1.08	0.001

Number of letters	Penta–graphs
	E(2)
100	
200	0.002
300	0.004
400	0.007
500	0.011
600	0.015
700	0.021
800	0.027
900	0.034
1000	0.042

Table E–2 (~~C~~). Expected values of $\emptyset_r$ and $\emptyset_p$ (U).

N	$\emptyset_r$	$\emptyset_p$	N	$\emptyset_r$	$\emptyset_p$	N	$\emptyset_r$	$\emptyset_p$	N	$\emptyset_r$	$\emptyset_p$	N	$\emptyset_r$	$\emptyset_p$
11	4.23	7.34	29	31	54	47	83	144	65	160	277	83	262	454
12	5.08	8.80	30	33	58	48	87	150	66	165	286	84	268	465
13	6.00	10.4	31	36	62	49	90	157	67	170	295	85	275	476
14	7.00	12.1	32	38	66	50	94	163	68	175	304	86	281	488
15	8.08	14.0	33	41	70	51	98	170	69	180	313	87	288	499
16	9.23	16.0	34	43	75	52	102	177	70	186	322	88	294	511
17	10.5	18.1	35	46	79	53	106	184	71	191	331	89	301	522
18	11.8	20.4	36	48	84	54	110	191	72	197	341	90	308	534
19	13.2	22.8	37	51	89	55	114	198	73	202	351	91	315	546
20	14.6	25.3	38	54	94	56	118	205	74	208	360	92	322	558
21	16.2	28.5	39	57	99	57	123	213	75	213	370	93	329	571
22	17.8	30.8	40	60	104	58	127	221	76	219	380	94	336	583
23	19.5	33.8	41	63	109	59	132	228	77	225	390	95	343	596
24	21.2	36.8	42	66	115	60	136	236	78	231	401	96	351	608
25	23.1	40.0	43	69	120	61	141	244	79	237	411	97	358	621
26	25.0	43.4	44	73	126	62	145	252	80	243	422	98	366	634
27	27.0	46.8	45	76	132	63	150	261	81	249	432	99	373	647
28	29.1	50.4	46	80	138	64	155	269	82	255	443	100	381	660

Table E–3 (U).Factor table (U)

NUMBERS 1–400

1	Prime	36	2 3 4 6 9 12 18	70	2 5 7 10 14 35
2	Prime	37	Prime	71	Prime
3	Prime	38	2 19	72	2 3 4 6 8 9 12 18 24 36
4	2	39	3 13	73	Prime
5	Prime	40	2 4 5 8 10 20	74	2 37
6	2 3	41	Prime	75	3 5 15 25
7	Prime	42	2 3 6 7 14 21	76	2 4 19 38
8	2 4	43	Prime	77	7 11
9	3	44	2 4 11 22	78	2 3 6 13 26 39
10	2 5	45	3 5 9 15	79	Prime
11	Prime	46	2 23	80	2 4 5 8 10 16 20 40
12	2 3 4 6	47	Prime	81	3 9 27
13	Prime	48	2 3 4 6 8 12 16 24	82	2 41
14	2 7	49	7	83	Prime
15	3 5	50	2 5 10 25	84	2 3 4 6 7 12 14 21 28 42
16	2 4 8	51	3 17	85	5 17
17	Prime	52	2 4 13 26	86	2 43
18	2 3 6 9	53	Prime	87	3 29
19	Prime	54	2 3 6 9 18 27	88	2 4 8 11 22 44
20	2 4 5 10	55	5 11	89	Prime
21	3 7	56	2 4 7 8 14 28	90	2 3 5 6 9 10 15 18 30 45
22	2 11	57	3 19	91	7 13
23	Prime	58	2 29	92	2 4 23 46
24	2 3 4 6 8 12	59	Prime	93	3 31
25	5	60	2 3 4 5 6 10 12 15	94	2 47
26	2 13		20 30	95	5 19
27	3 9	61	Prime	96	2 3 4 6 8 12 16 24 32 48
28	2 4 7 14	62	2 31	97	Prime
29	Prime	63	3 7 9 21	98	2 7 14 49
30	2 3 5 6 10 15	64	2 4 8 16 32	99	3 9 11 33
31	Prime	65	5 13	100	2 4 5 10 20 25 50
32	2 4 8 16	66	2 3 6 11 33	101	Prime
33	3 11	67	Prime	102	2 3 6 17 34 51
34	2 17	68	2 4 17 34	103	Prime
35	5 7	69	3 23	104	2 4 8 13 26 52

