~~RESTRICTED~~ ~~CONFIDENTIAL~~

TM 32-220

DEPARTMENT OF THE ARMY TECHNICAL MANUAL

BASIC

CRYPTOGRAPHY

records taken from WFF's home

DEPARTMENT OF THE ARMY • *APRIL 1950*

~~RESTRICTED~~

558.2

~~CONFIDENTIAL~~

WARNING

Authority for release of this document to a foreign government must be secured from the Director of Intelligence, GSUSA.

When this document is released to a foreign government, it is released subject to the following conditions: This information is furnished with the understanding that it will not be released to another nation without specific approval of the United States of America, Department of the Army; that it will not be used for other than military purposes; that individual or corporation rights originating in the information whether patented or not will be respected; and that the information will be afforded substantially the same degree of security as afforded by the United States of America, Department of the Army.

30 April 1959

Paul S. Willard
Colonel,   AGC
Adjutant General

DEPARTMENT OF THE ARMY TECHNICAL MANUAL

TM 32-220

This manual supersedes TM 11-484, 20 March 1945, and TM 11-485, 8 June 1944

BASIC

CRYPTOGRAPHY

DEPARTMENT OF THE ARMY • *APRIL 1950*

DEPARTMENT OF THE ARMY
WASHINGTON 25, D. C., *5 April 1950*

TM 32–220 is published for the information and guidance of all concerned.

· [AG 300.7 (2 Sep 49)]

BY ORDER OF THE SECRETARY OF THE ARMY:

OFFICIAL: J. LAWTON COLLINS
    EDWARD F. WITSELL *Chief of Staff, United States Army*
    Major General, USA
    The Adjutant General

DISTRIBUTION:

    GSUSA (1); Tech Sv (2); Arm & Sv Bd (1); AFF (10);
    OS Maj Comd (5); Basic Comd (1); MDW (1); A (ZI)(25),
    (Overseas) (10); CHQ (10); D (2); B (5); Bn 11 (5);
    FC (1); USMA (10); Sch (2); PMS&T (2); Tng Ctr (2);
    SPECIAL DISTRIBUTION.

For explanation of distribution formula, see SR 310–90–1.

CONTENTS

This manual supersedes TM 11-484, 20 March 1945, and TM 11-485, 8 June 1944

PART ONE

ELEMENTARY MILITARY CRYPTOGRAPHY

CHAPTER 1

INTRODUCTION

Section I. GENERAL

1. Scope

This manual consists of two parts as follows:

a. Part one is an introduction to the elementary principles of military cryptography. In this part a few typical examples of cipher systems and code systems are presented; the procedure in cryptographing and decryptographing by means of the systems is shown in detail; methods of preparing keys suitable for use in connection with them are illustrated; errors and their correction are discussed; and finally, a few of the most important precautions to be observed in safeguarding systems and cryptograms from enemy cryptanalysts are set forth. Only such considerations as apply to military cryptography are included.

b. Part two develops the principles established in part one and treats of the more advanced systems. Following the presentation sequence of part one, transposition systems are discussed first, then substitution systems. Considerable attention is devoted to combined substitution and transposition methods. Following this is a description of a limited number of cipher devices and machines, together with a discussion of their present-day limitations. Finally, code systems are discussed briefly with special emphasis upon enciphered code systems.

2. Developments in Cryptography

a. Cryptography is by no means a static art or science and viewpoints are always undergoing change; what is regarded as wholly impracticable today may, through some unforeseen improvement in technique, become feasible tomorrow, and it is unwise to condemn a system too hastily. For example, before World War I, and indeed for the first 2 years of that conflict, the use of codebooks in the theater of operations was

regarded as wholly impracticable.[1] Colonel Hitt in his *Manual for the Solution of Military Ciphers,* published in 1916, stated:

The necessity for exact expression of ideas practically excludes the use of cod₊ for military work, although it is possible that a special tactical code might be useful for preparation of tactical orders.

Also, in an official British Army *Manual of Cryptography* prepared in 1914 is found the following statement:

Codes will first be considered, but as they do not fulfill the conditions required of a means of secret communication in the field, they need not be dealt with here at length.

In the 1935 edition of this text the foregoing quotations were immediately succeeded by the following comment:

It need only be pointed out in this connection that today code methods predominate in the secret communication systems of the military, naval, and diplomatic services of practically all the large nations of the world. Nevertheless, it is likely that within the next decade or two the pendulum may once more swing over to the other position and cipher methods may again come to the fore, especially if mechanical and electrical cipher machines are perfected so that their operation becomes practicable for general use. It is for this reason, if for no other, that the cryptographer who desires to keep abreast of progress must devote considerable attention to the more complicated cipher methods of the past and present time, for with the introduction of mechanical and electrical devices the complexities and difficulties of these hand-operated methods may be eliminated.

In preparing the revision of this text in 1943, the author found it necessary to say that the forecast he made in 1935 in regard to the rebirth of cipher methods had been fully justified by the present trend, which is in a direction away from code and toward cipher methods, because of important advances made in the field of mechanical and electrical cryptographic mechanisms.

b. Modern electrical communication methods and instrumentalities are finding an increasing need for applications of cryptographic theory and practice to their efficient operation. For example, in very recent years there has developed a distinct need for secure methods and means for distorting voice communications by telephone or radiophone, and for distorting facsimile transmissions by wire or radiotelegraphy. Teleprinter services permitting direct cryptographic intercommunication by machines operated from a typewriter keyboard make it desirable to have means whereby, although the keyboard is operated to correspond to plaintext characters, the latter are instantaneously and automatically enciphered in transmission and the received signals are instantaneously and automatically deciphered upon reception at the receiving end. Thus the printing mechanism at the receiving station records the original

---

[1] See, in this connection, Friedman, William F., *American Army Field Codes in the American Expeditionary Forces During the First World War,* Signal Security Service Publication, OCSigO, War Department, Washington, 1942.

plain-text characters set up on the keyboard at the sending station but interception of the signals passing over the line or by radio would yield only cipher text.

c. It is difficult to foresee the specific cryptographic methods which might some day be useful in connection with developments of the foregoing nature. Progress in the electrical and electronic fields exercises an important effect upon developments in the cryptographic field. Methods which today appear to yield a high degree of cryptographic security but which are impractical for hand operation a few years from now, may be readily mechanized and become highly practical. On the other hand, methods which today do provide a high degree of security may, a few years from now, become obsolete because high-speed electrical analytical machines have been devised for their rapid solution. Consequently, if among the many and more or less complex methods set forth herein certain ones appear to fall outside the realm of what is today considered practicable, it should be remembered that the purpose in describing them is to present various basic cryptographic principles, and not to set forth methods that may with a high degree of probability be encountered in military cryptography in the immediate future.

Section II. TERMINOLOGY

3. Basic Definitions

In a study of military cryptography as employed in the U. S. Army, the following definitions will be useful:

a. SIGNAL COMMUNICATIONS. Any means of transmitting messages in plain or encrypted text 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. AGENCY OF SIGNAL COMMUNICATION. The organization, teams, and personnel necessary to perform operational duties pertaining to signal communications.

c. MESSAGE. Used in its broadest sense in Department of the Army and other official publications, the term "message" includes all instructions, reports, orders, documents, photographs, maps, or other information, transmitted by means of signal communication. In this manual, however, the term "message" implies instructions, reports, orders, and similar communications usually transmitted by electrical means.

d. MEANS OF SIGNAL COMMUNICATION. A medium (including equipment) used by an agency for transmitting messages. There are two

3

dozen or more different means; the most important, so far as this manual is concerned, are—

(1) *Wire:*
    Telephone.
    Telegraph.
    Teletypewriter.
    Facsimile (picture or photo transmission).

(2) *Radio:*
    Radiotelephone.
    Radiotelegraph.
    Radio teletypewriter.
    Radio facsimile.

e. WRITER. The person who actually prepares and signs the message blank. The writer may be the originator or his officially designated representative.

f. ORIGINATOR. The authority who orders the message written and sent. The commander may delegate this authority to one or more subordinates. Officers assigned as members of a unit's general staff are assumed to have been so designated.

g. TIME OF ORIGIN. The time shown on a message by the writer to indicate the hour and minute when he completed its writing.

h. ADDRESSEE. The authority (organization, office, or person) to whom a message is directed by the originator.

i. MESSAGE CENTER. That signal communication agency of a headquarters, or echelon thereof, which is charged with the receipt, routing and delivery of all official messages except: those which are transmitted directly from the originator to the addressee by means of a personal agent, or telephone or teletypewriter provided for his personal use; mail handled by military or civil postal services, and purely local messages.

j. COMMUNICATIONS CENTER. One or more agencies of signal communication equipped to receive, route, and transmit official messages. A communications center may be established at a point fixed or mobile.

4. Cryptology and Secret Communication

a. Secrecy of intercommunication in military operations is of the utmost importance. Need for it has been recognized from the earliest days of organized warfare. That branch of knowledge which treats the production, use and solution of the means and methods of secret[2] communications is called *cryptology.*

---

[2] Throughout this manual the term "secret" will be used in its ordinary sense as given in the dictionary. Whenever the designation is used in the more restricted sense of the security classification as defined in AR 380–5, it will be so indicated. There are in current use the classifications, *Restricted, Confidential, Secret,* and *Top Secret,* listed in ascending order of degree.

4

b. Intercommunication may be conducted by any means susceptible of ultimate interpretation by one of the five senses, but those most commonly used are visual or auditory. Aside from the use of simple visual and auditory signals for intercommunication over relatively short distances, the usual method of intercommunication involves, at one stage or another, the act of *writing, speaking* over a telephone, or of *drawing* or *taking a picture.*

c. To preserve secrecy of intercommunication by telephone, there are means and methods of disguising the electrical currents in telephony so that the messages or conversations can be understood only by persons provided with the proper equipment. The same thing is true of secrecy in the electrical transmission of pictures, drawings, maps, etc. However, this manual is concerned only with secrecy of intercommunication by means of messages conveying in written words the thoughts, orders, reports, etc., of the originator to the addressee.

d. Writing may be either *visible* or *invisible.* In the former, the characters are inscribed with ordinary writing materials and can be seen with the naked eye; in the latter, the characters are inscribed by means or methods which make the writing invisible to the naked eye. Invisible writing is done with certain chemicals called *invisible, sympathetic,* or *secret inks* which have the property of either being initially invisible to the naked eye or becoming so after a short time. In order to make writing done with secret inks visible, special processes must usually be applied. There are also methods of producing writings which is invisible because the characters are of microscopic size. These methods usually require either special photographic apparatus or very delicate mechanical instruments called micropantographs, by means of which ordinary writing may be copied in extremely reduced size. Magnifying lenses must be used to make such writing visible to the naked eye.

e. Invisible writing and visible writing prepared in a form unintelligible in the language in which it is written, constitute *secret writing.* Both of these forms of secret writing have their uses in military communications, but this manual deals only with visible secret writing.

5. Plain Text and Encrypted Text

a. A visible message which conveys an intelligible meaning in the language in which it is written, with no hidden meaning, is said to be in *plain text.* A message in plain text is called a *plain-text message,* a *clear-text message,* or a *message in clear.*

b. A visible message which conveys no intelligible meaning in any language is said to be in *encrypted text.* Such a message is termed a *cryptogram.*

c. A visible message may convey an intelligible meaning which may not be the real meaning intended. To quote a simple example of a mes-

5

sage containing a secret or hidden meaning, prepared with the intention of escaping suppression by censors in war time, the sentence "Son born today" may mean "Three transports left today." Messages of this type are in encrypted text and are said to be in *open code*. Although occasionally useful in espionage and counter-espionage, secret communication systems of this sort are impractical for field military use, and will not be dealt with further in this manual.

d. The term "correspondents" is used in this manual to designate persons who exchange messages with each other. Between the originator and the addressee there may be persons who actually write and handle the messages, who convert the plain texts into cryptograms, or who reconvert the cryptograms into plain texts. The originator and the addressee may also do this work but in the U. S. Army such work is usually done by special personnel who act as agents of the correspondents.

e. The term "enemy" is used in this manual to designate all persons who obtain messages or copies of messages not intended for them.

6. Cryptography, Cryptographing, and Decryptographing

a. Cryptography is that branch of cryptology which treats of various means and methods for rendering plain text unintelligible and reconverting unintelligible text into plain text or the application thereof.

b. To *cryptograph*[3] (*encrypt*) is to convert a plain-text message into a cryptogram by following certain rules agreed upon in advance by correspondents, or furnished them or their agents by higher authority. The process of *cryptographing* a message produces a *cryptogram*.

c. To *decryptograph* (*decrypt*) is to reconvert a cryptogram into the equivalent plain-text message *by a direct reversal of the cryptographing process;* that is, by applying to the cryptogram the key used in cryptographing the plain text.

d. A person skilled in the art of cryptographing and decryptographing, or one who has a part in making a cryptographic system is called a *cryptographer;* a clerk who cryptographs and decryptographs, or who assists in such work, is called a cryptographic clerk.

7. Codes, Ciphers, and Enciphered Code

a. Cryptographing and decryptographing are accomplished by means collectively designated as *codes* and *ciphers*. Such means are used for either or both of two purposes: (1) secrecy, and (2) economy or brevity. Secrecy usually is far more important in military cryptography than economy or brevity. In ciphers or *cipher systems* cryptograms are produced by applying the cryptographic treatment to *individual letters* of the plain-text messages, whereas in codes or *code systems* cryptograms are produced by applying the cryptographic treatment to entire words,

---

[3] Compare the terms *"cryptography," "cryptogram,"* and *"cryptograph"* with the terms *"telegraphy," "telegram,"* and *"telegraph."*

6

phrases, and sentences of the plain-text messages. The specialized mean-
ings of the terms *code* and *cipher* are explained in detail later.

b. A cryptogram produced by means of a cipher system is said to be
in cipher and is called a *cipher message,* or sometimes simply a *cipher.*
Such act or operation of cryptographing is called *enciphering,* and the
enciphered version of the plain text, as well as the act or process itself,
is often referred to as the *encipherment.* The cryptographic clerk who
performs the process serves as an *encipherer.* The corresponding terms
applicable to the decryptographing of cipher messages are *deciphering,
decipherment,* and *decipherer.* A clerk who serves both as an encipherer
and decipherer of messages is called a *cipher clerk.*

c. A *cipher device* is an apparatus or a simple mechanism for literal
encipherment and decipherment, usually manually powered; a *cipher
machine* is an apparatus or complex mechanism for literal encipherment
and decipherment, usually requiring an external power source.

d. A cryptogram produced by means of a code system is said to be
in code and is called a *code message,* or sometimes simply a *code.* The
text of the cryptogram is referred to as *code text.* This act or operation
of cryptographing is called *encoding,* and the encoded version of the plain
text, as well as the act or process itself is referred to as the *encodement.*
The clerk who performs the process serves as an *encoder.* The corres-
ponding terms applicable to the decryptographing of code messages are
decoding, decodement, and *decoder.* A cryptographic clerk who serves
both as an encoder and decoder of messages is called a *code clerk.*

e. Sometimes, for special purposes, the code text of a cryptogram
undergoes a further step in concealment involving an enciphering process,
thus producing what is called a cryptogram in *enciphered code,* or an
enciphered-code message. Encoded cipher, the cipher text of a crypto-
gram which subsequently undergoes encodement, is also possible but rare.

f. In U. S. Army tables of organization and other publications, cipher
clerks and code clerks are cryptographic technicians. They are specifically
trained to encipher, decipher, encode, and decode messages, using
authorized means, equipment, and procedures.

8. General System and Specific Key

a. The total of all the basic, invariable rules followed in cryptograph-
ing a message according to a given method, together with all the agree-
ments, conventions or private understandings drawn up between the
correspondents or their authorized agents or furnished them by higher
authority, constitute the *general cryptographic system.*

b. In the general cryptographic system usually a number, a group of
letters selected at random, a word, a phrase, or a sentence, is used as a
key. The element selected governs the manner in which a cipher device
or a cipher machine is prepared for the encipherment or decipherment

7

of a specific message, or it controls the steps followed in cryptographing a specific message. This element—usually of a variable nature and changeable at the will of the correspondents, or prearranged for them or for their agents by higher authority—is the *specific key*. The specific key may also involve the use of a set of specially prepared tables, a special document, or even a book.

c. Hereafter, the general cryptographic system will be referred to as the *system*, and the specific key, as the *key*.

9. Cryptanalytics and Cryptanalysis

a. In theory, any cryptographic system except one can be broken down if enough time and skill are devoted to it, and if the volume of traffic is large enough. This can be done even if the general cryptographic system and the specific key are unknown at the start. The exception is the "one time" system in which the key is used only once and in itself must have no systematic construction, derivation, or meaning. In military operations theoretical rules must usually give way to practical considerations. How the theoretical rule in this case is affected by practical considerations will be taken up in subsequent portions of this manual.

b. That branch of cryptology which deals with the principles, methods, and means employed in the solution or *analysis* of cryptograms is called *cryptanalytics*.

c. The steps and operations performed in applying the principles of cryptanalytics constitute *cryptanalysis*. To cryptanalyze a cryptogram is to *solve* it by cryptanalysis.

d. A person skilled in the art of cryptanalysis is called a *cryptanalyst*, and a clerk who assists in such works is called a *cryptanalytic technician*.

Section III. TWO CLASSES OF CRYPTOGRAPHIC SYSTEMS

10. Transposition and Substitution

a. Technically there are only two distinct types of treatment which may be applied to plain text to convert it into secret text, yielding two different *classes* of cryptograms. In the first, called *transposition*, the *elements* or *units* of the plain text, whether one is dealing with individual letters or groups of letters, syllables, whole words, phrases and sentences, retain their original identities and merely undergo some change in their relative positions or sequences so that the message becomes unintelligible. In the second, called *substitution*, the elements of the plain text retain their original positions or sequences but are replaced by other elements with different values or meanings.

b. It is possible to cryptograph a message by a substitution method and then to apply a transposition method to the substitution text, or vice

8

versa. Such combined transposition-substitution methods do not form a third category of methods. They are occasionally encountered in military cryptography, but the types of combinations that are sufficiently simple to be practicable for field use are very restricted.

11. Letter, Syllable, and Word Methods

Under each of the two principal classes of cryptograms as outlined in the preceding paragraph, a further classification can be made with respect to the nature of the *textual elements* or *units* with which the cryptographic process deals. These textual units are (1) individual letters, or groups of letters in regular sets, and (2) complete words. Methods which deal with the first type of units are called *letter methods,* including, when such is the case, *syllable methods;* those which deal with the second type of units are called *word methods.*

12. Cipher Systems and Code Systems

It is necessary to indicate that the classification into letter, syllable, and word methods is more or less arbitrary or artificial in nature, and is established for purpose of convenience only. No sharp line of demarcation can be drawn in every case, for occasionally a given system may combine methods of treating single letters, groups of letters, syllables, whole words, phrases and sentences. When in a single system the cryptographic treatment is applied to textual units of regular length, usually single letters or pairs, and is only exceptionally applied to textual units of irregular length, the system is called a *cipher system.* Likewise, when in a single system the cryptographic treatment is applied to textual units of irregular length, usually whole words, phrases, and sentences, and is only exceptionally applied to single letters, pairs, or groups of letters and syllables, the method is called a *code system* because it generally involves the use of a code book.

Section IV. SECURITY AND TIME ELEMENTS IN CRYPTOGRAPHIC SYSTEMS

13. Interception, Radio Direction Finding, and Radio Position Finding

a. Messages transmitted by electrical means can be heard and copied by persons who are not the correspondents or their authorized agents. Messages transmitted by radio can be manually copied or automatically recorded by suitably adjusted radio apparatus located within range of the transmitter. Some messages transmitted over wire lines can likewise be

manually copied or automatically recorded by special apparatus suited for the purpose. Correspondents have no way of knowing whether or not radio transmissions are being copied by the enemy, since the unauthorized copying does not interfere in the slightest degree with signals being transmitted. Interception of wire traffic is much more difficult than of radio, mainly because the equipment must be located very near the wire line, or connected directly to it. The act of listening-in and copying or recording electrically-transmitted messages by persons other than the correspondents or their authorized agents is called *interception*. The purpose of interception is to obtain copies of messages transmitted and, by studying them, to obtain information. In time of war, it must be assumed that the enemy will intercept all messages transmitted by any signal communication agency susceptible of interception.

b. It is also possible to determine, with a fair degree of accuracy, the direction of a radio transmitter from a given location and, by establishing the direction from two or more locations, it is possible to determine the geographical location of the transmitter. The science which deals with the means and methods of determining the direction in which a radio transmitter lies is called *radio direction finding;* the method of determining the geographical location of a radio transmitter, by the use of two or more direction-finding installations, is called *radio position finding.*

c. Messages may be transmitted by signals with special apparatus which distort, disguise, or completely hide the signals themselves, so that the processes of interception and recording the signals are very difficult, and intercept personnel may not even be aware of the existence of such signals. All such methods of transmitting messages fall in the class designated in this manual as *systems of secret signaling.* Signaling by means of so-called "black light," that is, invisible or infra-red light waves, falls into this category. Methods of disguising or distorting voice or picture transmissions (par. 2c) require more or less highly-specialized apparatus for the interception of the signals and their interpretation or recording in recognizable form. As a rule, the signals of practically all systems of secret signaling can be intercepted and recorded in a form suitable to making the signals understood by one of the senses, usually visual or auditory. Ordinarily, this requires special apparatus but can sometimes be done without the specific apparatus used in forming or sending the signals, or the "key" used in their distortion, or disguise.

14. Traffic Analysis and Cryptanalysis

a. A great deal of information of military value can be obtained by studying signal communications without solving the crytographed messages constituting the traffic. The procedure and the methods used have yielded results of sufficient importance to warrant the application of a

special term to this field of study; namely, *traffic analysis*[4], which is the study of signal communications and intercepted or monitored traffic for the purpose of gathering military information without recourse to cryptanalysis.

b. In general terms, traffic analysis is the careful inspection and study of signal communications for the purpose of penetrating camouflage superimposed upon the communication network for purposes of security. Specifically, traffic analysis reconstructs radio communication networks by: (1) noting volume, direction, and routing of messages; (2) correlating transmission frequencies and schedules used among and within the various networks; (3) determining directions in which transmitters lie, by means of radio direction finding; (4) locating transmitters geographically, by radio position finding; (5) developing the system of assigning and changing radio call signs; (6) studying all items that constitute "conversations" or "chat" exchanged among operators on radio channel.

c. From a correlation of general and specific information derived from these procedures, traffic analysis is able not only to ascertain the geographic location and disposition of troops and military units (technically called "order of battle") and important troop movements, but also to predict with a fair degree of reliability the areas and extent of immediately pending or future activities. Traffic analysis procedures are followed to obtain information of value concerning the enemy, and to determine what information concerning our own forces is made available to the enemy through our own signal communications.

d. These very important results are obtained without actually reading the texts of the intercepted messages; the solution and translation of messages are the functions of cryptanalysis and not traffic analysis. However, the cryptanalyst is frequently able to make good use of bits of information disclosed by traffic analysis such as faults noted in message routing and errors in cryptography causing messages to be duplicated or canceled. Cryptanalysis can provide important information for traffic analysis, since the solution of messages often yields data on impending changes in signal communication plans, operating frequencies and schedules, etc. It also yields data on specific channels, networks, or circuits which are most productive of intelligence, so that effective control and direction of intercept agencies for maximum results can be achieved.

e. In addition to (1) traffic analysis and (2) cryptanalysis as means of obtaining information relating to communications, further data may be obtained (3) by the use of secret agents for espionage, (4) by the capture and interrogation of prisoners, (5) by the capture of headquarters or command posts with records more or less intact, and (6) by treason or carelessness on the part of personnel who handle communications. Of

---

[4] Which may be abbreviated *tranalysis.*

these six main sources, traffic analysis and cryptanalysis are the most valuable. The amount of vital information they furnish cannot be accurately estimated as it fluctuates with time, place, circumstances, equipment, and personnel. For most effective operation, the results of both cryptanalysis and traffic analysis can be fitted together to yield a unified picture of the communications scheme. Therefore, if all transmitting stations can be located quickly and if all communications can be intercepted and solved, extremely valuable information concerning strength, disposition of forces, and proposed moves will be continually available.

f. The facts set forth above are applicable to our own forces as well as the enemy's.

g. The process of intercepting and copying our own or friendly radio and wire transmissions for the purpose of detecting and correcting violations of regulations is called *monitoring;* it provides increased protection of our own signal communications.

15. Communication Intelligence and Communication Security

a. Communication intelligence is evaluated information concerning the enemy, derived principally from a study of his signal communications. The main components of communication intelligence are as follows:

(1) Interception of signals or messages and forwarding raw traffic to communication intelligence centers for study.

(2) Traffic analysis, including radio direction finding and radio position finding. (Evaluated information from this source is often called *traffic intelligence.*)

(3) Cryptanalysis or solution (and translation, when necessary) of the texts of the messages.

(4) Evaluation of data, that is, analysis of results obtained from the preceding steps and their correlation, collation, and comparison with results obtained from other sources of information.

b. Communication security is the protection resulting from all measures designed to deny to unauthorized persons information of value which may be derived from communications. The main components of communication are as follows:

(1) *Physical security,* that component of communication security which results from all measures necessary to safeguard classified communication equipment, and material from access thereto by unauthorized persons.

(2) *Cryptosecurity,* that component of communication security which results from the provision of technically sound *cryptosystems*[5] and their proper use.

---

[5] *Cryptosystems* may be categorized as literal and nonliteral. This manual is concerned solely with *literal* or *cryptographic* systems.

12

(3) *Transmission security,* that component of communication security which results from all measures designed to protect transmissions from interception and traffic analysis.

c. Further details on the subject of communication security will be found in JANAP 122(A) Joint Communications Instructions.

16. Time Needed for Cryptanalysis and its Dependent Factors

a. In military operations time is a vital element. The influence or effect that analysis of military cryptograms may have on the tactical situation depends on various time factors.

b. Of these factors, the following are the most important:

(1) The length of time necessary to transmit intercepted enemy cryptograms to solving headquarters. This factor is negligible only when signal communication agencies are properly and specifically organized to perform this function.

(2) The length of time required to organize raw materials, to make traffic analysis studies and to solve the cryptograms, and the time required to make copies, tabulate, and record data.

(3) The nature of information disclosed by traffic analysis studies and solved cryptograms; whether it is of immediate or operational importance in impending action, or whether it is of historical interest only in connection with past action.

(4) The length of time necessary to transmit information to the organization or bureau responsible for evaluating the information. Only after information has been evaluated does it become *military intelligence.*

(5) The length of time necessary to transmit resulting military intelligence to the agency or agencies responsible for tactical operations, and the length of time necessary for the agency to prepare orders for the action determined by the intelligence and to transmit them to the combat units concerned. The last sentence under (1) above applies here also.

c. Of the factors mentioned in *b* above, the only one of direct interest in this manual is the length of time required to solve the cryptograms. This is subject to great variation, dependent upon other factors, of which the following are the most important:

(1) *The degree of cryptographic security* in the system. The degree of security depends upon the technical soundness of the system itself. Technical soundness, in turn, determines the resistance to analysis which the system offers. Cryptographic systems vary widely in technical soundness, but this manual does not attempt to demonstrate such variation.

(2) The adequacy and technical soundness of regulations drawn up by designers of the cryptographic system for the guidance of cryptographic technicians who are its actual users.

(3) The extent to which cryptographic technicians follow these regulations and procedures. Security of a good cryptographic system can be almost completely destroyed by a few cryptographic technicians who fail to observe the regulations, are careless in their observance, in sheer ignorance commit serious violations of cryptographic security, *or adopt bad technical habits*. As a result, these technicians jeopardize not only their own lives but the lives of thousands of their comrades.

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

(5) The number, skill, and efficiency of organization and cooperation of signal intelligence units assigned to the work. Cryptanalytic headquarters are organized in units of ascending size, ranging from a few persons in the forward echelons to many persons in the rear echelons. Such organization avoids duplication of effort and, especially in forward areas where spot intelligence is most useful, makes possible the quick interpretation of cryptograms in already solved systems. In all these units, proper organization of highly skilled workers is essential for efficient operation.

(6) The amount and character of information and intelligence available to the cryptanalytic headquarters. Isolated cryptograms exchanged between a restricted, small group of correspondents, about whom and whose business no information is available, may resist the efforts of even a highly organized, skilled cryptanalytic office indefinitely. If, however, a certain amount of such information is obtained, the situation may be entirely changed. In military operations usually a great deal of collateral information is available, from sources indicated in paragraph 14e. As a rule, a fair amount of more or less definite information concerning specific cryptograms is at hand, such as proper names of persons and places, and events in the immediate past or future. Although the exchange of information between intelligence and cryptanalytic staffs is very important, the collection of information derived from an intensive study of already solved traffic is equally as important because it yields extremely

valuable *cryptanalytic intelligence* which greatly facilitates the solution of new cryptograms from the same sources.

17. Degree of Crytographic Security Required of a System for Military Use

The ideal cryptographic system for military purposes would be a *single, all-purpose* system which would be practicable for use not only by the largest fixed headquarters but also by the smallest troop unit in the combat area, and which would also present 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 realm of possibility so far as present methods of cryptographic communication are concerned; in fact, a multiplicity of systems must be employed, each more or less specifically designed for a particular purpose. Of each such system, *the best that can be expected is that the degree of security be great enough to delay solution by the enemy for such a length of time that when the solution is finally reached the information thus obtained has lost all its "short term," immediate, or operational value, and much of its "long term," research, or historical value.*

18. Fundamental Practical Requirements of a Cryptographic System for Military Use

a. Military cryptograms must meet certain fundamental requirements of a practical nature because of definite limiting conditions in present military signal communication means and methods.

b. These requirements are (1) reliability, (2) security, (3) rapidity, (4) flexibility, and (5) economy. Their relative importance is in the order named.

c. Reliability is of first importance. Reliability, as applied to a cryptographic system or device, means that the cryptograms produced by the sending or originating office will be decryptographed promptly, accurately, and without ambiguity by the receiving office; that the cryptographic system, whether a book, machine, or device, will be on hand and in good working order, available for instant use; and that when used it can be expected to be operative as long as needed. Simplicity is implied in reliability; usually, the more simple the system, the more reliable it is. Security is the protection afforded by a sound cryptographic system; rapidity, the speed with which messages can be cryptographed and decryptographed, usually expressed in words or 5-letter groups per minute. The conflicting requirements of *security* and *rapidity* vary according to circumstances. Signal communication personnel must be governed by general principles, subject to existing circumstances, rather than by rigid

regulations. Maximum security at all times should be the goal, but in messages exchanged among the higher headquarters some speed may be sacrificed to meet greater security requirements, while in messages exchanged among the lower headquarters security must often give way to greater speed requirements. For this reason various cryptographic systems must be available to meet varying types of situations. As to flexibility, a cryptographic system specifically adapted for a particular usage cannot serve as an all-purpose system. A codebook designed for frontline use can hardly serve the needs of a high headquarters in the rear; nor can a cryptographic system designed for use by a high headquarters serve the needs of a small combat unit. As to economy, the simpler the operations involved, the shorter will be the texts produced, the amount of time required to produce the cryptographic material, use it, and transmit the messages; and the greater will be the economy.

   d. Specific requirements which should be met by a cryptographic system for general military use are set forth below.

   (1) Cryptograms must be in a form suitable for transmission by standard telegraphic equipment and methods. This requirement generally eliminates all systems except those which produce cryptograms composed of characters readily transmitted by a telegraphic system employing either the Morse or the teleprinter alphabet. Cryptographic systems using Arabic numerals are not so desirable as those using letters because the Morse signals for numbers are longer, except when "cut" numbers are used, and are more difficult for the average American telegraph or radio operator to handle. Systems which produce cryptograms composed of mixtures of letters and figures, or of letters, figures, and punctuation signs, and which must be transmitted by Morse telegraphy are unsuited for practical usage. However, where such intermixtures are produced automatically by the cryptographic mechanism and are transmitted, received, and deciphered automatically, as certain teleprinter enciphering systems, their use is permissible. In order to be suitable for economical Morse telegraphic transmission, the cryptographic text must be capable of being arranged in regular sets of characters for these reasons: first, it promotes accuracy in telegraphic transmission (since an operator knows he must receive a definite number of characters in each group, no more and no less); and secondly, cryptanalysis is usually made more difficult when the length of the words, phrases, and sentences of the plain text is not apparent. The usual grouping is in sets of five characters, although occasionally other groupings may be made in special circumstances. Such grouping is not necessary in teleprinter encipherment systems.

16

(2) Regular channels of signal communication carry but a limited volume of traffic. Their most efficient operation demands that the smallest number of characters actually necessary to convey a given message be transmitted. Therefore, the cryptographic text should be no longer than its equivalent clear text. In an exceptional case, the cryptographic text may be longer than the equivalent clear text, but a system in which the cryptographic text is twice the length of the equivalent clear text is useful only if it is of outstanding merit and suitable for certain restricted or special use. No system in which the cryptographic text is more than twice the length of the equivalent clear text is practicable for military usage. Most of the cryptographic systems in current use produce cryptograms which correspond in length with that of the original plain-text message or are somewhat shorter.

(3) General requirements of reliability and speed are that the operations of cryptographing and decryptographing be relatively simple and rapid. For use in the combat zone, operations must be capable of being performed under difficult field conditions and must not require the remembering and application of a long series of steps or rules. They must be such as to reduce the mental strain on the operator to a minimum. Complex processes requiring several distinct steps are not suited to use in the combat zone, but occasionally systems involving only two steps, if each step is simple and rapid, may be practicable for military usage.

(4) Cipher devices or machines for field use must be light in weight, rugged in construction, and simple in operations, requiring the services of only one operator. Requirements to be met by high-speed cipher machines are too complex to be described in this manual.

(5) The system must be such that errors, which invariably occur in cryptographic communications, can be corrected easily and rapidly by cryptographic technicians. A system is impractical if frequently it is necessary to call for a repetition of the whole transmission, or for a rechecking of the original cryptographing.

e. Only a few of the systems which fulfill at least several of the foregoing practical requirements are included in this manual.

CHAPTER 2
ELEMENTARY TRANSPOSITION SYSTEMS

Section 1. SIMPLE MONOLITERAL TRANSPOSITION METHODS

19. Transposition Ciphers in General

Transposition ciphers are like "jig-saw puzzles" in that all the pieces of which the whole original is composed are present but are merely disarranged. The pieces into which the picture forming the basis of a jig-saw puzzle may be divided are irregular in size and shape, but the pieces into which the plain text forming the basis of a transposition cipher may be divided must be much more regular, for the sake of practicability. They must be either single letters or pairs of letters, or sets of letters in regular groupings, or, in an exceptional case, whole words. Most transposition methods however, deal with individual letters and are therefore termed "monoliteral methods." The other methods are termed "polyliteral methods."

20. Geometric Designs

a. Practically all monoliteral or polyliteral transposition ciphers involve the use of a design or geometric figure, such as a square, rectangle, triangle, trapezoid, etc., in which the letters of the plain text are first *inscribed* or written according to a previously agreed-upon direction of writing and then *transcribed* or rewritten according to another and different, previously agreed-upon direction to form the text of the cryptogram. In nearly all cases the specific key consists in (1) using designs of a specific nature and dimensions, and (2) varying the direction or manner of inscription or transcription, or both.

b. In working with transposition ciphers or, for that matter, most types of ciphers, cross-section paper will be found very convenient. Cross-section paper with ¼-inch squares is most suitable. For brevity in reference, the individual small squares of such cross-section paper will hereafter be called *cells*.

21. Route Transpositions

a. Suppose the correspondents agree to use the method of monoliteral transposition known as *route transposition*. The message is inscribed

within a rectangle in the usual manner of writing, that is, from left to right and in consecutive lines from top to bottom. If one or more cells are vacant at the end, *nulls* or *dummy* letters—letters having no significance—are inserted as "fillers" to complete the rectangle. Then, to form the cipher text, the letters in the design are taken out of the design and rewritten or transcribed by following or tracing one of many different routes. It is possible for each route to have a different starting point, and normally it is one of the four corners, of the rectangle. A few typical routes are illustrated in figure 1 where, for the sake of ease in following the route, the plain-text message is assumed to be merely the sequence of letters A B C ... X.

(A) Simple horizontal:

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

(B) Simple vertical:

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

(C) Alternate horizontal:

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

(D) Alternate vertical:

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

Figure 1

(E) Simple diagonal:

	(1)	(2)	(3)	(4)
	ABDGHO	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

(F) 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

(G) Spiral, clockwise:

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

(H) Spiral counterclockwise:

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

Figure 1—Continued.

b. It is apparent that instead of following the normal direction of writing, that is, from left to right and from the top downwards, the letters of the plain text may be inscribed according to any one of the routes agreed upon, and then transcribed to form the cipher text by taking the letters from the rectangle in the normal manner, that is, in this case from left to right, and from the top downwards, or *by following any other route of transposition.*

22. Example of Encipherment and Decipherment by Monoliteral Route Transposition

a. Now take a special example of encipherment by monoliteral transposition. Use the message ATTACK HAS BEEN POSTPONED UNTIL TOMORROW TWO AM, and employ a relatively complicated method. Suppose that the general system agreed upon is the one being described, and that the specific key consists of the following elements:

(1) Using a completely filled rectangle of seven columns;

(2) Inscribing the letters of the plain text within the rectangle by following route (F) (3) of figure 1;

(3) Transcribing the thus inscribed letters (to form the cipher text) by following route (E) (6) of figure 1.

Since the message contains a total of 40 letters, and it has been agreed to use a completely filled rectangle of seven columns, it is necessary to add two nulls to make the total number of letters a multiple of seven. A rectangle of seven columns of cells and six lines of cells is therefore prepared. The design is then filled in as shown in figure 2.

b. To decryptograph such a cryptogram the process is merely reversed. First, the total number of letters in the cipher text must be found. Since

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

Cryptogram:

TMLAO WROWT ROMOT DUNTI LENOP
TSEEN POBSA HACKT TA

Figure 2

it is 42, and since a completely filled rectangle of seven columns has been agreed upon, a design consisting of seven columns and six rows is outlined on cross-section paper. The cipher text is then inscribed according to route (E) (6) of figure 1, and after this has been completed the plaintext letters are read according to route (F) (3), figure 1. It is apparent that it is necessary to remember a relatively long series of rules, and even when the cryptographing has been accomplished correctly the degree of security is very low. Note how obviously the whole word UNTIL manifests itself in the cipher text. Parts of other words can also be seen. The degree of security remains very low despite the variability afforded by the dimensions of the rectangle, the method of inscription and transcription and their starting points.