Table E-3 (U). Factor Table (U)--Continued

NUMBERS 1–400 -- Continued

105	3 5 7 15 21 35
106	2 53
107	Prime
108	2 3 4 6 9 12 18 27 36 54
109	Prime
110	2 5 10 11 22 55
111	3 37
112	2 4 7 8 14 16 28 56
113	Prime
114	2 3 6 19 38 57
115	5 23
116	2 4 29 58
117	3 9 13 39
118	2 59
119	7 17
120	2 3 4 5 6 8 10 12 15 20 24 30 40 60
121	11
122	2 61
123	3 41
124	2 4 31 62
125	5 25
126	2 3 6 7 9 14 18 21 42 63
127	Prime
128	2 4 8 16 32 64
129	3 43
130	2 5 10 13 26 65
131	Prime
132	2 3 4 6 11 12 22 33 44 66
133	7 19
134	2 67
135	3 5 9 15 27 45
136	2 4 8 17 34 68
137	Prime
138	2 3 6 23 46 69
139	Prime
140	2 4 5 7 10 14 20 28 35 70
141	3 47
142	2 71
143	11 13
144	2 3 4 6 8 9 12 16 18 24 36 48 72
145	5 29
146	2 73
147	3 7 21 49
148	2 4 37 74
149	Prime
150	2 3 5 6 10 15 25 30 50 75
151	Prime
152	2 4 8 19 38 76
153	3 9 17 51
154	2 7 11 14 22 77
155	5 31
156	2 3 4 6 12 13 26 39 52 78
157	Prime
158	2 79
159	3 53
160	2 4 5 8 10 16 20 32 40 80
161	7 23
162	2 3 6 9 18 27 54 81
163	Prime
164	2 4 41 82
165	3 5 11 15 33 55
166	2 83
167	Prime
168	2 3 4 6 7 8 12 14 21 24 28 42 56 84
169	13
170	2 5 10 17 34 85
171	3 9 19 57
172	2 4 43 86
173	Prime
174	2 3 6 29 58 87
175	5 7 25 35
176	2 4 8 11 16 22 44 88
177	3 59
178	2 89
179	Prime
180	2 3 4 5 6 9 10 12 15 18 20 30 36 45 60 90
181	Prime
182	2 7 13 14 26 91
183	3 61
184	2 4 8 23 46 92
185	5 37
186	2 3 6 31 62 93
187	11 17
188	2 4 47 94
189	3 7 9 21 27 63
190	2 5 10 19 38 95
191	Prime
192	2 3 4 6 8 12 16 24 32 48 64 96
193	Prime
194	2 97
195	3 5 13 15 39 65
196	2 4 7 14 28 49 98
197	Prime
198	2 3 6 9 11 18 22 33 66 99
199	Prime
200	2 4 5 8 10 20 25 40 50 100
201	3 67
202	2 101
203	7 29
204	2 3 4 6 12 17 34 51 68 102
205	5 41
206	2 103
207	3 9 23 69
208	2 4 8 13 16 26 52 104
209	11 19
210	2 3 5 6 7 10 14 15 21 30 35 42 70 105
211	Prime
212	2 4 53 106