23. Use of Nulls in Transposition

a. It will be noted that the two nulls selected as fillers to complete the rectangle in the preceding example were the letters L and T. These were chosen rather than such letters as J, K, Q, X, or Z, for a reason which is important to note. Since transposition ciphers of this type involve merely a rearrangement of the letters, without any change whatever in their identities, it follows that the natural or normal frequencies of letters of plain text remain unchanged. Now, the letters of every alphabetic language have characteristic frequencies, as a result of which certain clues are afforded in cryptanalysis. The presence, in transposition ciphers, of letters of very low frequency (in English), such as J, K, Q, X, or Z, is very unusual and therefore if these are employed merely as fillers they may afford clues as to the real number of letters in the plain text, the starting or finishing points of the real text, etc. For this reason it is best to insert as fillers in transposition ciphers letters of medium or high frequency, such as E, T, R, I, N, O, A, S, D, L, or C, for these will not afford any clues to solution. Nulls, when employed for the purpose of making cryptanalysis more difficult, may also be inserted in specific positions as prearranged, or they may be inserted at random if the system permits. This is true of other cryptographic systems, but as a general rule the use of nulls, especially in cipher systems, is to be discouraged. Very often they add little if any security, and thus merely increase the length of the cryptographic text without any compensating advantages.

b. Whenever it is necessary to add nulls in order to complete a transposition message in any respect, or for any reason whatsoever, they must be added *before* the transposition process is applied and not afterward; otherwise it will be difficult or even impossible for the decryptographing clerk to read the message. This is especially true when the service regulations require that the final group in a cryptogram be a complete group, containing exactly as many letters as all other groups in the message.

24. Special Cases of Route Transposition

a. The oldest and simplest transposition method known, that called reversed writing, is a special case of one of the routes shown in figure 1. Here the text is written in the opposite direction from the normal; for example, BRIDGE DESTROYED is written EGDIRB DEYORTSED. The variability of the scheme, that is, the *specific key,* consists of the fact that the reversal may be applied to groups of fixed length, to whole words, to sentences, or to the whole text. The security of simple reversed writing may be somewhat increased by disguising the original word lengths, by which is meant a destruction of the normal, or natural word limits by combining a part of one word with a part of the next to form either *false words* or groups of regular length.

b. Some examples of reversed writing follow. Let the message be: BRIDGE DESTROYED AT ELEVEN PM.

    (1) Reversing only the words and retaining original word lengths:
        Cipher: **EGDIRB DEYORTSED TA NEVELE MP**

    (2) Reversing only the words and regrouping into false word lengths:
        Cipher: **EG DIRB DEYORT SEDTA NEVE LEMP**

    (3) Reversing the whole text and regrouping into fives:
        Cipher: **MPNEV ELETA DEYOR TSEDE GDIRB**

    (4) Reversing the whole text, regrouping into fives, and inserting a null in every fifth position:
        Cipher: **MPNER VELEO TADEB YORTH SEDEA GDIRB**

c. A second very simple type of transposition, that known as *vertical writing,* is a special case of another of the routes shown in figure 1.

The message BRIDGE DESTROYED is written in two vertical columns, and the cipher text is taken from the horizontal pairs thus formed. The message becomes:

	BS
	RT
	IR
	DO
BSRTI RDOGY EEDDE	GY
	EE
	DD
	E

Figure 3.

When the plain text is inscribed in pairs of letters in vertical writing and then the cipher text is taken by transcribing the columns, a slightly different result is obtained. Using the plain text message BRIDGE DESTROYED, the cipher becomes:

	BR
	ID
	GE
	DE
	ST
BIGDS RYDRD EETOE	RO
	YE
	D

Figure 4.

23

This type of transposition is sometimes called the *rail-fence* cipher because it can be produced by writing the message in the following form:

B I G D S R Y D
R D E E T O E

which yields the same cipher result as before.

25. Remarks on Monoliteral Route Transposition

Reversed writing and vertical writing of the types indicated yield extremely simple cryptograms. In practice they are sometimes used in connection with other more or less simple cryptographing methods to increase their security. The cryptographic security of the other methods thus far indicated is also very low, despite the apparently large degree of variability they afford. The reason is that the route to be followed in the inscription or transcription process is definitely fixed under each type of route. In other types of transposition soon to be discussed, a much wider latitude for variation in the route is afforded by the use of key words to control or to guide these processes. Geometric designs are also used in these types of transposition, and key words determine the dimensions of the design, or else, if only one key word is used, it determines one dimension, the other being determined by the length of the text. Examples given in their proper place will serve to illustrate the processes.

26. Key Words and Numerical Keys

a. It is often necessary, in performing certain cryptographic operations, to employ a *numerical key*, which may consist of a relatively long sequence of numbers difficult or impossible for the average cipher clerk to memorize. To avoid making it necessary that such sequences of numbers be carried on the person in written form, a dangerous procedure, cryptographers have devised very simple methods of deriving such sequences from words, phrases, or sentences, which can usually be remembered much more easily than can unintelligible, relatively long sequences of numbers. One of the simplest methods is to assign numerical values to the letters of the key in accordance with their relative positions in the ordinary alphabet. Such a key is called a *derived numerical key*. This method of assigning the numbers is very flexible and varies with different uses to which numerical keys are put. For purposes of transposition, the method shown below is very satisfactory.

b. Let the prearranged key word be the word CARBUNCLE. Since the word contains the letter A, which comes first in the alphabet, the number 1 is written under this letter in the key word. Thus:

C A R B U N C L E
  1

The next letter of the normal alphabet that occurs in the key word is B, which is assigned the number 2. The letter C, which occurs twice in the key word, is assigned the number 3 for its first occurrence, the number 4 for its second occurrence, and so on. The final result is:

Basic key word: C-A-R-B-U-N-C-L-E

Derived numerical key: 3-1-8-2-9-7-4-6-5

c. The method may, of course, be applied to phrases or to sentences, so that a very long numerical key, impossible ordinarily to remember, may be so derived at will from an easily remembered *key text*.

d. It is advisable to make note of a few points valuable in connection with the choice of key text:

(1) It should be such as can be easily remembered. Often a key composed of two or more short words is better than one consisting of a single long word. Thus, the whole sentence WHEN DO WE EAT would be better than the single word EXTRAORDINARY.

(2) It should consist of one or more *simple,* familiar words admitting of but *one* spelling. A word such as REINFORCEMENT is inadvisable because the spelling REENFORCEMENT is also admissible. It goes almost without saying the use of words suitable for "spelling bees," even though they may be familiar, everyday words as DEFINITELY, SEPARATELY, REPETITION, etc., is likewise inadvisable.

(3) It should contain as many different letters as possible, in no systematic sequence. Words with several repeated letters, such as ELEMENT, BANANA, MISSISSIPPI, etc., form poor key words.

(4) It should present no associations with the special situation in which it is used, so as not to be easily guessed by the enemy. For example, to use personal or geographic names associated with a region in the theater of operations is bad practice. The key word GETTYSBURG employed in a cryptogram originating in the vicinity of Gettysburg would be bad practice. Or to use for this purpose words of common military usage, such as BATTALION, REGIMENT, ARTILLERY, SIGNAL CORPS, MACHINE GUN, etc., is likewise bad practice.

e. It is convenient to designate key text in letters as a *literal key*. As noted, a literal key may consist of a single letter, a single word, a phrase, a sentence, whole paragraph, or even a book. The method of deriving a numerical key from a literal key given in b above is only one of a number of methods, but it is the most commonly employed. It is also subject to variation in detail. But, so far as the cryptanalyst is concerned, just how the numerical key is derived from a specific literal key is usually of interest to him only if this knowledge will assist in subsequent solutions

25

of cryptograms prepared according to the same basic system. Often the cryptanalyst is wholly unconcerned as to whether a literal or a numerical key has been used in connection with cryptographing of the messages, and he may frequently be unaware of the fact that a literal key has been used as the basis for deriving a numerical key.

Section II. COLUMNAR TRANSPOSITION METHODS

27. Columnar Transposition with Completely Filled Rectangles

a. One of the most common types of transposition involving the use of a key word or a derived numerical key is that known as *keyed* or *variable-key columnar transposition*. In this type the letters are usually written in a geometric design, most often a rectangle, by inscribing them in the ordinary manner, that is, in horizontal lines from left to right and from the top downwards, and then the letters are transcribed by "reading" the columns in the sequence determined by the numerical key. If the text does not contain a sufficient number of letters to fill the last line completely, as many nulls as are necessary to do so are added at the end. Figure 5 is an example of cryptographing by this method.

Key word: 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

Note. The letters D and N in the final two cells are nulls, inserted to complete the rectangle.

Cryptogram:

PASAN DDOTE TCPAE CFBON OROOD IATRI CTOOY
TOOAM SDLNN LMTN

Figure 5.

b. To decryptograph such a cryptogram, a rectangle with the proper number of cells, determined by the length of the message and the length of the key, must first be prepared. In the foregoing example, since the cipher text consists of 49 letters and the key consists of 7 letters or num-

Cryptogram:

PASAN DDOTE TCPAE CFBON OROOD IATRI CTOOY TOOAM
SDLNN LMTN

4 – 3 – 1 – 2 – 5 – 6 – 7   **4 – 3 – 1 – 2 – 5 – 6 – 7**

													P					
													A					
													S					
													A					
													N					
													D					
													D					

                   (a)   (b)

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*

(c)

*The letters D and N are recognized as nulls.

Figure 6.

27

bers, the rectangle shown in (a) of figure 6 is prepared and then the columns (of cells) are filled in numerical order. An early stage in the decryptographing is represented in (b) of figure 6. It is only after the process has been finished that the complete message reappears, as shown in (c) of figure 6.

c. The method indicated above may vary considerably by changing (1) the key word, (2) the route followed in inscribing the letters of the plain text, and (3) the route followed in transcribing them to form the cipher text. A change in key daily, or oftener, is possible; or, by drawing up a whole list of daily keys for a given period, automatic change in key can be provided for without indicating in the cryptograms the applicable key. It is also possible to prepare a long list of suitable keys and to designate each key by an *indicator* inserted in the cryptogram in a pre-arranged position. Indicators may be words, numbers, groups of letters, or single letters. For example, each key in a list of 500 may be indicated by a single pair of letters inserted at the beginning, at the end, or at any prearranged position of the cryptogram. This procedure has a disadvantage, however: if an error occurs at the particular position of the crypto-gram containing the indicator, the decryptographing is made difficult if not impossible. For this reason indicators, if used, are often inserted in at least two positions in the cryptogram, usually at or near the beginning and end.

d. The letters of the plain text may be inscribed in the rectangle according to any one of the routes indicated in figure 1. If the tran-scribing process is accomplished by reading whole columns or whole rows, according to a prearranged plan which follows a route perpendicu-lar to the inscribing route (except in the case of spiral inscription), the decryptographing process is simple. Only certain of the simpler combina-tions of inscription and transcription are suitable for military use, the most practicable being those illustrated in figures 5 and 6.

28. Columnar Transposition with Incompletely Filled Rectangles

a. The degree of cryptographic security of columnar transposition is much increased if the rectangle is *not completely filled*. It is impossible to go into the reasons for this increased security without demonstrating solutions; suffice it to say that the solution will be more difficult than would be suspected if one or more cells are vacant in the last row of the rectangle. An example of cryptographing and decryptographing is shown in figure 7.

b. To decryptograph such a cryptogram one must first count the number of letters in the text and then outline on cross-section paper a rectangle which will exactly contain the message, crossing off the cells which must remain vacant. In the foregoing example, the text contains 30 letters and, since the key contains 7 letters, the outlined rectangle is as

shown in figure 8 of (a). From the complete rectangle $7 \times 5 = 35$ cells, 5 cells must remain vacant at the end.

c. The cipher text is then inserted in key-number order, the result of inserting the first two groups of the text being shown in (b), figure 8. It is only after the process has been finished that the complete message becomes apparent.

Message:

REQUEST IMMEDIATE REENFORCEMENTS

Key word: 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	E	N	F
O	R	C	E	M	E	N
T	S					

Cryptogram:

SINEU EEEQM RCRIT OTEME RSTAF NEDEM

Figure 7.

Cryptogram:

SINEU EEEQM RCRIT OTEME RSTAF NEDEM

4 – 5 – 3 – 2 – 7 – 1 – 6   4 – 5 – 3 – 2 – 7 – 1 – 6

(a)   (b)

Figure 8.

29. Modification of Columnar Method

A variation of the columnar procedure, but one that produces exactly the same results, may be found useful. First, write the message in groups corresponding to the length of the key. Thus, using the same key and message as in paragraph 28, the following is obtained:

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
R E Q U E S T	I M M E D I A	T E R E E N F	O R C E M E

4-5
T S

The letters are then taken from the groups and are transcribed in groups of five, all letters marked 1 being taken first, then all those marked 2, and so on. Thus, the first two cipher text groups are SINEU EEEQM, and the complete text is identical with that produced in figure 7.

30. Addition of Nulls to Complete a Final Group

The example given in the preceding case happened to contain 30 letters, a number that is an exact multiple of five. Thus, the final group in the cryptogram automatically became a complete group. For accuracy, the final group of every message should be complete; therefore, if the number of letters in the text of a message is not a multiple of five, it should be made so by the addition of nulls, *before* the transposition process is applied (see par. 23*b*).

Section III. MISCELLANEOUS TRANSPOSITION METHODS

31. Transposition Systems Employing Special Designs

a. Triangles, trapezoids, and other polygons are among the many designs used to produce transposition ciphers. Most of them, however, are impractical for wide military use but are used occasionally by secret agents.

b. A grille is a common transposition device of some practical importance. There are several types and one of the most common is that known as the *rotating* grille. It is usually made of a square sheet of cross-section paper from which cells have been cut in definite but apparently irregular positions. The grille is superimposed on another sheet of cross-section paper of the same dimensions and the letters of the message are written in the cells exposed by the perforations. Usually the grille is then given a 90° turn clockwise or counterclockwise, as agreed, and the fresh cells exposed by the perforations are filled with the next few letters of the text. If the grille has been prepared properly it is possible to give it four turns of 90° each, at the end of which all the cells on the under sheet of cross-section paper are occupied by letters. The grille is then removed and the letters of the sheet underneath it are transcribed in accordance with some prearranged route to form the cipher text. Natur-

ally, the correspondents must have identical grilles and every step must be definitely prearranged. Although it is possible to construct grilles with many different arrangements of perforations, the necessity for carrying the device on the person, and the many agreements and understandings necessary for its successful operation make the method hardly suitable for field military use. Furthermore, practical difficulties connected with the preparation and distribution of many grilles would make it almost inevitable that several messages would be enciphered by the same grille. The degree of cryptographic security afforded by them is not so great as may be suspected; sometimes single messages of fair length may be solved.

32. Polyliteral and Word Transposition

a. Thus far only individual letters, as units for the transposition process have been discussed. It is possible to use pairs of letters, sets of three or more letters, or entire words as units; procedures are the same in monoliteral and polyliteral transpositions. Sometimes more complicated routes may be followed in transposition; for example, a route may be a prearranged succession of moves made by a knight in chess. It is usually necessary to have at hand a printed form showing the complete route, and this makes these methods impractical for field use. They may, however, be used in special cases.

b. The cipher system used by the Federal Army in the Civil War represents a good example of word transposition. In the earliest form in which this cipher was used by the Federals only one route was used, which consisted in writing the text in six columns, going up the sixth, down the first, up the fifth, down the second, up the fourth, and down the third. Arbitrary words were substituted for proper names, nulls were introduced at regular positions, and words even often misspelled for further obscurity. For example, the word "operation" was often spelled as two words: "opera," and "shun." Later, many additional routes were provided, relatively long lists of arbitrary equivalents for names, numbers, dates, common military terms, etc., were added, and the whole system was made considerably more complicated. While the security afforded by this system was probably ample for those days, it would hardly be sufficient today to permit its use even in cases where a delay of only a few hours is required. Furthermore, if long lists of arbitrary equivalents must be handled, the system presents all the disadvantages of a poor cipher system with but few of the advantages offered by a good code system.

33. Single and Double Transposition Methods

In single transposition methods the letters go through only one transposition from plain text to cipher text. It is possible to take the letters

resulting from a first transposition and apply a second transposition to them; cryptograms so prepared often present a very great degree of security. Triple and quadruple transposition is possible but wholly impracticable for common use. Only a very limited number of double transposition methods are practicable for military use, but the degree of security afforded by certain of them is much greater than that afforded by certain much more complicated substitution methods.

34. Factors Concerning Use of Transposition Systems

a. The transposition methods described above provide a wide range of cryptographic security; in some there is very little security, in others there is a great deal. All transposition systems usually present important advantages in speed and simplicity. These advantages have led to attempts to increase security in some manner or other; double transposition schemes, rotating grilles, and other more complicated methods have consequently been developed. In only certain types are written memoranda or devices required. Very often the entire cryptographing process in even very complex methods may be easily memorized by persons of very good intelligence, such as secret agents. For these reasons transposition systems are often useful in espionage and counterespionage activities.

b. But transposition ciphers for military usage present three very serious disadvantages. In the first place, the methods are such that they do not allow any latitude for errors in handling. Often if a single letter is omitted or added, as not infrequently happens in telegraphic transmission, the whole message becomes difficult if not impossible to decryptograph. In the second place, if two or more messages prepared in the same key and *containing exactly the same number of letters* are available for study, no matter how complicated the method employed, the cryptograms can be solved, and the key recovered, and applied to other cryptograms in the same key but with different numbers of letters. In military cryptography it is not unusual, in cases of heavy traffic, to have as many as 100 or 200 messages transmitted on the same day, all in the same key. Control from a central headquarters of the exact message length would obviously be impossible. The chances, therefore, that the enemy may actually intercept and find several messages of identical length are not negligible. Thus, a transposition method presenting an extremely high degree of cryptographic security when only a few messages are to be cryptographed fails seriously when employed for heavy traffic. Finally, in certain cases, where the double transposition produces a great degree of security, it is almost inevitable that a poorly trained or careless cryptographic clerk will fail to perform both steps correctly. Not only messages prepared by one poor or careless operator, but all other messages, even though correctly prepared, are thus laid open to solution.