Table E-3 (U). Factor Table (U)--Continued

NUMBERS 1–400 --Continued

213	3 71
214	2 107
215	5 43
216	2 3 4 6 8 9 12 18 24 27 36 54 72 108
217	7 31
218	2 109
219	3 73
220	2 4 5 10 11 20 22 44 55 110
221	13 17
222	2 3 6 37 74 111
223	Prime
224	2 4 7 8 14 16 28 32 56 112
225	3 5 9 15 25 45 75
226	2 113
227	Prime
228	2 3 4 6 12 19 38 57 76 114
229	Prime
230	2 5 10 23 46 115
231	3 7 11 21 33 77
232	2 4 8 29 58 116
233	Prime
234	2 3 6 9 13 18 26 39 78 117
235	5 47
236	2 4 59 118
237	3 79
238	2 7 14 17 34 119
239	Prime
240	2 3 4 5 6 8 10 12 15 16 20 24 30 40 48 60 80 120
241	Prime
242	2 11 22 121
243	3 9 27 81
244	2 4 61 122
245	5 7 35 49
246	2 3 6 41 82 123
247	13 19
248	2 4 8 31 62 124
249	3 83
250	2 5 10 25 50 125
251	Prime
252	2 3 4 6 7 9 12 14 18 21 28 36 42 63 84 126
253	11 23
254	2 127
255	3 5 15 17 51 85
256	2 4 8 16 32 64 128
257	Prime
258	2 3 6 43 86 129
259	7 37
260	2 4 5 10 13 20 26 52 65 130
261	3 9 29 87
262	2 131
263	Prime
264	2 3 4 6 8 11 12 22 24 33 44 66 88 132
265	5 53
266	2 7 14 19 38 133
267	3 89
268	2 4 67 134
269	Prime
270	2 3 5 6 9 10 15 18 27 30 45 54 90 135
271	Prime
272	2 4 8 16 17 34 68 136
273	3 7 13 21 39 91
274	2 137
275	5 11 25 55
276	2 3 4 6 12 23 46 69 92 138
277	Prime
278	2 139
279	3 9 31 93
280	2 4 5 7 8 10 14 20 28 35 40 56 70 140
281	Prime
282	2 3 47 94 141
283	Prime
284	2 4 71 142
285	3 5 15 19 57 95
286	2 11 13 22 26 143
287	7 41
288	2 3 4 6 8 9 12 16 18 24 32 36 48 72 96 144
289	17
290	2 5 10 29 58 145
291	3 97
292	2 4 73 146
293	Prime
294	2 3 6 7 14 21 42 49 98 147
295	5 59
296	2 4 8 37 74 148
297	3 9 11 27 33 99
298	2 149
299	13 23
300	2 3 4 5 6 10 12 15 20 25 30 50 60 75 100 150
301	7 43
302	2 151
303	3 101
304	2 4 8 16 19 38 76 152
305	5 61
306	2 3 6 9 17 18 34 51 102 153
307	Prime
308	2 4 7 11 14 22 28 44 77 154
309	3 103
310	2 5 10 31 62 155
311	Prime