CHAPTER 3

ELEMENTARY SUBSTITUTION SYSTEMS

Section I. GENERAL

35. Fundamental Nature of Substitution Methods, Cipher Systems and Code Systems

Methods now to be described differ from those above in that elements or textual units composing the original plain text retain their relative positions, but not their identities, and are replaced by other elements or textual units so that the external form of the writing is cryptographic in nature. For this reason these methods are called *substitution methods*. They may deal with individual letters, pairs of letters, sets of letters in regular groups, syllables, whole words, phrases, and sentences. Substitution methods may accordingly be subdivided into *letter methods, syllable methods,* and *word methods,* as in the case of transposition methods; but such a classification is a rather arbitrary one and is not based on the nature, form, or external appearance of the cryptographic text. For example, a substitution method dealing with single letters of the plain text may not involve their replacement by other single letters. In some cases whole words may be used to replace single letters. Outwardly, such a cryptogram gives the appearance of dealing with words, but its internal nature is quite clear: single-letter substitution has been effected. The classification indicated is, nevertheless, a useful one. When the cryptographic process involves the treatment of individual letters or pairs of letters, and only exceptionally the treatment of syllables or whole words, the method is known as a *substitution cipher system;* and when the process involves the treatment of whole words, phrases, or sentences, and only exceptionally the treatment of individual letters, groups of letters, or syllables, the method is known as a *code system,* because it usually necessitates the use of a *code book.*

36. Nature of Alphabets

a. The simplest kind of substitution cipher is that which is known in literature as Julius Caesar's Cipher, but which, as a matter of fact, was a favorite long before his day. In this cipher each letter of the text of a message is replaced by the letter standing the third to the right of it in the ordinary alphabet; the letter A is replaced by D, the letter B by E, and so on. The word CAB becomes converted into FDE which is cipher.

b. The English language is written by means of 26 simple characters called *letters* which, taken together and considered as a *sequence of symbols,* constitute the *alphabet* of the language. 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. Whereas English words are composite or polysyllabic and may consist of one to eight or more syllables, Chinese words are all monosyllables and each monosyllable is a word. Written languages of the majority of other civilized peoples of today are, however, alphabetic and polysyllabic in construction, so that principles discussed here apply to all of them.

c. The letters composing the English alphabet used today are the results of a long period of evolution, the complete history of which may never fully be known. They are conventional symbols representing *elementary sounds,* and any other simple symbols, so long as the sounds which they represent are agreed upon by those concerned, will serve the purpose equally well. If taught from early childhood that the symbols $, *, and @ represent the sounds "Ay," "Bee," and "See," respectively, the combination @$* would still be pronounced CAB, and would, of course, have exactly the same meaning as before; or suppose that two persons have agreed to change the sound values of the letters, F, G, and H, and after long practice have become accustomed to pronouncing them as "Ay," "Bee," and "See," respectively. They would then write the "word" HFG, pronounce it CAB, and see nothing strange whatever in the matter. But to others not party to their arrangements HFG constitutes cipher. The combination of sounds called for by this combination of symbols is perfectly intelligible to the two who have adopted the new sound values for those symbols and therefore pronounce HFG as CAB, but HFG is utterly unpronounceable and wholly unintelligible to others who are reading it according to their own long established sound-symbol basis. It would be stated that there is no such word as HFG, which would mean merely that the particular combination of sounds represented by this combination of letters has not been adopted by convention to represent a thing or an idea in the English language. Thus it is seen that, in order for the written words of a language to be pronounceable and intelligible to all who speak that language, it is necessary, first, that the sound values of the letters or symbols be universally understood and agreed upon and, secondly, that the particular combination of sounds denoted by the letters should have been adopted to represent a thing or an idea. Spoken plain language consists of vocables; that is, combinations and permutations of elementary speech-sounds which have by long usage come to be adopted and recognized as representing definite things and ideas. Written plain language consists of *words;* that is, combinations and permutations of simple symbols, called letters, which represent visually and call forth vocally the elementary speech-sounds of which the spoken language is composed.

34

d. It is clear also that in order to write a polysyllabic language with facility it is necessary to establish and to maintain by common agreement or convention, equivalency between *two* sets of elements, first, a set of elementary sounds and, second, a set of elementary symbols to represent the sounds. When this is done the result is what is called an *alphabet,* a word derived from the names of the first two letters of the Greek alphabet, "alpha" and "beta."

e. Theoretically, in an ideal alphabet each symbol or letter would denote only one elementary sound, and each elementary sound would invariably be represented by the same symbol. But such an alphabet would be far too difficult for the average person to use. It has been conservatively estimated that a minimum of 100 characters would be necessary for English alone. Attempts toward producing and introducing into usage a practical, scientific alphabet have been made, one being that of the Simplified Spelling Board in 1928, which advocated a revised alphabet of 42 characters. Were such an alphabet adopted into current usage, in books, letters, telegrams, etc., the flexibility of cryptographic systems would be infinitely extended and the difficulties set in the path of the enemy cryptanalysts vastly increased. The chances for its adoption in the near future are, however, quite small. Because of the continually changing nature of every living language, it is doubtful whether an original perfect alphabet could, over any long period of time, remain so and serve to indicate with great precision the exact sounds which it was originally designed to represent.

37. Normal Alphabets and Cipher Alphabets

a. In the study of cryptography the dual nature of the alphabet becomes apparent. It consists of two parts or components, (1) an arbitrarily arranged sequence of symbols.

b. The *normal alphabet* for any language is one in which these two components are the ordinary sequences that have been definitely fixed by long usage or convention. The dual nature of our normal or everyday alphabet is often lost sight of. When we write A, B, C, . . . we really mean:

Sequence of sounds: "Ay" "Bee" "See" . . . .
Sequence of symbols: A B C . . . .

Normal alphabets of different languages vary considerably in the number of characters composing them and the arrangement or sequence of the characters. The English, Dutch, and German alphabets each have 26, the French 25, the Italian 21, Spanish 27 (including the digraphs *ch* and *ll*), Russian 31. The Japanese language has a syllabary consisting of 72 syllabic sounds, to express which 48 characters are employed.

c. A *cipher alphabet* or a *substitution alphabet,* as it is sometimes called, is one in which the elementary speech-sounds are represented by

characters other than those representing them in the normal alphabet. These characters may be letters, figures, signs, symbols, or combinations of them.

d. A more technical definition of a familiar cipher may now be given: When the plain text of a message is converted into encrypted text by the use of one or more cipher alphabets, the resultant cryptogram constitutes a *substitution cipher.*

38. Two Components of an Alphabet

It is convenient to designate that component of a cipher alphabet constituting the sequence of speech-sounds the *plain component,* and the component constituting the sequence of symbols the *cipher component.* If the plain component is omitted in a cipher alphabet, the latter is understood to be the normal sequence. For brevity and clarity, a letter of the plain text, or of the plain component of a cipher alphabet, is designated by suffixing a small letter "p" to it: A_p means A of the plain text, or of the plain component of a cipher alphabet. Similarly, a letter of the cipher text, or of the cipher component of a cipher alphabet, will be designated by suffixing a small letter "c" to it: X_c means X of the cipher text, or of the cipher component of a cipher alphabet. The expression $A_p = X_c$ means that A of the plain text, or A of the plain component of a cipher alphabet, is represented by X in the cipher text, or by X in the cipher component of a cipher alphabet.

39. Standard and Mixed Cipher Alphabets

In the arrangement or sequence of letters forming its cipher component, cipher alphabets are of two kinds:

a. Standard cipher alphabets, in which the sequence of letters in the cipher component is the same as the normal, but reversed in direction or shifted from its normal point of coincidence with the plain component.

b. Mixed cipher alphabets, in which the sequence of letters or characters in the cipher component is no longer the same as the normal in its entirety.

40. Enciphering and Deciphering Alphabets

All cipher alphabets may be classified on the basis of their arrangement as *enciphering* or *deciphering* alphabets. An enciphering alphabet is one in which the sequence of letters in the plain component coincides with the normal sequence, and is arranged in that manner for convenience in encipherment. In a deciphering alphabet the sequence of letters in the cipher component coincides with the normal, for convenience in deciphering. For example, in figure 9, (a) shows a mixed cipher alphabet arranged as an enciphering alphabet; (b) shows the corresponding

deciphering alphabet. An enciphering alphabet and its corresponding alphabet present a *verse and inverse* relationship to each other. To invert a deciphering alphabet is to write the corresponding enciphering alphabet; to invert an enciphering alphabet is to write the corresponding deciphering alphabet.

Enciphering Alphabet

(a) Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
     Cipher: JKQVXZWESTRNUIOLGAPHCMYBDF

Deciphering Alphabet

(b) Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ
     Plain: RXUYHZQTNABPVLOSCKIJMDGEWF

Figure 9.

Section II. MONOALPHABETIC SUBSTITUTION SYSTEMS

41. Single-Alphabet Substitution

If a message is enciphered, letter-for-letter, by using one cipher alphabet which has been drawn up for the purpose, the resulting cryptogram is said to be enciphered by a single alphabet and to be a single-alphabet, or *monoalphabetic*, substitution cipher. More complex ciphers may use several alphabets in the enciphering of a single message. When two or more cipher alphabets are used, the resulting cryptogram is said to be a *polyalphabetic* cipher.

42. Standard Alphabet Ciphers

a. Standard cipher alphabets are of two sorts:

(1) *Direct standard,* in which cipher component is the normal sequence but shifted to the right or left of its point of coincidence in the normal alphabet. Example:

$\longrightarrow$

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: QRSTUVWXYZABCDEFGHIJKLMNOP

$\longrightarrow$

It is obvious that the cipher component can be applied to the plain component at any one of 26 points of coincidence, but since the alphabet that results from one of these applications coincides exactly with the normal alphabet, a series of only 25 (direct standard) cipher alphabets results from the shifting of the cipher component.

(2) *Reversed standard,* in which the cipher component is also the normal sequence but runs in the opposite direction from the normal. Example:

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: QPONMLKJIHGFEDCBAZYXWVUTSR

Here the cipher component can be applied to the plain component at any of 26 points of coincidence, each yielding a different cipher alphabet. There is in this case, therefore, a series of 26 (reversed standard) cipher alphabets.

b. It is often convenient to refer to or designate one of a series of cipher alphabets without ambiguity or circumlocution. The usual method is to indicate the particular alphabet to which reference is made by citing a pair of equivalents in that alphabet. For example, the reversed alphabet above, one of a series of 26 related alphabets, may be designated as that in which $L_p = F_c$ or $W_p = U_c$. But the most common basis of reference is the letter which represents the first or initial letter of the plain component, usually A_p. Thus, the key for the cipher alphabet just referred to, as well as that preceding it, is $A_p = Q_c$, and it is said that the key letter for the cipher alphabet is Q_c.

43. Reciprocal Alphabets

a. The cipher alphabet in paragraph 42a (2) is also a *reciprocal alphabet;* that is, the equivalents show reciprocity and are reversible or reciprocal in pairs. For example, in the alphabet referred to, $A_p = Q_c$ and $Q_p = A_c$; $B_p = P_c$ *and* $P_p = B_c$, etc. The reciprocity exists throughout the alphabet and is a result of the method by which it was formed.

b. A series of related reciprocal alphabets may be derived by juxtaposing at all possible points of coincidence two components which are identical but progress in opposite directions. This holds regardless of whether the components are composed of an even or an odd number of elements. The reciprocal alphabet (par. 42a (2)) is one of such a series of 26 alphabets.

c. A single or isolated reciprocal alphabet may be produced in one of two ways:

(1) By constructing a complete reciprocal alphabet by arbitrary or random assignments of values in pairs. That is, if A_p is made K_c, then K_p is made A_c; if B_p is made R_c, then R_p is made B_c, and so on. If the two components thus constructed are slid against each other no additional reciprocal alphabets will be produced.

(2) By juxtaposing a sequence comprising an *even* number of elements against the same sequence shifted exactly half way to the right (or left), as seen below;

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

d. A reciprocal alphabet is an inverse alphabet, since it may serve either as an enciphering or deciphering alphabet.

44. Procedure in Encipherment and Decipherment

a. When a message is enciphered monoalphabetically, that is, by means of a single cipher alphabet, letters of the text are replaced by the equivalents in the cipher alphabet selected by prearrangement. Example:

Message: THREE MACHINE GUNS CAPTURED.
Enciphering Alphabet: Reversed Standard, $A_p = D_c$
Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: DCBAZYXWVUTSRQPONMLKJIHGFE
Letter-for-letter encipherment:

THREE MACHINE GUNS CAPTURED
KWMZZ RDBWVQZ XJQL BDOKJMZA

The cipher text is then grouped in fives and the indicator letter D[a] inserted as the initial letter of the first group (or any other prearranged group).

Cryptogram:

DKWMZ ZRDBW VQZXJ QLBDO KJMZA

Figure 10.

b. The procedure in decipherment is merely the reverse of that in encipherment. The initial letter of the message, D, indicates $A_p = D_c$ in the cipher alphabet. The deciphering alphabet is therefore as follows:

Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Plain: DCBAZYXWVUTSRQPONMLKJIHGFE
The message deciphers thus:
Cipher: (D) KWMZ ZRDBW VQZXJ QLBDO KJMZA
Plain: THRE EMACH INEGU NSCAP TURED

The deciphering clerk rewrites the text in word lengths:

THREE MACHINE GUNS CAPTURED

c. When a mixed alphabet is used, the enciphering and deciphering processes are the same as those described under *a* and *b* above. For speed in cryptographing, the cipher alphabet is prepared in the form of an enciphering alphabet, and for speed in decryptographing, in the form of a deciphering alphabet.

---

[a] If this or any such similar convention has been agreed upon by the correspondents.

Section III.   TYPES OF MIXED CIPHER ALPHABETS

45. Systematically Mixed Cipher Alphabets

It will be recalled that in a mixed cipher alphabet the sequence of letters or characters in the cipher component does not correspond to the normal sequence. There are various methods of mixing up the letters of the cipher component, and those which are based upon a scheme that is systematic in its nature are very useful because they make possible the derivation of one or more mixed sequences from any easily remembered word or phrase, and thus do not necessitate the carrying of written memoranda. They are called *systematically mixed cipher alphabets*.

46. Key-word Mixed Alphabets

a. One of the simplest types of systematically mixed cipher alphabets is the *key-word mixed alphabet*. The cipher alphabet consists of a key word or phrase (with repeated letters, if present, omitted after their first occurrence), followed by the letters of the alphabet in their normal sequence (with letters already occurring in the key, of course, omitted). Example, with GOVERNMENT the key word:

Enciphering alphabet.... $\begin{cases}\text{Plain:} & \text{ABCDEFGHIJKLMNOPQRTSUVWXYZ} \\ \text{Cipher:} & \text{GOVERNMTABCDFHIJKLPQSUWXYZ}\end{cases}$

b. Mixed alphabets formed by including all repeated letters of the key word or key phrase were common in Edgar Allan Poe's day but are impractical because they make decipherment difficult.

Enciphering alphabet.... $\begin{cases}\text{Plain:} & \text{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \text{Cipher:} & \text{NOWISTHETIMEFORALLGOODMENT}\end{cases}$

Deciphering alphabet....
$\begin{cases}\text{Cipher:} & \text{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \text{Plain:} & \begin{matrix}\text{P} & \text{VHMSGD} & \text{QKAB} & \text{OEF} & \text{C} \\ & \text{L} & \text{J} & \text{RWYN} & \text{I} \\ & \text{X} & & \text{T} & \text{Z} \\ & & & \text{U} & \end{matrix}\end{cases}$

The average cipher clerk would have considerable difficulty in decryptographing a cipher group such as TOOET, each letter of which has three or more equivalents, and from which the plain-text words (N) INTH, ..FT THI (S), IT THI ... , etc., can be formed on decipherment.

c. An example of a key-word mixed alphabet is shown in figure 9, where, in its enciphering form, the cipher component presents to the experienced eye the skeleton of the key upon which the alphabet is based: WESTERN UNION TELEGRAPH COMPANY. Any easily remembered word, phrase, or sentence may be used. The starting point of the sequence, when used as a cipher component, may be indicated in the usual manner. For example, in the alphabet referred to, the

alphabet key is $A_p = J_c$. Two or more correspondents using the pre-arranged key, WESTERN UNION TELEGRAPH COMPANY, would obtain the same disarranged sequence; when this sequence is to form the cipher component of a cipher alphabet, the prearranged key letter $A_p = J_c$ would result in giving each correspondent exactly the same cipher alphabet. The key words or phrases need not consist of any definite number of letters, but it is advisable to use for keys such words or phrases as will most thoroughly disarrange the normal sequence. (See, in this connection, par. 26.) A key-word mixed alphabet will manifest the key word or parts of it only when the alphabet is in the form of an enciphering alphabet. Note that alphabet (b) of figure 9 no longer gives any external evidence of having been derived from the phrase WESTERN UNION TELEGRAPH COMPANY.

47. Transposition-mixed Alphabets

a. It is possible to disarrange the sequence even more thoroughly by applying a simple method of transposition to the key-word sequence as if it were a message. An example is illustrated in figure 11.
Key word:

<div align="center">

TELPHONY

</div>

(a) Simple columnar transposition:

<div align="center">

TELPHONY
ABCDFGIJ
KMQRSUVW
XZ

</div>

Mixed sequence:

<div align="center">

TAKXEBMZLCQPDRHFSOGUNIVYJW

</div>

(b) Numerical key, columnar transposition:

<div align="center">

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

</div>

Mixed sequence:

<div align="center">

EBMZHFSLCQNIVOGUPDRTAKXYJW

</div>

<div align="center">

Figure 11.

</div>

b. The last two systematically mixed cipher alphabets are *transposition-mixed alphabets*. Almost any of the methods of transposition described in sections IV and V of this chapter may be applied to them.

48. Decimation Method of Forming Mixed Alphabets

Another simple method of forming a mixed alphabet is the *decimation method*. In this method, letters in the normal alphabet, or in a key-word mixed alphabet, are "counted off" according to a selected odd interval. As each letter is decimated—that is, eliminated from the basic alphabet by counting off—it is entered in a separate list to form the sequence of the mixed alphabet. For example, to form a mixed alphabet by this method from an alphabet based on the key phrase SING A SONG OF SIX PENCE with 7 the interval selected, proceed as follows:

a. Key-word (or basic) alphabet:

SINGAOFXPECBDHJKLMQRTUVWYZ

b. When the letters are counted off by 7's from left to right, F will be the first letter arrived at, H the second, T the third:

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

Fig. B

These letters are entered in a separate list (F first, H second, T third, etc.) and eliminated from the key-word alphabet.

c. When the end of the key-word alphabet is reached, return to the beginning, skipping the letters already eliminated:

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

Fig. C

d. Mixed alphabet.

FHTIEMZPQNDWCVBSLXAGOKYJRU

49. Random-Mixed Alphabets

Practical considerations, of course, set a limit to the complexities that may be introduced in constructing systematically mixed alphabets. Beyond a certain point there is no object in further mixing. The greatest amount of mixing by systematic processes will give no more security than that resulting from mixing the alphabet by random selection, such as by putting the 26 letters in a box, thoroughly shaking them up, and then drawing the letters out one at a time. Whenever the laws of chance operate in the construction of a mixed alphabet, a thorough disarrangement is bound to be produced. Random-mixed alphabets give more cryptographic security than do the less complicated systematically mixed alphabets because they afford no clues to positions of letters, given the

positions of a few of them. Their chief disadvantage is that they must be reduced to writing, since they cannot readily be remembered, nor can they be reproduced at will from an easily remembered key word.

50. Number of Single Alphabets Available from a Basic Alphabet

It is obvious that the cipher component of a cipher alphabet may be shifted or slid against the plain component at 26 points of contact so as to produce a series of different enciphering alphabets. For example, the mixed sequences given under (b) of figure 11, when used as a cipher component, yields the following two of a series of 26 cipher alphabets:

Enciphering Alphabets

(1) Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
    Cipher: EBMZHFSLCQNIVOGUPDRTAKXYJW

(2) Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
    Cipher: WEBMZHFSLCQNIVOGUPDRTAKXYJ

The message DAILY REPORT NOT RECEIVED YET would be enciphered by the first alphabet as:

Plain: DAILY REPOR TNOTR ECEIV EDYET
Cipher: ZECIJ DHUGD TOGTD HMHCK HZJHT

and by the second alphabet as:

Plain: DAILY REPOR TNOTR ECEIV EDYET
Cipher: MWLNY PZGOP RVORP ZBZLA ZMYZR

Externally the two cryptograms seem different except in length. The two enciphering alphabets present the same sequence in the cipher component, but this entirely disappears in the corresponding deciphering alphabets, which are as follows:

Deciphering Alphabets

(1) Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ
    Plain: UBIRAFOELYVHCKNQJSGTPMZWXD

(2) Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ
    Plain: VCJSBGPFMZWIDLORKTHUQNAXYE

It is possible to write the same message in 25 different external forms, each using a different cipher alphabet of a series derivable from a basic sequence. The basic sequence or alphabet in such a case is often called a *primary sequence* or a *primary alphabet;* derived alphabets are called *secondary alphabets.* In producing secondary alphabets the basic sequence must be juxtaposed and slid against itself, or against the normal sequence, or against another mixed sequence. In all cases secondary alphabets form a series of alphabets that are interrelated and

43

that either directly or indirectly manifest relationships which are important from a cryptanalytic point of view. It should be clear now that by means of a single, prearranged, secret word it is possible for two correspondents to send a whole set of messages all in different mixed alphabet, or to use a different alphabet for each of 26 consecutive days.