Table E-3 (U). Factor Table (U)--Continued

NUMBERS 1–400 --Continued

312	2 3 4 6 8 12 13 24 26 39 52 78 104
313	Prime
314	2 157
315	3 5 7 9 15 21 35 45 63 105
316	2 4 79 158
317	Prime
318	2 3 6 53 106 169
319	11 29
320	2 4 5 8 10 16 20 32 40 64 80 160
321	3 107
322	2 7 14 23 46 161
323	17 19
324	2 3 4 6 9 12 18 27 36 54 81 108 162
325	5 13 25 65
326	2 163
327	3 109
328	2 4 8 41 82 164
329	7 47
330	2 3 5 6 10 11 13 22 30 33 55 66 110 165
331	Prime
332	2 4 83 166
333	3 9 37 111
334	2 167
335	5 67
336	2 3 4 6 7 8 12 14 16 21 24 28 42 48 56 84 112 168
337	Prime
338	2 13 26 169
339	3 113
340	2 4 5 10 17 20 34 68 84 170
341	11 31
342	2 3 6 9 18 19 38 57 114 171
343	7 49
344	2 4 8 43 86 172
345	3 5 15 23 69 115
346	2 173
347	Prime
348	2 3 4 6 12 29 58 87 116 174
349	Prime
350	2 5 7 10 14 25 35 50 70 175
351	3 9 13 27 39 117
352	2 4 8 11 16 22 32 44 88 176
353	Prime
354	2 3 6 59 118 177
355	5 71
356	2 4 89 178
357	3 7 17 21 51 119
358	2 179
359	Prime
360	2 3 4 5 6 8 9 10 12 15 18 20 24 30 36 40 45 60 72 90 120 180
361	19
362	2 181
363	3 11 33 121
364	2 4 7 13 14 26 28 52 91 182
365	5 73
366	2 3 6 61 122 183
367	Prime
368	2 4 8 16 23 46 92 184
369	3 9 41 123
370	2 5 10 37 74 185
371	7 53
372	2 3 4 6 12 31 62 93 124 186
373	Prime
374	2 11 17 22 34 187
375	3 5 15 25 75 125
376	2 4 8 47 94 188
377	13 29
378	2 3 6 7 9 14 18 21 27 42 54 63 126
379	Prime
380	2 4 5 10 19 20 38 76 95 190
381	3 127
382	2 191
383	Prime
384	2 3 4 6 8 12 16 24 32 48 64 96 128
385	5 7 11 35 55 77
386	2 193
387	3 9 43 129
388	2 4 97 194
389	Prime
390	2 3 5 6 10 13 15 26 30 39 65 78 130 195
391	17 23
392	2 4 7 8 14 28 49 56 98 196
393	3 131
394	2 197
395	5 79
396	2 3 4 6 9 11 12 18 22 33 36 44 66 99 132 198
397	Prime
398	2 199
399	3 7 19 21 57 133
400	2 4 5 8 10 16 20 25 40 50 80 100 200

Table E–4 (~~C~~). Table of primes up to 2000 (U)

1	139	337	557	769	1013	1249	1493	1741
2	149	347	563	773	1019	1259	1499	1747
3	151	349	569	787	1021	1277	1511	1753
5	157	353	571	797	1031	1279	1523	1759
7	163	359	577	809	1033	1283	1531	1777
11	167	367	587	811	1039	1289	1543	1783
13	173	373	593	821	1049	1291	1549	1787
17	179	379	599	823	1051	1297	1553	1789
19	181	383	601	827	1061	1301	1559	1801
23	191	389	607	829	1063	1303	1567	1811
29	193	397	613	839	1069	1307	1571	1823
31	197	401	617	853	1087	1319	1579	1831
37	199	409	619	857	1091	1321	1583	1847
41	211	419	631	859	1093	1327	1597	1861
43	223	421	641	863	1097	1361	1601	1867
47	227	431	643	877	1103	1367	1607	1871
53	229	433	647	881	1109	1373	1609	1873
59	233	439	653	883	1117	1381	1613	1877
61	239	443	659	887	1123	1399	1619	1879
67	241	449	661	907	1129	1409	1621	1889
71	251	457	673	911	1151	1423	1627	1901
73	257	461	677	919	1153	1427	1637	1907
79	263	463	683	929	1163	1429	1657	1913
83	269	467	691	937	1171	1433	1663	1931
89	271	479	701	941	1181	1439	1667	1933
97	277	487	709	947	1187	1447	1669	1949
101	281	491	719	953	1193	1451	1693	1951
103	283	499	727	967	1201	1453	1697	1973
107	293	503	733	971	1213	1459	1699	1979
109	307	509	739	977	1217	1471	1709	1987
113	311	521	743	983	1223	1481	1721	1993
127	313	523	751	991	1229	1483	1723	1997
131	317	541	757	997	1231	1487	1733	1999
137	331	547	761	1009	1237	1489		

INDEX (Ø)

[redacted]

By Order of the Secretary of the Army:

W. C. WESTMORELAND,
General, United States Army,
Chief of Staff.

Official:
KENNETH G. WICKHAM,
Major General, United States Army,
The Adjutant General.

Distribution:

To be distributed in accordance with DA Form 12–12, Sec II requirements for training publications, pertinent to TOE 32–52, 32–56, 32–77 and 32–500.

U. S. GOVERNMENT PRINTING OFFICE: 1972 O - 468-095