51. Miscellaneous Types of Cipher Alphabets

a. The cipher alphabets shown thus far have used only letters, but alphabets in which the cipher component consists of figures, or groups of figures, are not uncommon in military cryptography. Cipher alphabets using signs and symbols are not suitable for military cryptography because they can neither be telegraphed nor telephoned with any degree of accuracy, speed, or facility. Since there are but ten digits it is obvious that, in order to represent a complete alphabet in figure ciphers, combinations of at least two digits are necessary. The simplest kind of such an alphabet is that in which $A_p = 01$, $B_p = 02$, . . . $Z_p = 26$.

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

Figure 12.

b. Instead of a simple alphabet of the preceding type, it is possible to use a simple diagram of the type shown in figure 12. Here the digits at the side and top of the rectangle are used to designate, according to the coordinate system, the cell occupied by each letter and punctuation mark within the rectangle. When used for such purposes, the figures (or letters) constituting coordinate elements are referred to as *row and column indicators*. It is usually necessary to agree beforehand upon which indicator will be given as the first half of the equivalent for a letter, the row indicator or the column indicator, in order to avoid ambiguity or error. In all of the systems to be described here, the row indicator will always form the first half of an equivalent. Accordingly in figure 12, the letter $A_p = 11$, $B_p = 12$, and so forth.

c. A variation of the foregoing diagram is exemplified in figure 13. Here, letters of the alphabet are inserted in the 25 cells of a large square, I and J being written together in one cell. Then a key word of five letters is applied to the top of the large square and the same or a different key word is applied to the side of the square to form column and row indicators. In figure 13, for example, $S_p = TI$; $W_p = EH$; etc.

44

(2)

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

Figure 13.

The message RAIDERS HAVE GONE is enciphered thus:

```
Plain:    R   A   I   D   E   R   S   H   A   V   E   G   O   N   E
Cipher:  TH  WW  HT  WT  WE  TH  TI  HI  WW  EW  WE  HH  IT  II  WE
```

The cryptogram is then transmitted in groups of five letters:

Cryptogram: THWWH TWTWE THTIH IWWEW WEHHI TIIWE

d. In these two systems just described,

(1) The letters of the alphabet within the square or rectangle may be fixed in a mixed sequence, either systematically or random-mixed sequences being possible.

(2) The column and row indicators may be the same, or different; when letters are used they may form a key word or they may not; the key words, if formed, may be identical or nonidentical.

e. When letters are used as column and row indicators, they may be selected so as to result in producing cipher text that resembles "made-up words," that is, words composed of regular alternations of vowels and consonants. For example, if in figure 13 the row indicators consisted of the vowels A E I O U in this sequence from the top down, and the column indicators consisted of the consonants B C D F G in this sequence from left to right, the word RAIDS would be enciphered as OCABE FAFOD, which very closely resembles code of the type formerly called artificial code language. Such a system may be called a *false,* or *pseudo-code* system.[7]

---

[7] Prior to 1934, International Telegraph Regulations required code words of five letters to contain at least one vowel and code words of ten letters to contain at least three vowels. The Madrid Conference held in 1932 amended these regulations to permit the use of code groups containing any combination of letters. These unrestricted code groups were authorized for use after 1 January 1934.

45

Section IV. MONOALPHABETIC SUBSTITUTION
WITH VARIANTS

52. Purpose of Providing Variant Values

The individual letters composing ordinary intelligible plain text are used with varying frequencies; some, such as (in English) E, T, R, I, and N, are used much more often than others, such as J, K, Q, X, and Z. In fact, each letter has a *characteristic frequency* by means of which definite clues are afforded in the solution of simple substitution ciphers. This has led cryptographers to devise methods for disguising, suppressing, or eliminating the characteristic frequencies manifested by the letters of cryptograms produced by simple monoalphabetic substitution. One such method is that in which the letters of the plain component of the cipher alphabet are assigned two or more equivalents in the cipher component and they are, for this reason, called *variant values*. In some cases the letters of the plain component receive numbers of variant values, or variants, in proportion to their normal frequencies; in other cases, all the letters receive equal numbers of variant values, determined by the total number available.

53. Figure Ciphers with Variant Values

a. The use of figures in pairs as substitution equivalents makes available a total of 100 different pairs, those from 00 to 99. They may all be used in a complete system, or only certain ones may be selected, as prearranged.

b. One of the most common varieties of ciphers using all the pairs of digits is that in which the alphabet is reduced to 25 letters (by making I and J interchangeable or by eliminating a letter such as Q), and each letter is assigned four values which may be used at will. The assignment of values may be based upon a key word of four letters, each of which designates the starting points of a *normal sequence* of 25 numbers. An example is shown in figure 14, wherein the key word is TRIP. This means that in the first set of numbers, 01 to 25, the first number, 01, is assigned to the letter T; in the second set, from 26 to 50, the first number, 26, is assigned to the letter R; in the third set, from 51 to 75, the first number, 51, is assigned to the letter I; finally, in the last set, from 76 to 00, the first number, 76, is assigned to the letter P.

The letter A_p may be represented by any one of four equivalents, 08, 35, 68, and 87; the letter B_p by 09, 36, 69, 88; and so on. The equivalent used in any particular instance is selected at random, so that the word CAB may be represented in cipher by any one of a total of 64 combinations, such as 10–08–09, 70–35–09, 37–08–69, etc. In the final cryptogram

the figures may be run together in groups of five. The cipher group 10080, on deciphering, would be split up into 10–08–0.

A—08 35 68 87	I–J—16 43 51 95	S—25 27 60 79
B—09 36 69 88	K—17 44 52 96	T—01 28 61 80
C—10 37 70 89	L—18 45 53 97	U—02 29 62 81
D—11 38 71 90	M—19 46 54 98	V—03 30 63 82
E—12 39 72 91	N—20 47 55 99	W—04 31 64 83
F—13 40 73 92	O—21 48 56 00	X—05 32 65 84
G—14 41 74 93	P—22 49 57 76	Y—06 33 66 85
H—15 42 75 94	Q—23 50 58 77	Z—07 34 67 86
	R—24 26 59 78	

Figure 14.

c. In this case, within each set of 25 the numbers progress serially, each set being treated as a ring or circle. It is of course possible to mix the sequence to destroy this serial progression, thus giving four mixed alphabets which can be used at random.

d. Another variation is to assign each letter a set of numbers in accordance with its relative frequency in ordinary English, so that each of the most frequently used letters such as E, T, R, I, and N will have perhaps seven or eight different equivalents, whereas letters of low frequency such as J, K, Q, X, and Z will each have but one equivalent.

54. Use of Rectangles to Provide Variant Values

a. Instead of drawing up alphabets as in figure 14, it is possible to use the diagram shown in figure 12, but with several variant digits as row indicators instead of a single digit for each row. For example, the row indicators may be of the following arrangements:

1–6–7	1–2–3	1–2–3	5–4–3
2–5–8	4–5–6	8–9–4	6–9–2
3–4–9	7–8–9	7–6–5	7–8–1, etc.

Thus, if the first arrangement is used, A$_p$ would have the equivalents 11, 61, 71; B$_p$, 12, 62, 72; etc. The word RUN might be represented by any one of 27 different combinations, such as 28–31–24, 28–91–54, etc.

b. A variation of the foregoing system is that in which, by use of a diagram of the type shown in figure 13, a number of different letters are applied to each row and column, or 2-figure numbers may be used for this purpose. In this case a series of as many as 50 pairs of digits may be used as row indicators, and another series of 50 pairs as the column indicators.

c. The use of variants lends itself to application in a pseudo-code system such as described in paragraph 51e. It presents many possibilities for

47

variation, with or without key words, with one or more alphabets distributed within the square or rectangle, with alphabets extended to include figures, punctuation signs, common syllables and words, etc. Sometimes pseudo-code is encountered when the groups of a numerical cipher system (or a figure-code system) are converted into letters, in order to make the cryptographic text conform to certain telegraph regulations and thus have the message accorded a more favorable rate of charge (sec. II, ch. 4). Thus, a group such as 0125784256 might be converted into the group BAFOSULAFE. If the conversion table is irregular in its construction and is kept secret, this adds an encipherment step to the system.

55. Disadvantages of Monoalphabetic Substitution with Variants

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 plain text. Furthermore, there is no compensating advantage from the standpoint of cryptographic security. When methods are such that the cipher equivalents are passed through another process which returns the cipher text to a length identical with that of the equivalent plain text, they are usually too complicated, too slow, and too subject to error to be practical. They are often the result of combining substitution and transposition processes in one system. Methods which substitute three or more characters for one letter of the original text are not at all practical for military cryptography.

Section V.   POLYALPHABETIC SUBSTITUTION SYSTEMS

56. Monoalphabetic and Polyalphabetic Substitution

a. In the substitution methods thus far discussed it has been noted that only one cipher alphabet is used in the encipherment of a message, and that as a class they constitute the type of system designated as monoalphabetic substitution. It is true that in certain of the systems monoalphabetic substitution with variant equivalents takes place, there are two or more complete alphabets involved and that these systems may, therefore, with apparently good reason be designated as polyalphabetic substitution. This designation, however, will be seen to be somewhat inaccurate when cases of *true polyalphabetic substitution* come to be studied. The real or essential difference between the two systems may best be made clear by setting forth the primary object in each case.

b. In monoalphabetic substitution with variant values, the object of having different sets of equivalents is to suppress so far as possible by *simple* methods the characteristic frequencies of letters. One such method consists in merely providing one or more different values as cipher

48

equivalents of the same plain-text letter, or a few different values as equivalents of some of the high-frequency letters. Now there are certain conditions inherent in the method itself, conditions which cannot here be indicated, that result in producing in the cryptograms certain definite clues leading to the rapid establishment, in cryptanalysis, of the equivalence of different variant values. Furthermore, in these systems the varying or alternative equivalents for plain-text letters are subject to the free choice and caprice of the encipherer. If he is careful and conscientious in the work he will actually make use of all the variant values afforded by the system; but if he is slip-shod and hurried in his work, he will use the same equivalent repeatedly rather than take pains and time to refer to his charts, tables, or diagrams to find variants. The result is that the cryptograms based upon these methods are open to easy solution, even when the basic methods are such as would make a solution difficult without the interception of carelessly enciphered messages. What is necessary is a system in which there is established a definite procedure for automatically shifting or changing the cipher alphabets employed in the encipherment of a single message; a method which within certain limits is beyond the momentary whims of cipher clerks, and which to a higher degree makes difficult the establishment of the equivalency of different cipher values. These are the objects of true polyalphabetic substitution systems. The number of such systems is large. Therefore, it will be possible to describe only a few of the more common or typical examples of methods practicable for military use.

c. The three methods (a) simple monoalphabetic substitution, (b) monoalphabetic substitution with variants, and (c) true polyalphabetic substitution, are attended by the following consequences in the plain text cipher relationship, a careful study of which will help to understand their similarities and differences:

(1) Encipherment—

In method (a) each plain-text letter is represented by one and always the same cipher equivalent.

In method (b) and method (c), each plain-text letter is represented by two or more different cipher equivalents, but in method (b) the variations are subject only to the whim of the encipherer, whereas in method (c) the identities of the cipher letters are determined by the positions they occupy in the text.

(2) Decipherment—

In method (a) and method (b), each cipher equivalent represents one and always the same plain-text letter.

In method (c) one and the same cipher equivalent represents two or more different plain-text letters, the identities of which are determined by the positions they occupy in the text.

49

57. Example of Polyalphabetic Substitution

a. A simple example may be used to illustrate what is meant by true polyalphabetic substitution. Suppose that two correspondents agree upon a numerical key, for example, 74030274, each digit of which means that the plain-text letter to which the digit applies as a key number is to be replaced by the letter that stands a corresponding number of places to the right of it in the normal alphabet. For example, if R is to be enciphered by key number 7, it is to be replaced by Y. The numerical key is written under the letters of the plain-text letter for letter, and is repeated until the whole text is covered. Let the message be REENFORCE-MENTS BEING RUSHED. The encipherment of a message is shown in figure 15. For convenience in counting forward (to the right) to find cipher equivalents, a normal alphabet is given at the top of the figure.

Normal alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Plain: REENFORCEMENTS BEING RUSHED
Key: 74030274740302 74740 302747
Cipher: YIEQFQYGLQEQTU IIPRG UUOIK
The text is then transmitted in *five-letter groups.*
Cryptogram: YIEQF QYGLQ EQTUI IPRGU UUOIK

Figure 15.

b. To decipher such a cryptogram, the clerk writes the numerical key over the cipher letters and then counts backward (to the left) in the normal alphabet as many places as indicated by the key number standing over each letter. Thus:

Normal alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Key: 74030 27474 03027 47403 02747
Cipher: YIEQF QYGLQ EQTUI IPRGU UUOIK
Plain: REENF ORCEM ENTSB EINGR USHED
Message: REENFORCEMENTS BEING RUSHED

Figure 16.

58. Systematizing the Work

The work of encipherment may be materially shortened by systematizing the procedure. Instead of having to write the key over and over again in order to cover the text completely, the text may be written in sets of letters corresponding in length to the length of the key. Thus the text may be written underneath a single appearance of the key in successive short horizontal lines, leaving space between the lines for the insertion of cipher equivalents, as shown in figure 17a. Instead of enciphering the letters

```
7 4 0 3 0 2 7 4
R E E N F O R C
E M E N T S B E
I N G R U S H E
D
```

Figure 17a.

by individual, repeated countings, two strips of paper bearing normal alphabets may be juxtaposed in the proper relative positions to encipher a whole *column* of letters at one setting of the strips. Thus, for the first column, with the key number 7, the strips are juxtaposed so that the first letter in the column, viz., R (which is to be represented by the seventh letter to the right of it, and is therefore to be enciphered by Y of the lower strip) is directly above Y, as follows:

Plain:
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ

The equivalents for the rest of the letters of the first column may now be rewritten down in their proper places, reference being made to the alphabet strips to see what the cipher letters should be: $E_p = L_c$; $I_p = P_c$; $D_p = K_c$. For the second column the two alphabet strips are in these relative positions:

Plain:
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ

The cipher equivalents for the second column are: $E_p = I_c$; $M_p = Q_c$; $N_p = R_c$. The process is continued in this manner until all the columns have been enciphered, as shown in figure 17b.

```
7 4 0 3 0 2 7 4

R E E N F O R C
Y I E Q F Q Y G

E M E N T S B E
L Q E Q T U I I

I N G R U S H E
P R G U U U O I

D
K
```

Figure 17b.

The cipher text is then transcribed in groups of five letters, reading the successive lines in the normal manner, that is, from left to right and from the top downwards, yielding the groups YIEQF, QYGLQ, etc. It is

51

no more difficult to encipher a message by this systematized procedure than by the longer and slower method of writing the text out in long lines and repeating the key over and over again. What is more important is that the shortened procedure promotes accuracy in encipherment. A few seconds careful checking of the relative positions in which the two alphabet strips are set is all that is required but this checking is very necessary, for if that is wrong all the cipher letters in that column to which this setting applies will be in error.

59. Using Key Words to Indicate Number, Identity, and Sequence of Cipher Alphabets Employed

a. If reference is made to the two settings of alphabet strips in paragraph 58, it will be noted that in the first setting $A_p = H_c$, in the second $A_p = E_c$. If the eight settings of the strips are studied it will be found that the letters which A_p represents successively are H, E, A, D, A, C, H, and E, giving the word HEADACHE. These settings, when first presented in the foregoing description, correspond merely to the numerical key 74030274, but this numerical key is also expressible in terms of letters, which when put together properly spell a word. This is only another way of showing that key words may be employed in this type of substitution as in those previously described. Key words of various lengths and composition may be used, consisting of single words, long phrases, or sentences. In general, the longer the key the greater is the degree of cryptographic security. The method as a whole is often referred to as the *repeating key method*.

b. The number of elements in the key—that is, the number of letters or figures composing it—determines the number of alphabets to be employed. The identity of each element of the key, the specific letter or figure it happens to be, determines specifically which of a set of cipher alphabets pertaining to the whole system will be used. And the specific sequence or relative order of the elements of the key determines specifically the sequence with which the cipher alphabets are employed within the encipherment. The total number of cipher alphabets pertaining to or composing the system may be limited or unlimited. When they are produced as a result of the sliding of two basic or primary alphabets against each other, the number is limited to 26 in the English alphabet.

c. A brief notation for indicating or designating a specific key letter is to suffix the subscript "k" to it, just as the subscripts "p" and "c" are suffixed to letters to indicate letters of the plain text or cipher text, respectively. When the key letter occurs in an equation, it can be enclosed within parentheses to avoid ambiguity. Thus, B_p $(D_k) = E_c$ means that plain-text letter B when enciphered by key letter D (in a certain alphabet system) yields the cipher letter E.

60. Use of Other Types of Alphabets

a. It has been noted that in the case of monoalphabetic ciphers, alphabets of various types may be employed. This is likewise true of polyalphabetic ciphers. Instead of using two alphabet strips bearing the normal alphabetic sequence to determine the cipher equivalent of a letter enciphered by a given key number or key letter, one may use a pair of strips, one of which bears the normal direct, the other the normal reversed sequence. In the former case one is dealing with direct standard, in the latter, with reversed standard alphabets.

b. Polyalphabetic substitution with direct or reversed standard alphabets does not result in nearly so great a degree of cryptographic security as that resulting from the simple artifice of providing mixed alphabets for the strips. All sorts of mixed alphabets may be used. One of the strips may bear the normal direct or reversed sequence; the other a mixed sequence. Both strips may bear identical mixed sequences proceeding in the same direction, or in opposite directions. Finally, both strips may bear different mixed sequences.

c. In all cases, except where reciprocal alphabets are produced, it is essential that the correspondents agree upon the sequence or strip from which the plain and the cipher letters respectively will be taken, that is, it is necessary to indicate which sequence constitutes the plain component, which the cipher component. If this is not done, two correspondents will have difficulty in deciphering one another's messages. Also, as noted above, it is necessary to agree as to which letter the key letter is to be set against. The usual method is to agree that the initial letter of the plain component, usually A_p, will be set opposite the key letter, though other conventions are possible.

d. The sequences on the strips may be permanent or invariable, but naturally the degree of cryptographic security in this case is considerably lower than if they can be changed easily at the will of the correspondents and by prearrangement. It is possible that a secret word may serve as the basis not only for the key for shifting the strips, but also for the mixing of the alphabetic sequences. For example, two correspondents may agree to use the key CENTRAL AMERICA; to use the first part as the basis for constructing the mixed plain component; the second part, for constructing the cipher component; and to use the whole phrase as the key for enciphering the message. All the methods of constructing systematically mixed alphabets as described in section III of this chapter are applicable.

Section VI.   CIPHER DISKS AND SQUARE TABLES

61. Cipher Disks

a. In the foregoing section it was noted that the separate alphabets employed in the encipherment are produced by the use of only two strips of paper bearing the normal alphabet. Such strips are often referred to as *sliding alphabets,* because they can be shifted or slid against each other in any one of 26 points of contact or coincidence. Exactly the same results, so far as cipher equivalents are concerned, can be obtained by the use of other devices. First, there are the so-called cipher wheels or cipher disks in which an alphabet is written on the periphery of a *rotating* disk, the circumference of which is divided into 26 equal segments, and this disk is made to revolve concentrically upon a similar but slightly larger *fixed disk.* Figure 18 shows the now obsolete U. S. Army Cipher Disk, which is of this simple type. Here the alphabetic sequences are printed on glossy celluloid, are permanent, and admit of no variation. The use of unglazed celluloid upon which blank segments appear would permit of writing letters and erasing them as often as desirable. Thus, quick and easy change of alphabets would be possible.
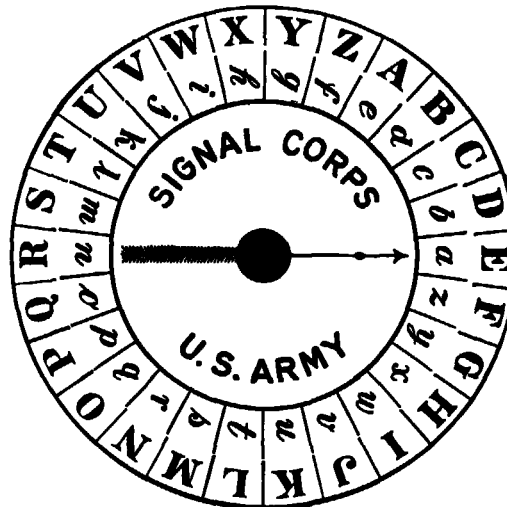
To encipher a message, the key letter or the first letter of the key word or phrase is set opposite "a." Let us assume it to be "E." The cipher letters to be written are those opposite the text letter when "a" on the circle is set opposite "E" on the card. For example, "send powder" would be written "MARBPQIBAN." To use a key word or phrase, each letter is used in turn to encipher one letter only. When the last letter of the key word is used, repeat until all letters of the message are enciphered. Numbers when enciphered with the disk must be spelled out.

Figure 18.

b. The cipher alphabets produced by the cipher disk shown in the figure are merely reversed standard alphabets, the same as are produced by the use of sliding strips of paper, and by the use of certain tables which are discussed below. The method of employing the disk needs no discussion. It may serve in monoalphabetic or polyalphabetic substitution with a key word or key number.

62. Square Tables

a. Tables known in the literature of cryptography under various names, such as "Vigenère Table", "Square Table", "Quadricular Table", "Pythagorean Table", "Cipher Square", "Cipher Chart", etc., are often employed in polyalphabetic substitution. All the results produced by their use can be duplicated by the employment of sliding alphabets or revolving disks. The modern form of the Vigenère Table is shown in figure 19. Such a table may be used in various ways, differing from one another in minor details. The most common method is to consider the top line of the table as containing the plain-text letters, the first column at the left as containing the key letters. Then each successive horizontal line con-

Plain-Text Letter

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

Figure 19. The Vigenère Table.

tains the cipher equivalents for the plain-text sequence ABC ... Z enciphered by the key letter which stands at its left in the first column. Thus, the cipher alphabet corresponding to key letter D is the sequence of letters in the fourth horizontal line under the plain-text line, where $A_p = D_c$, $B_p = E_c$, etc. It will be easy to remember, in using such a table, that the equivalent of a given plain-text letter, T_p, for example, enciphered by a given key letter, O_k, lies at the intersection of the vertical column headed by T, and the horizontal row begun by O. In this case T_p $(O_k) = H_c$. The same result will be found on referring to sliding, direct standard alphabets.

b. Minor modifications of the Vigenère Table are encountered. If the top line is made a reversed normal sequence, leaving the interior of the table unchanged, or if the successive horizontal rows are made to contain the reversed normal sequence, leaving the top row (plain text) unchanged, then the results given by using the table are the same as those given by using the obsolete cipher disk shown in figure 18. Again, the same general results can be obtained by using a set of alphabets in tabular form known under the names of Porta's Table and Napoleon's Table, which is shown in figure 20.

```
AB   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

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

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

              etc.

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

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

Figure 20.

In this table the alphabets are all reciprocal, for example, G_p $(W_k) = V_c$, V_p $(W_k) = G_c$. Reciprocal alphabets when arranged in this form are sometimes called *complementary alphabets*. Note that in each alphabet either of two letters may serve as key letter indifferently: G_p (W_k) or G_p $(X_k) = V_c$.

c. Another modification of the basic table, and one that employs numbers instead of letters as cipher equivalents is shown in figure 21. Since many more than 26 different equivalents are available (100 pairs of digits from 00 to 99, it is possible to insert many plain-text elements in

*	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	1	2	3	4	5	6	7	8	9	*
a	10	11	12	13	14	15	16	17	18	a	19	20	21	22	23	24	25	26	27	a	28	29	30	31	32	33	34	35	a	36	37	38	39	40	41	42	43	44	45	a
b	11	12	13	14	15	16	17	18	19	b	20	21	22	23	24	25	26	27	28	b	29	30	31	32	33	34	35	36	b	37	38	39	40	41	42	43	44	45	10	b
c	12	13	14	15	16	17	18	19	20	c	21	22	23	24	25	26	27	28	29	c	30	31	32	33	34	35	36	37	c	38	39	40	41	42	43	44	45	10	11	c
d	13	14	15	16	17	18	19	20	21	d	22	23	24	25	26	27	28	29	30	d	31	32	33	34	35	36	37	38	d	39	40	41	42	43	44	45	10	11	12	d
e	14	15	16	17	18	19	20	21	22	e	23	24	25	26	27	28	29	30	31	e	32	33	34	35	36	37	38	39	e	40	41	42	43	44	45	10	11	12	13	e
f	15	16	17	18	19	20	21	22	23	f	24	25	26	27	28	29	30	31	32	f	33	34	35	36	37	38	39	40	f	41	42	43	44	45	10	11	12	13	14	f
g	16	17	18	19	20	21	22	23	24	g	25	26	27	28	29	30	31	32	33	g	34	35	36	37	38	39	40	41	g	42	43	44	45	10	11	12	13	14	15	g
h	17	18	19	20	21	22	23	24	25	h	26	27	28	29	30	31	32	33	34	h	35	36	37	38	39	40	41	42	h	43	44	45	10	11	12	13	14	15	16	h
i	18	19	20	21	22	23	24	25	26	i	27	28	29	30	31	32	33	34	35	i	36	37	38	39	40	41	42	43	i	44	45	10	11	12	13	14	15	16	17	i
j	19	20	21	22	23	24	25	26	27	j	28	29	30	31	32	33	34	35	36	j	37	38	39	40	41	42	43	44	j	45	10	11	12	13	14	15	16	17	18	j
k	20	21	22	23	24	25	26	27	28	k	29	30	31	32	33	34	35	36	37	k	38	39	40	41	42	43	44	45	k	10	11	12	13	14	15	16	17	18	19	k
l	21	22	23	24	25	26	27	28	29	l	30	31	32	33	34	35	36	37	38	l	39	40	41	42	43	44	45	10	l	11	12	13	14	15	16	17	18	19	20	l
m	22	23	24	25	26	27	28	29	30	m	31	32	33	34	35	36	37	38	39	m	40	41	42	43	44	45	10	11	m	12	13	14	15	16	17	18	19	20	21	m
n	23	24	25	26	27	28	29	30	31	n	32	33	34	35	36	37	38	39	40	n	41	42	43	44	45	10	11	12	n	13	14	15	16	17	18	19	20	21	22	n
o	24	25	26	27	28	29	30	31	32	n	33	34	35	36	37	38	39	40	41	o	42	43	44	45	10	11	12	13	o	14	15	16	17	18	19	20	21	22	23	o
p	25	26	27	28	29	30	31	32	33	p	34	35	36	37	38	39	40	41	42	p	43	44	45	10	11	12	13	14	p	15	16	17	18	19	20	21	22	23	24	p
q	26	27	28	29	30	31	32	33	34	q	35	36	37	38	39	40	41	42	43	q	44	45	10	11	12	13	14	15	q	16	17	18	19	20	21	22	23	24	25	q
r	27	28	29	30	31	32	33	34	35	r	36	37	38	39	40	41	42	43	44	r	45	10	11	12	13	14	15	16	r	17	18	19	20	21	22	23	24	25	26	r
s	28	29	30	31	32	33	34	35	36	s	37	38	39	40	41	42	43	44	45	s	10	11	12	13	14	15	16	17	s	18	19	20	21	22	23	24	25	26	27	s
t	29	30	31	32	33	34	35	36	37	t	38	39	40	41	42	43	44	45	10	t	11	12	13	14	15	16	17	18	t	19	20	21	22	23	24	25	26	27	28	t
u	30	31	32	33	34	35	36	37	38	u	39	40	41	42	43	44	45	10	11	u	12	13	14	15	16	17	18	19	u	20	21	22	23	24	25	26	27	28	29	u
v	31	32	33	34	35	36	37	38	39	v	40	41	42	43	44	45	10	11	12	v	13	14	15	16	17	18	19	20	v	21	22	23	24	25	26	27	28	29	30	v
w	32	33	34	35	36	37	38	39	40	w	41	42	43	44	45	10	11	12	13	w	14	15	16	17	18	19	20	21	w	22	23	24	25	26	27	28	29	30	31	w
x	33	34	35	36	37	38	39	40	41	x	42	43	44	45	10	11	12	13	14	x	15	16	17	18	19	20	21	22	x	23	24	25	26	27	28	29	30	31	32	x
y	34	35	36	37	38	39	40	41	42	y	43	44	45	10	11	12	13	14	15	y	16	17	18	19	20	21	22	23	y	24	25	26	27	28	29	30	31	32	33	y
z	35	36	37	38	39	40	41	42	43	z	44	45	10	11	12	13	14	15	16	z	17	18	19	20	21	22	23	24	z	25	26	27	28	29	30	31	32	33	34	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	*	0	1	2	3	4	5	6	7	8	9	*

Figure 21.

the top line of the table in addition to the 26 letters. For example, one could have the 10 digits; a few common double-letter combinations, such as DD, LL, RR, SS; a few of the most frequently used pairs of letters, such as TH, ER, IN, or even such common syllables as ENT, ING, and ION.

63. Square Tables Employing Mixed Alphabets

a. In the tables thus far shown the alphabets have been direct or reversed standard sequences, but just as mixed sequences may be written upon sliding strips and revolving disks, so can mixed alphabets appear in tabular form. The table shown in figure 22, based upon the key word sequence derived from the word LEAVENWORTH, is an example that is equivalent to the use of a strip bearing the same key word sequence sliding against another strip bearing the normal 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
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
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
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 E
V N W O R T H B C D F G I J K M P W S U X Y Z L E A
N W O R T H B C D F G I J K M P Q S U X Y Z L E A V
W O R T H B C D F G I J K M P Q S U X Y Z L E A V N
O R T H B C D F G I J K M P Q S U X Y Z L E A V N W
R T H B C D F G I J K M P Q S U X Y Z L E A V N W O
T H B C D F G I J K M P Q S U X Y Z L E A V N W O R
H 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
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
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 B
D F G I J K M P Q S U X Y Z L E A V N W O R T H B C
F G I J K M P W S U X Y Z L E A V N W O R T H B C D
G I J K M P Q S U X Y Z L E A V N W O R T H B C D F
I J K M P Q S U X Y Z L E A V N W O R T H B C D F G
J K M P Q S U X Y Z L E A V N W O R T H B C D F G I
K M P Q S U X Y Z L E A V N W O R T H B C D F G I J
M P Q S U X Y Z L E A V N W O R T H B C D F G I J K
P Q S U X Y Z L E A V N W O R T H B C D F G I J K M
Q S U X Y Z L E A V N W O R T H B C D F G I J K M P
S 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
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
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 U
Y Z L E A V N W O R T H B C D F G I J K M P Q S U X
Z 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
```

Figure 22.

The usual method of using such a table is the same as that in the preceding cases. The only difference is that the key letters must now be sought in a mixed sequence, whereas in the preceding tables they were located in normal direct or reversed sequences. Example, using figure 22:
$$C_p (S_k) = X_c.$$

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

Figure 23.

b. Figure 23 illustrates a case in which a mixed alphabet is sliding against itself. The usual method of employing such a table is exactly the same as that explained before. The only difference is that both the plain-text letters and the key letters must be looked for in mixed sequences. Example, using figure 23: $U_p (R_k) = V_c$.

c. It has been indicated that the basis of reference in most cryptographic operations involving key words is the letter A_p. In employing sliding alphabets it is usual to set the key letter as located in the cipher component opposite the letter A as located in the plain component. But, as shown in paragraphs 42*b* and 60*c*, the key letter as located in the cipher component is usually set opposite the initial letter of the plain component. In all examples preceding that in figure 23, the key letter has been A. In figure 23, since the plain component is also a mixed sequence and its initial letter is Q, the sliding alphabets are set against each other so that the given key letter in the cipher component is opposite Q in the plain component. Thus, to duplicate the results given by the use of figure 23 in finding the value of $U_p (R_k)$, it is necessary to set the sliding strips in the following relative positions:

Plain: QUESTIONABLYCDFGHJKMNPRVWXZQUESTIONABLYCDEFGHJKM
Cipher: QUESTIONABLYCDFGHJKMNPRVWXZ

Here it is seen that U_p (R_k) = V_c, which is identical with the result obtained from the use of the table. There are other ways of using the table, however, each having a correspondingly modified method of employing sliding strips in order to obtain identical results.

Section VII.   OBSERVATIONS ON CIPHER SYSTEMS

64. More Complex Substitution Systems

a. The substitution systems discussed above are all based on relatively simple methods. They can all be solved rapidly. More complicated systems have been devised, however, and are used in certain situations. They are briefly described in this section.

b. Virtually all systems based upon the principle of a repeating key can be solved because of certain cyclic or periodic phenomena, which the use of a repeating key exhibits externally or internally in the cryptograms. There are methods for preventing the external manifestation in the cryptograms of these phenomena, or their suppression and disguise if present internally. In some, the principle is to make the elements of a fixed or invariable-length key apply to variable or irregular-length groupings of the plain text so that no cyclic phenomena are exhibited by the cryptograms. In others, the principle is to apply irregular lengths of the key, or a variable-length key to regular and fixed groupings of the plain text, with the same object in view. In still other methods, both principles are combined, or the key itself is of such a nature that it does not repeat itself. This may be brought about by constructing or establishing a non-repeating key, or by employing the key in a special manner. Systems in which the successive letters of the cipher text or successive letters of the plain text after the initial letter serve as successive key-letters are also used with the object of avoiding or eliminating periodicity.

c. In the majority of the methods described the encipherment deals with single letters, and is therefore *monographic* in nature. There are, however, certain methods in which encipherment is by pairs of letters, called *digraphic substitution,* or by sets of three letters, called *trigraphic substitution. Polygraphic substitution methods,* as they are called, have for their object the suppression, so far as possible, of the characteristic frequencies of individual letters, by means of which solution may be reached. The methods may employ extensive tables, small squares, rectangles, and other designs, or sets of sliding or rotating alphabets. The *Playfair Cipher,* which was for many years a standard field cipher in the British Army and was for a short time during World War I employed by the U. S. Army, is an example of digraphic substitution.

65. Combined Substitution-Transposition Systems

In paragraph 10*b*, reference was made to the possibility of combining within a single system both transposition and substitution methods; that is, of first enciphering by a method of one type and then taking the resulting cipher text and passing it through an encipherment of the other type. The usual order is first to substitute and then to transpose, but the reverse of this order of procedure is also possible. In some methods, quite complex, there may be a first substitution, then a transposition, and finally a substitution again. Despite the fact that three steps are involved, certain of these systems may be practical for military use under special conditions where speed is not as important as security. These cannot be described in this manual.

66. Cipher Devices and Cipher Machines

a. Only a little practical experience with any of the methods described is necessary to convince one that on the whole they are slow, more or less cumbersome, and subject to errors that often delay or make impossible the decryptographing of messages. Furthermore, from the point of view of cryptographic security, when employed in regular voluminous traffic they leave much to be desired. Consequently, cryptographers, both experienced and inexperienced, have been led to attempt to devise apparatus which will not only facilitate cryptographing and decryptographing, but will also increase the degree of cryptographic security. Small instruments constructed for this purpose, operated by hand, are called *cipher devices.* Scores of them have been devised, but only a few are sufficiently practicable for field use, and still fewer are of such construction that they produce cryptograms of unusual security. Among the better examples of such cryptographs is one which was for some years (1922–42) employed in the U. S. Army under the name of *Cipher Device, Type M–94.* Modern security requirements made such a device obsolete, however, and it has been replaced by a better one, the Converter M-209 ( ) (TM 11–380).

b. There are larger cryptographic machines which are much more nearly automatic in nature and can therefore be operated at a much greater rate of speed. These are usually equipped with typewriter keyboards which can be manipulated with considerable speed; the machine may also print the results of the enciphering or deciphering operations. Sometimes they are equipped with electrical transmitters and can thus serve not only to encipher and decipher messages but also to transmit them automatically. A mechanism of the latter nature is usually in the form of a modified printing telegraph machine, or else it consists of an auxiliary piece of apparatus used in conjunction with the teleprinter.

Such apparatus can obviously be practicably employed only among the larger headquarters where traffic is sufficiently heavy to warrant its use.

67. Disadvantages and Limitations of Cipher Systems

Except for certain electrically operated cipher machines equipped with a typewriter keyboard, most cryptographic methods using "manual" or "pencil and paper" cipher systems are unsatisfactory for military purposes. Practically all such systems can be solved by enemy cryptanalysts, and those suitable for use in the theater of operations offer fewer obstacles to solution than systems suitable for use in the rear areas. Cipher systems are not economical in time units required in electrical transmission; the best that they can do is to produce cryptograms no longer than the original plain text. For use within small tactical units in the forward areas there are other cryptographic methods which offer advantages of speed, simplicity, and brevity and which, properly used, afford sufficient cryptographic security. These are often preferred over cipher methods in the forward echelons of the combat zone. These methods involve the use of lists of groups of letters or figures to which arbitrary meanings have been assigned. They are called "field codes," "prearranged-message codes," "brevity codes," "voice codes," "jargon codes," etc. Codes will be discussed in the succeeding sections of this manual.

CHAPTER 4

ELEMENTARY CODE SYSTEMS

Section I.   GENERAL

68. Difference Between Code and Cipher Systems as Methods of Cryptography

A code system is a more or less highly specialized form of substitution. The basic principle underlying substitution cipher systems is the replacement of the individual letter in the plain text of a message by other letters, figures, or symbols. Occasionally the replacement or substitution process is applied to groups of letters, and when this is done the groups are usually of definite, or regular length. In cipher systems the units with which the cryptographic treatment deals are the smallest of which plain text can be composed. The basic principle underlying code systems, however, is the replacement of entire words, long phrases, or complete sentences constituting the plain text of a message by arbitrarily selected equivalents having little or no relation to the elements they replace. These equivalents may be other words, groups of letters, groups of figures, or combinations. It is only exceptionally that the replacement or substitution process is applied to elements smaller than whole words, and when this is done the elements are single letters, groups of letters, or syllables. In code systems the units with which the cryptographic treatment deals are aggregates of smaller units—individual letters combined in various groups of irregular length; that is, words, phrases, sentences.

69. Code Books and Codes

a. If it were possible to memorize a long list of words, phrases, and sentences, together with the arbitrary equivalents called *code groups* assigned to represent them, there would be no need of having written or printed code books. In a code book, the words, phrases, and sentences are listed in a systematic manner and accompanied by their code equivalents. Correspondents must possess identical copies of the document in order to communicate with one another. An ordinary dictionary may, and often does serve the purpose of code communication, so far as single words are concerned, but as a rule a specially prepared document containing the words, phrases, and sentences, suited to particular types of correspondence, is used. Such documents are called, in the United States

and in Great Britain, *code books* or, simply, *codes*. In other countries they are called *repertories, word books, cipher dictionaries, enciphering and deciphering tables, etc.*, although the term "code" is becoming prevalent throughout the world.

b. There are various types of codes each suited to particular types of correspondence. Some are large books used for general business or social correspondence; others are intended for particular industries—for example, rubber, sugar, steel, and automobile—and contain highly specialized technical vocabularies. Most large commercial firms have their own *private codes*, constructed especially for their use. This manual however, is concerned only with codes suitable for military communication. While the resemblances between the ordinary commercial codes and the usual military codes are marked, their primary purposes are different. Code is used in commercial communications principally to effect economy in cost of communicating, secrecy being of secondary importance. In modern military signal communications code is used to effect secrecy, brevity, and speed, especially in front-line signal communications. However, in lengthy administrative messages, the economy afforded by a properly constructed code is important.

70. Brevity Afforded by Code Systems

a. Messages cryptographed by means of a code book are secure only when the code book is kept secret. There are, however, code systems in which secrecy is not a factor. Such systems are intended for brevity or, in transmission by commercial telegraph, for economy. Code books afford a means for abbreviating or condensing the writing necessary to convey information. A single, comparatively short group of code characters may represent a whole word of as many as 15 or more letters, a long phrase, or a complete sentence. Thus, as a rule, the text of a code message is much shorter than the plain text, and therefore costs less to send. Naturally, the *condensing power* of a code book varies with the extensiveness of its *vocabulary*, since in a small book there can be listed only the most common words and only a few phrases and sentences; whereas, in a large book practically all the words likely to be used in telegraphic communication, and many common phrases and sentences may be included. When a code book is used to condense text only for purposes of economy, it is called a *nonsecret code*. Examples of such codes are the ordinary commercial codes sold in book stores. A code book may combine the features of economy and secrecy, in which case the book itself must be safeguarded from the enemy as a *secret code*.

b. In addition to money saving, code systems save time and labor in transmission and reception, as the number of characters handled in code systems is smaller than in cipher systems. The saving of time is an

important factor in front line communications where speed is essential and sometimes outweighs security considerations.

c. In military cryptography, the greatest degree of condensation is afforded by "prearranged-message codes," "brevity codes," and the like. A *prearranged-message code* is a tactical code adapted to the use of units requiring special or technical vocabularies; it is composed almost exclusively of groups representing complete or nearly complete messages and is intended for shortening messages and concealing their content. A *brevity code* has for its sole purpose the shortening of messages. A *field code* is primarily a small tactical code which contains a large number of code groups representing words and a few common short phrases, from which sentences can be composed; a *syllabary*, which is a list of code groups representing individual letters, combinations of letters, or syllables, is usually provided for spelling out words or proper names, not present in the vocabulary; *numerical tables*, or lists of code groups representing numbers, dates, and amounts, are also included. A *jargon code* is another name for a simple, very short code in which bona fide dictionary words, baptismal names of persons, the names of rivers, lakes, etc., are used as code groups. A *voice code* is used for transmission by the small radio-telephone sets used in combat areas and may be a prearranged-message code, a brevity code, or a jargon code. Other names used to designate such codes are *combat code*, and *operations code*.

71. Operation of Encoding and Decoding

These two terms apply to the cryptographing and decryptographing respectively, of messages by means of a code. In encoding a message, a code clerk merely replaces the various words, phrases, sentences, and numbers of plain text by their code equivalents. The code text is built up from code units each representing the longest possible plain-text unit the code book affords. For example, if the sentence ENEMY FORCE ESTIMATED AT ONE BATTALION ENCOUNTERED ONE MILE SOUTH-EAST OF ROCK CREEK CHURCH is to be encoded, and the code book lists the phrase ENEMY FORCE ESTIMATED AT, the code group representing this phrase would be used rather than separate code groups representing the individual words ENEMY, FORCE, ESTIMATED, and AT, all of which might also be present in the code. The process of decoding is the reverse of that of encoding. Each code group is looked up in the code book, its meaning found and written down. Where the errors in transmission are few, the process is rapid; but even a small number of errors in a message may obscure the meaning or render a message unintelligible.

Section II. CODE GROUPS

72. Composition of Code Groups

a. The elements of which code groups are composed may be of one or more of the following types:

(1) *Bona fide words*—real words taken from the dictionaries of one or more languages. The usual languages employed as sources for code words of this type are Dutch, English, French, German, Italian, Latin, Portuguese, and Spanish.

(2) *Artificial words*—groups of letters having no real meaning, constructed more or less systematically by arrangements of vowels and consonants so as to give these groupings the appearance and pronounceability of bona fide words.

(3) Groups of letters presenting no appearance of bona fide or artificial words and resembling cipher groups.

(4) Groups of arabic figures.

b. For special purposes, code groups composed of intermixtures of letters and figures within groups may be used. Call signs for radio stations, such as W2KA and W5AZZ, are examples of such intermixtures often used in radio call-sign codes. In certain highly specialized naval or military codes, the intermixture of letters and figures is sometimes necessary. Such intermixtures, however, are either not accepted or, if accepted, are charged for at a greatly increased rate when they appear in messages transmitted by commercial communications agencies.

c. A code may contain two or more parallel sets of code groups of different types. For example, in many commercial codes and in some military and naval codes, there is one series of code groups of the bona fide or artificial word type and another series of the figure-group type, both applying to the same series of words, phrases, and sentences of the code. There are several reasons for this. In most parts of the world where italic or roman letters are used for writing, letters possess greater advantages in accuracy of reading and handling by telegraph personnel. This is necessary for correct transmission and reception of messages. However, in some parts of the world—for example, Turkey, Russia, China—telegraph personnel, except in the large cities, are unfamiliar with the English alphabet and hence many errors in transmission arise. But arabic digits are almost universally recognized and used, so that for communications between obscure ports and small cities in foreign countries, figure groups are preferred over letter groups. There are certain methods of condensing code groups composed of figures into still smaller groups composed of letters by means of *condensers,* so that many firms use figure groups for such purposes in expensive transmissions. Finally, in certain methods of enciphering code messages for the sake of greater

secrecy, figure groups often form the basis for the encipherment more readily than do letter groups.

d. Prior to 1 January 1934, in practically all modern codes constructed by experts, letter code groups were of the artificial-word type. On that date new rules in international communication became effective,[8] permitting the use of letter code groups without restriction in their formation, as class (3) in *a* above. It is probable that almost all of the codes published subsequently to the above date will contain letter code groups of the unrestricted type.[9]

e. The greatest advantage possessed by letter groups over figure groups lies in the availability of a far greater number of permutations, or interchanges, of letter groups, because there are 26 letters which may be permuted to form letter code groups, whereas there are only 10 digits which may be permuted to form figure groups. If code groups of five elements are used, then there are available 26^5, or 11,881,376 groups of five letters, and only 10^5, or 100,000 groups of five figures. Now since the number of permutations of 26 letters taken in groups of five is so great, only permutations conforming to special types may be selected for use, and there will still remain a sufficient number of code groups for even the largest codes. Certain types of code groups are selected so that possible error in telegraphic transmission can be reduced to a minimum. If the code groups have been constructed scientifically it is possible to correct such errors quickly without having the message repeated.

73. Length of Code Groups

The length of code groups used, whether the groups consist of two, three, four, or five elements, depends upon the size of the code. This applies almost exclusively to field military or naval codes, where transmission is through a governmental agency; in commercial messages or in governmental communications transmitted over privately-operated lines, five-letter or five-figure groups are used almost exclusively because of the regulations adopted by the International Telegraph Conferences and by commercial telegraph and cable companies. As a general rule in the transmission of code and cipher messages, each group of five letters is counted as one word regardless of the number and arrangement of vowels; each group of five figures is counted as one word.

74. Permutation Tables of Two-Letter Differential

a. Code groups of modern codes are constructed by use of tables which permit more or less automatic and systematic construction in the form desired. These are called *permutation tables.* Because they may be used

[8] See Telegraph Regulations, International Telecommunication Convention, Madrid, 1932.
[9] For a treatise on the development of codes see "The History of Codes and Code Language, the International Telegraph Regulations pertaining thereto, and the bearing of this history on the Cortina Report," by Major William F. Friedman, Sig.-Res., Government Printing Office, 1928.

to correct most errors made in transmission or writing, such tables are usually included in the code book and are called *mutilation tables, garble tables, error-detector charts, etc.* Before the invention of permutation tables, code as a system of communication was not wholly reliable. Scientifically constructed tables, however, include a feature (see *b* below) which has remedied this fault to a great extent.

b. To make an error in a group of five letters is not unusual on the part of the average telegraph or radio operator. If a difference of only one letter distinguishes one code group from another in the same code, as ABABA and ABABE, then serious errors may be introduced in the meaning of a message, or the message may be made unintelligible by only a few transmission errors. If, however, every code group in the code book is distinguished from all other code groups in the same code by a difference of at least *two* letters, then there would have to be two errors in a single group and these two errors would have to produce a code group actually present in the code before a wrong meaning would be conveyed. This principle of making code groups within the same code differ from each other by a minimum of two letters is called the *two-letter differential.* It is most easily incorporated in code groups by constructing the permutation table to this end. The differential may be the absolute difference in the identities of two letters or the relative positions occupied by them. For example, BACOF, and BACUG differ from each other in the identities of the final pair of letters; considered as a *combination* of letters, the two groups present a two-letter difference. The two groups BACOF and BOCAF, however, differ in the relative positions occupied by two of their letters, but considered as a permutation of letters, these two groups as well as the two groups BACOF and BACUG, present a two-letter difference. In short, when at least two corresponding letters in a pair of code groups differ in their identities, the two code groups are said to present a 2-letter difference. Errors arising from the exchange of position of two letters, without a change in their identities, are referred to as errors of *transposition.* They are not unusual but fortunately, as a rule, they involve only letters which are either adjacent or alternate. For example, in the pair of groups BACOF and BOCAF there is a transposition of the alternate-letter type. In recent codes, attempts have been made to devise permutation tables which will eliminate one of the two members of every pair of groups which differ from each other by the mere transposition of two adjacent or alternate letters. Codes using groups based upon a permutation table will show the table and explain how to use it in correcting the usual mutilations of groups.

c. The use of the two-letter differential reduces the possibilities for constructing letter-code groups from 26^5 (11,881,376) to 26^4 (456,976), but, considering the advantages, the sacrifice is worthwhile.

d. Permutation tables for the construction of figure-code groups are similar in nature and purpose to tables for the construction of letter-code

groups. However, because of the more limited number of characters available for permutations, the maximum number of 2-figure difference groups possible in a 5-figure code is 10^4, or 10,000.

Section III.   ONE-PART AND TWO-PART CODES

75. Arrangement of Contents of Codes

a. In their construction or arrangement, codes are generally of two types:

(1) *One-part,* or alphabetical codes. The plain-text groups are arranged in alphabetical order accompanied by their code groups in alphabetical or numerical order. Such a code serves for decoding as well as for encoding.

(2) *Two-part,* or randomized codes. The plain-text groups are arranged in alphabetical order accompanied by their code groups in a nonalphabetical order. The code groups are assigned to the plain-text groups at random by drawing the code groups out of a box in which they have been thoroughly mixed, or by some other manner in which the element of chance operates. Such a list can serve only for encoding. For decoding, another list must be provided in which the code groups are arranged in alphabetical or numerical order and are accompanied by their meanings as given in the encoding section. For this reason a two-part code is often called a *cross-reference code.* The following brief extracts from typical one-part and two-part codes illustrate the difference between them:

One-part code.		Two-part code.			
		Encoding Section		Decoding Section	
ABABD	A	GAJVY	A	ABABD	Obstructed
ABACF	Abaft	TOGTY	Abaft	ABACF	Term
ABAHK	Abandon	FEHIL	Abandon	ABAHK	Zero
ABAJL	.... it	BAYLT	.... it	ABAJL	If it has not
ABALN	Abandoned	ZYZYZ	Abandoned	ABALN	To be sent by
ABAMP	.... by	NYSYZ	.... by	ABAMP	Acceding
ABAWZ	Abandoning	IFWUZ	Abandoning	ABAWZ	Building
ABBAD	Abandonment	RUMGO	Abandonment	ABBAD	Do not attempt
--------------		--------------		--------------	
ZYZYZ	Zero	ABAHK	Zero	ZYZYZ	Abandoned

b. Between the two extremes are codes which have features of both; that is, complete sections may be arranged in random sequence, but within each section the contents are arranged in some systematic or logical order. This is true, however, only of some of the older codes. In modern types, the two-part construction is more common.

c. When a strict alphabetical arrangement is used in the sequence of the phrases, the code is said to be a *strictly alphabetical code;* when the phrases are listed under separate headings based upon the principal word or idea in the whole expression, the code is said to be a *caption code.* The following extracts will serve to illustrate the two types:

Caption code	*Strictly alphabetical*
Assistance	Assistance
Give *assistance*	Assistance for
Require *assistance*	Assistance from
No *assistance* required	Assistance has been sent
Assistance has been sent	Assistance to
Assistance for	Assistant
Assistance from	Assisted
Assistance to	. . . .
Assistant	Give
Assisted	Give assistance
etc.	. . . .
	No
	No assistance required
	. . . .
	Require
	Require assistance

d. More precise and economical encoding is possible with a caption code than with an alphabetical code. With the caption code it is easier to assemble an extended variety of expressions and shades of meaning under specific headings than with the alphabetical code. On the other hand, the use of a caption code involves more time and labor in encoding, especially by untrained or unskilled personnel, than the use of an alphabetical code. Where the phraseology of communication is standardized or stereotypic, the most common expressions may be listed in an alphabetical code as readily as in a caption code. In both types of codes there may be tabulated material, such as tables of numbers, dates, equipment, geographical or personal designations, either forming isolated sections in the code or inserted in the vocabulary under appropriate headings.

e. Two-part codes are used by many governments for their secret diplomatic, military, and naval communications because the advantages they offer over one-part codes are greater than their disadvantages. The disadvantages are: a two-part code is harder to handle than a one-part code because it is at least twice as large in content, since each code group and each plain-text element must appear twice; the cost of printing is approximately double; the amount of labor in compiling a two-part code is nearly four times greater because of the necessity for preparing the accurate cross-reference arrangement which is its basic principle.

76. Purposes of Two-Part Type of Code

a. The two-part code is a comparatively recent development in code systems. Its purposes are greater secrecy, and greater accuracy.

b. In a one-part code the plain-text groups progress from A to Z in a regular alphabetical sequence, accompanied by their code groups, also in a regular alphabetical or numerical sequence. If the word ABAFT is represented by a code group whose initial letter is A, or whose initial number is 1, then the word ABANDON will be represented by a group whose initial letter is also A, or whose initial number is also 1. In other words, the enemy cryptanalysts have definite clues to follow in breaking down the code because of the parallelism of the two sequences; the determination of the value of one code group affords definite clues to the value of many other code groups. In a two-part code, however, the word ABAFT might be represented by a group whose initial letter is T, or whose initial number is 8, and the word ABANDON might be represented by a code group whose initial letter is F, or whose initial number is 3. In other words, the two sequences are not alike in progression; hence the determination of the value of one code group will give no clues to the value of any other group.

c. In considering the greater accuracy of a two-part code over a one-part code, the following pair of phrases (in a hypothetical one-part code) are given as an example:

> WOVAM Will be ready to attack
> WOVEN Will not be ready to attack

Such an arrangement is subject to two sources of error. A code clerk working under great difficulties, in a hurry, may accidentally write down WOVAM instead of WOVEN as a result of the contiguity of the two sets of letters which are similar in appearance and are so close together on the page that his eye may take the group from the wrong line. Again, on account of the similarity in sound, his ear may deceive him into writing WOVEN when he should have written WOVAM. Now the meaning of the one group is the exact opposite of the meaning of the other and, since either meaning may fit in correctly with the context of the message, the error may remain undiscovered for some time, thus causing serious inconvenience or, in the case of combat, actual loss of life. Furthermore, although the making of two errors in a single group is rather unusual in transmission or reception, yet it does happen and, in such a case as the above, would not be detected. This is especially true in connection with tabular material such as lists of numbers, dates, and names, in which the context often fails to yield clues to the correction of garbles or errors, or to give conclusive evidence of the presence of an error. But in a two-part code such errors are improbable. In the first source of error mentioned above, the code clerk would be very much less

likely to confuse two entirely different groups of letters; in the second source, if two errors are made in the transmission or reception, and if these errors involve two letters producing a group which actually has a meaning in the code, this meaning is so unlikely to fit in correctly with the context that its probability of occurrence may be negligible. Thus, if this sort of error does happen, the meaning of the group fails to fit in with the context and at once indicates an error. Knowledge of such an error, even if it is impossible to correct it, is more preferable than ignorance of its existence, with a possible action based upon incorrect decodement.

Section IV. ENCIPHERED CODE

77. Purposes of Enciphered Code

a. Sometimes the code groups of a code message undergo a further process of encipherment. The resulting cryptogram constitutes an *enciphered code message.*

b. It is desirable to use enciphered code in two instances:

(1) When the basic code has had wide distribution and the message might fall into unauthorized hands. Commercial codes sold in bookstores, and even special codes distributed widely throughout governmental offices, illustrate the type of code to which this added safety factor should be applied.

(2) When increased security is necessary for highly classified communications. Although the basic code book may already be secret, further encipherment would greatly delay the solution of the code if it fell into the hands of enemy cryptanalysts.

c. It has already been stated that code messages may be solved by cryptanalytic principles without possession of the code. The length of time required for the process varies widely, and is dependent upon the conditions under which the work is done (see ch. 1). To increase the length of time required for solution, as in secret codes, the code text of the messages resulting from the use of the code is passed through a cipher process so that the messages will be in different keys, thus delaying the assembling and study of data, which is necessary to the solution.

78. Types of Encipherment

a. Both of the two general classes of cipher methods, transposition and substitution, may be used in enciphering code. The increased degree of secrecy because of encipherment depends entirely upon the nature of the system applied.

b. Transposition systems involving a rearrangement of complete groups may be employed where the degree of increased security does not

72

have to be of a high order, and where the original form of the groups must be retained even after encipherment. Transposition systems in which the order of the letters within groups is changed may also be employed. For example, a numerical key may indicate the transposed order of the letters of the code groups, so that a group such as XDFGY will become DFYXG.

c. Substitution systems of many sorts may be employed, ranging from simple monoalphabetic to the most complex types of substitution with cipher machinery. Tables of alphabets are often used. In some systems, a simple transposition process may be combined with a simple substitution process.

d. A favorite method in one-part codes having both letter-code and figure-code groups is that in which the letter-code group standing at a prearranged interval before or after the letter-code group representing the actual word or phrase intended to be conveyed is substituted. The interval may remain fixed within a single message, or it may vary according to some predetermined key. Numerical code groups make the use of large intervals practicable.

e. In modern practice, the most common methods of enciphering figure-code groups are those using addition or subtraction, with a *key book* containing arbitrary groups of figures. When such methods are properly used, they yield a high degree of security. The highest degree of security is attained when such a key book is used *only once*.

CHAPTER 5

COMPARISON OF CODE AND CIPHER SYSTEMS

79. Advantages and Disadvantages of Each Type of System

a. From the viewpoint of purely military cryptography, a comparison of the advantages and disadvantages of each method can be made only between systems suitable for each of the following three general categories:

(1) High-security, or "high-grade," systems for cryptographic intercommunication among the largest military units and the highest echelons of command.

(2) Medium-security, or "medium-grade," systems for cryptographic intercommunication among the intermediate units and echelons of command.

(3) Low-security, or "low-grade," systems for cryptographic intercommunication among the small units and the lowest echelons of command.

b. The principal factors to be taken into account in comparing code and cipher methods in cryptographic communication are reliability, security, rapidity, flexibility, and economy.

(1) *Reliability*. Reliable cipher machines made possible by modern engineering and cryptographic techniques satisfy all or a majority of these factors to a great degree, and such machines are now used in the U. S. Army for these high-grade systems. Although the machines are complex, their reliability can be assured by having properly trained personnel to operate and maintain them. Accuracy is also one of the elements of reliability and a good cipher machine can yield a higher degree of accuracy or completeness of text in cryptographic communication than can a code system. A mistake in one or two code groups may obscure, alter, or render unintelligible the meaning of a whole message, but in cipher systems, often wrong letters may be corrected, or missing letters may be supplied, by the context. It must be remembered, however, that in some cipher systems a single error of a fundamental type, such as using the wrong key or the wrong "setting," may prevent the deciphering of the message.

(2) *Security*. If reliability were the only or the most important factor, code would be preferable to cipher for all echelons of

command, because the simplicity of a code book is to be preferred to the complexity of a large cipher machine. But unenciphered code is not sufficiently secure for the communications of the highest echelons and headquarters. If encipherment must be added as a second step in the cryptographic process, it practically destroys the simplicity features of a code system; unless the enciphering method is fairly complex, it adds little security. In a properly designed cipher machine, embodying sound cryptographic principles based upon a thorough knowledge of cryptanalytic principles, the single-step-encipherment process can yield cryptograms of very great security. In a good code system, however, the solution of one or even of several messages does not entail the immediate breakdown of the entire system, with the consequent ability to read all messages, as is usually the case in a cipher system.[10] Codebooks, of course, can be rendered useless by compromise. Actual possession for a long period of time is not necessary; methods of rapid photography may be applied and a book of several hundred pages copied in a few minutes.

(3) *Rapidity.* The speed with which a cipher machine equipped with a typewriter keyboard can be operated leaves even simple, unenciphered code far behind in the matter of rapidity.

(4) *Flexibility.* Complete flexibility would permit cryptographing the originator's own language without change necessitated by the limitations that exist in all but the most extensive codebooks. Thus, a cipher machine is much more flexible than a code and can be used for all sorts of messages; whereas, in a code containing words, phrases, and sentences prepared for a specific type of communication, rewording the original text as written by the originator is often necessary, if the words, phrases, and sentences in the codebook are to be used; otherwise the original wording must be encoded word by word, or even syllable by syllable.

(5) *Economy.* Whether expressed in terms of money or manpower, cipher systems are more economical than code systems for high-echelon communications. Code text is usually shorter than the equivalent plain text, because it is condensed or abbreviated, but a single clerk operating a rapid cipher machine

---

[10] A good cipher system may be compared to a library housed in a large structure of many rooms with all doors and all windows securely locked. If an intruder can force an entry into the structure, he will find a master key which will open all the locks and give him access to *all* the books in the library. A good code system (especially a two-part code) may be compared to a library housed in a similar structure, but no two locks are alike and no master key is available or can be made. Therefore, the lock on *each* door must be worked at patiently as a separate problem. Thus, although the intruder may force his way into one room, this gives him access to only a small part of the library; in order to read all the books, he must force his way into each room, which takes much time, since each lock presents a separate and special problem.

can turn out 10 to 15 times as much work as one operating a code system; furthermore, codes must be prepared, printed, and distributed. These steps take much time and labor and are often performed under considerable difficulty. A continuously operative code compilation section must be maintained to replace codes as fast as they become compromised by continued use, or by capture. The handling of the manuscript and proofs in printing entails the necessity of ever watchful secrecy; and finally, the prompt and thorough distribution of codes to all who must use them is sometimes very difficult, especially where the distribution must be made over an extensive territory. Therefore, for high-echelon cryptographing communications, ciphers are more economical than codes, but the economy factor is least important.

c. It is clear that high-grade systems should include all or as many as possible of the five factors listed in *b* above; moreover, the advantages afforded by good cipher machines make cipher systems more desirable than code systems for the high-grade cryptographic systems required by high-echelon cryptographic intercommunication. In addition, secondary or "back-up" systems must be provided so that in case of machine or power failure, there will be available some means for cryptographic communication. Finally, emergency systems must be provided for cryptographic communication when neither apparatus nor codebooks can be employed.

d. Medium-grade cryptographic systems for intercommunication among intermediate echelon commands must meet almost the same severe requirements as systems for intercommunication among high-echelon commands. Here again, cipher machines are preferable to code. The machines may not be so large or complex, but if the same basic cryptographic system is employed by both the high-grade and the medium-grade machine, many advantages are noted. The problems of manufacture, maintenance, instruction of personnel in the operation of the system, distribution of keying data, etc., are simpler if they are basically the same for both types of machines. Moreover, it is possible for a message from an intermediate command to be deciphered by a high-echelon command, and vice versa, without using a second cryptographic system. For these reasons, cipher machines are widely used in the U. S. Army for medium-grade cryptographic communication and, in addition, certain manual systems requiring simple types of apparatus are also used. These may serve also as the secondary or "back-up" systems required for the high-echelon cryptographic communications.

e. (1) Even in the so-called "low-grade" systems, cipher machines are serving the purposes for which field codes were formerly supplied. Converter M–209–( ) is a small, mechanical cipher machine widely used in the U. S. Army for communications

within the small combat units. If properly used, it yields crypto-grams of considerable security. It is a complicated device; it has no keyboard, and is slow in operation. Despite its reduced size and weight, this device is not convenient for use in front-line areas, nor is it suitable for use in voice communication by small radio-telephone equipments such as the "walky-talky" or "handy-talky" sets.

(2) Manual or hand-operated cipher systems are also unsuitable for such purposes. The processes of enciphering and deciphering by means of such systems require very close mental attention to avoid errors; the more secure methods are hopelessly slow and the faster ones are not secure, in comparison with the security that a small, frequently-changed *two-part* code yields.

(3) Practical experience indicates that in messages of very small tactical units, in certain types of air-to-air or air-to-ground communications, and in certain forms of messages where the subject matter is highly stereotypic, as in weather reports and fire-control observations, code is often preferred over cipher. In all these cases, speed must give way to security; size and weight of equipment are important factors; simplicity of operation under battle conditions is vital, which eliminates methods requiring much training and concentrated attention. Also, if code is properly prepared, one or two code groups may express a command or a report that would require many groups of cipher text. Small codes meet the requirements in all these respects, and for this reason, code is still used to some extent in the U. S. Army, especially in the forward areas.

80. Fundamental Assumption of Military Cryptography

It has been seen that every good cryptographic system combines two more or less separate and distinct elements: a basic or unchangeable method or process, which is termed the general system; and a specific or variable factor which controls the steps under the general system and is termed the specific key. The secrecy of any military cryptographic system must be entirely dependent upon the specific key because it *must be assumed that the enemy is in full possession of all the details concerning the general system*. This assumption is warranted by the whole history of military cryptography and is based upon the two following considera-tions which all experienced cryptanalysts regard as valid. In the first place, in military cryptography there are more prolific sources from which to obtain information concerning cryptographic methods than there are in the isolated methods used by private individuals. In fact, by one means or another, the enemy can sooner or later come into possession of full information regarding the general cryptographic system. In the

77

second place, within a very short time the number of messages available for study becomes so great, and the inevitable blunders in the handling of communications have become so numerous that a solution by detailed study can always be made by the enemy, with a consequent disclosure of the general system. If a cryptographic system adopted for military use were such that messages in that system could be solved easily without the specific keys applicable to the messages once the underlying methods became known, the entire system would have to be changed, a new system devised, and thousands of persons in the military service trained in its operation. This, of course, would be impracticable. It is assumed that the enemy has knowledge of the general cryptographic system, its cipher devices, instruments, or machines. Only cryptographic documents which are given a limited distribution can be kept secret from the enemy, but they can be kept secret only for a variable length of time before they must be changed. These changes, as a rule, do not affect their method of usage. In cipher sytems, the specific key must be susceptible of easy and rapid changes by prearrangement between correspondents. In systems for use by secret agents or very small military parties in the theater of operations, the key may be an easily remembered word, phrase, sentence, or number; it must not require the carrying of written notes on the person. In systems for use by commanders of large and intermediate or even small headquarters in the theater of operations, the specific key may be in the form of written memoranda, paper tapes, and the like. Generally, the specific key must be the same throughout a given period of time for all the members of an intercommunicating network, or at least only a very limited number of specific keys must be in simultaneous effect; otherwise confusion and delay are inevitable. As a consequence of this requirement, the enemy may intercept a good many messages all in the same specific key. A cryptographic system for military use must conform to all requirements of practicability set forth in section IV, chapter 1, and to the foregoing section concerning the specific key; this system must be such that it is practically impossible for the enemy to solve any message quickly enough to make the information obtained of real or immediate value in the tactical situation, even though he is in full knowledge of the general method of the system, possesses the cipher device or apparatus, if used, and may have available for study 1,000 or more cryptograms sent on the same day. There is no single cryptographic system yet known which fully meets all these requirements, and in order to provide the necessary degree of security for a large army several different types of ciphers and cipher machines, as well as small codes for front line use, must be employed simultaneously.

CHAPTER 6
CORRECTION OF ERRORS

81. Sources of Error in Cryptography

Errors, mutilations, and garbles are some of the names applied to the inaccuracies that occur in cryptographic communication. They are so common and so troublesome that commanders who, for the most part, already regard cryptographic processes as hopelessly slow and cumbersome, often become much prejudiced against their use in active operations. Therefore, instruction in the correction of errors is an essential part of the training of personnel assigned to cryptographic work. Training and experience will reduce the time necessary to correct the most common types of errors, which may be traced to the following sources:

a. Cryptographing and decryptographing, including the simple process of copying by hand or by typewriter.

b. Transmission and reception by all means of signal communication other than those in which the cryptograms are physically carried from origin to destination.

82. Practical Suggestions for Eliminating Errors

a. Errors in cryptographing and decryptographing can be much reduced though not wholly eliminated, by systematizing the work so far as possible and *invariably* checking it. Great care must be exercised in the formation of letters in writing, and roman capitals should always be used. If copied messages are checked for correctness by two operators, one reading the letters to the other, a phonetic alphabet must be used in order to prevent misunderstandings. In forward areas it is impossible to provide suitable or convenient quarters for personnel engaged in cryptographic work, but in rear areas and at the larger headquarters this personnel will work much more efficiently in a quiet, well ventilated office. To check the accuracy of cryptographic work it is always advisable, when possible, that an operator other than the original cryptographic clerk decryptograph the message. In checking his own work, an operator should actually decryptograph it—not merely check his cryptographing—because it is a psychological fact that persons have a tendency to repeat an error unconsciously. The most serious errors in cryptographic work leading to difficulties and delays in decryptographing are not the mere mistakes in the writing down of letters, but are errors of a fundamental nature which the operator says, when it comes back to him, "I don't see how I could

have made it." Checking by actually decryptographing will usually eliminate such errors. At the destination, the *final copy* of a decryptographed message should invariably be checked against the *original* work sheets before being turned over to the addressee, and again preferably, by another operator. It is easy to omit the word NOT from a decoded message and to fail to note the omission, if the same operator merely reads over the decryptographed message. Here, again, psychological factors are involved, and clerks who are disposed to transpose letters and words, an unconscious habit of a peculiar psychological origin, must be especially careful in their work.

b. Carelessness in the writing of system and message indicators, or failure to insert them in their proper places in the message, will usually make prompt decryptographing of the received message difficult or impossible. They should be written with the greatest of care.

c. If an incoming message is partially or wholly unreadable, an attempt should be made to find the error in the faulty message. Often a message can be decryptographed by a simple expedient such as applying the key for the day preceding or following and correct date, or applying the daily key for a classification higher or lower and the correct classification. If, however, the garbled text still resists all efforts of correction, a procedure (service) message should be sent. The length of time one should continue with the attempt to break the faulty message before sending a service will depend upon the classification and precedence of the message, transmission problems involved, time required to complete service, etc.

d. The procedure in preparing and handling service messages dealing with errors in cryptographic messages is quite involved, in order not to compromise the cryptographic system or give clues as to the contents of the faulty message. Instructions covering the procedure to be followed in such servicing are issued from time to time and should be carefully followed.

e. The most important precaution to be observed, in order to avoid the transmission of messages which cannot be promptly decryptographed at the receiving end, is the rigid adherence to all instructions set forth in documents describing the cryptographic operations to be followed. Misunderstanding or ambiguity is rarely found in *properly prepared* documents detailing cryptographic operations, and a careful study and observance of the instructions will result in the preparation of messages without fundamental errors.

f. To be efficient in cryptographic work requires, in addition to the usual qualities of carefulness, accuracy, and attention to detail, the possession of certain psychological characteristics peculiar to the work. If absent, these characteristics as a rule cannot be developed, but if present they can be intensified and made more efficient by constant practice and experience. It is therefore advisable to select personnel for cryptographic work as for any other specialized work, to train them carefully, and

retain them as long as possible; the longer they remain in this work the less likely they are to repeat the errors with which the work abounds and the more likely they are to render highly efficient service.

g. Errors in transmission and reception are frequently made, especially in transmission by radio, because of interference, atmospheric disturbances, and the like. Cryptographic clerks should be familiar with the Morse and Bandot alphabets and the most common errors of wire and radio transmission methods, so as to be able to refer an error to its probable origin or to find clues for the correction of badly garbled groups when all other means fail. The following tables will be found useful:

Most common errors in Morse transmission

International Morse alphabet (used in radio, cables, and outside United States)			American Morse alphabet (used in the United States, except for radio)		
Letters and figures	Alphabet	Frequent errors	Letters and figures	Alphabet	Frequent errors
A	·—	i, m, t, et	A	·—	i, t, et
B	—···	d, ts	B	—···	d, h, ts
C	—·—·	f, k, j, r, nn	C	·· ·	s, z, ie
D	—··	b, s, l, ti	D	—··	b, ti
E	·	t, a, i	E	·	t
F	··—·	q, r, in	F	·—·	r, q, en
G	——·	m, n, o, q, me	G	——·	n, c, me
H	····	s, v, b, se	H	····	s, p, z, y, es
I	··	a, n, s	I	··	a, o, e
J	·———	w, o, eo, am	J	—·—·	c, k, ke
K	—·—	a, n, d, o, ta	K	—·—	j, n, ta
L	·—··	x, r, d, ed	L	—	t, n
M	——	a, n, i, tt	M	——	n, a, tt
N	—·	i, m, t, te	N	—·	o, t, te
O	———	g, k, m, w, mt	O	· ·	n, i, ee
P	·——·	j, w, g, l, r, an	P	·····	h, s
Q	——·—	g, k, o, x, z, ma	Q	··—·	f, g, u, in
R	·—·	a, n, f, g, s, l, w	R	· ··	s, i, ei
S	···	h, d, i, r, u, v	S	···	h, r, i
T	—	a, e, n	T	—	l, e, n
U	··—	a, s, v, it	U	··—	v, a, w, it
V	···—	h, u, x, st	V	···—	u, st
W	·——	a, m, o, r, u, at	W	·——	f, a, u, m, at
X	—··—	d, v, u, k, y, tu	X	·—··	l, y, f, ai
Y	—·——	x, w, k, c, nm	Y	·· ··	h, ii
Z	——··	b, d, g, q, mi	Z	··· ·	h, c, se
1	·————	0, 2	1	·—·.	p
2	··———	1, 3	2	··—··	3
3	···——	2, 4	3	···—··	4
4	····—	3, 5	4	····—	3
5	·····	4, 6	5	———	
6	—····	5, 7	6	······	p
7	——···	6, 8	7	——··	
8	———··	7, 9	8	—·····	
9	————·	8, 0	9	—··—	x
0	—————	9	0	—	L

81

TELETYPEWRITER GARBLE TABLE

AT THE TOP AND BOTTOM OF THE CHART ARE THE LETTERS ORIGINALLY TRANSMITTED.
IN THE SQUARES ARE THE CHARACTERS WHICH WOULD BE RECEIVED WITH GAIN OR LOSS OF PULSE
DEPENDING UPON WHETHER MACHINE IS IN "UC" (UPPER CASE) OR "LC" (LOWER CASE).

CHAPTER 7
FUNDAMENTAL RULES FOR SAFEGUARDING CRYPTOGRAMS

83. General

The rules given in this chapter are to be considered as a general guide only. Under actual operating conditions much is dependent upon special situations, and the specific cryptographic systems employed. Therefore, the particular rules and regulations currently in effect always will take precedence over those stated herein.

84. Fundamental Rules of Cryptographic Security

a. Failure to observe the fundamental rules of cryptographic security often makes possible the solution of cryptographic systems by enemy cryptanalysts. These rules apply to the originators of messages to be cryptographed as well as to cryptographic personnel. Detailed instructions for the writers of such messages are outside the scope of this manual. It is, however, desirable to indicate the following points:

(1) Stereotypic phraseology must be avoided, especially at the beginning and ending of a message. *The known or suspected presence of stereotypic phraseology constitutes the basis of many methods employed in cryptanalysis;* in some cases, indeed, the only possible method of solution makes use of the presence of stereotypic phraseologies, or, as they are often called, *cribs.* Operating instructions for currently authorized cryptosystems prescribe the application of measures which effectively reduce the dangers of stereotypic phraseology to the security of those systems; however, as an added precaution, routine reports of all kinds should be sent by agencies of signal communication not susceptible to interception.

(2) Special care must be taken to see that the messages are clear and concise. If a message is ambiguous or incomplete, unnecessary confusion results and the accuracy of the cryptographic operation is brought into question.

(3) Messages should be shortened by the deletion of unnecessary words. Conjunctions, prepositions, repetitions of words, and, especially, punctuation should be reduced to a minimum. When punctuation is necessary, it should be spelled out, either in full or in abbreviated form. Numbers should also be spelled out.

Where letters of the alphabet must be used, as in certain sym-
bols designating types of equipment, it may be necessary to
represent these letters by their authorized phonetic equivalents,
where it is essential that there be no possibility of error. Such
spelling out however, should be reduced to a minimum.

(4) Authorized abbreviations should be used whenever practicable.

(5) Regulations regarding the manner of indicating addresses and
signatures should be carefully followed.

(6) Regulations governing the security classification of messages
(Top Secret, Confidential, Restricted) must be observed at all
times.

*b. Much of the success which attends the efforts of cryptanalysts is
based upon ignorance and carelessness on the part of cryptographic per-
sonnel.* Rarely are cryptographic blunders the result of willful violation
of instructions; but if cryptographic personnel realize, that, by careless-
ness or ignorance, their own lives and those of thousands of their com-
rades are jeopardized, they will be more attentive to rules set up for their
guidance. The most important of these rules are as follows:

(1) *Questionable messages.* Never cryptograph a message which, in
the opinion of the cryptographer, violates any of the provisions
or regulatons relating to the drafting of messages, until the
question has been referred to and passed by someone with
authority to change the message.

(2) *Mixing plain and cryptographic text.* Never allow cryptographic
text with its equivalent plain language to appear in a crypto-
gram, and never mix plain and cryptographic text, *except in
messages where such mixtures are specifically permitted.* This
includes punctuation and abbreviations of any description. Such
messages afford valuable clues to the enemy. If a message is to
be cryptographed at all, it should be completely cryptographed.

(3) *Text of messages.*

(a) Never repeat in the clear the identical text of a message once
sent in cryptographic form, or repeat in cryptographic form
the text of a message once sent in the clear. Anything which
will enable an alert enemy to compare a given piece of plain
text with a cryptogram that supposedly contains this plain
text is highly dangerous to the safety of the cryptographic
system. Where information must be given out for publicity,
or where information is handled by many persons, the plain-
text version should be very carefully *paraphrased* before
distribution, to minimize the data an enemy might obtain
from an accurate comparison of the cryptographic text with
the equivalent, original plain text. To paraphrase a message
means to rewrite it so as to change its original wording as
much as possible without changing the meaning of the mes-

sage. This is done by altering the positions of sentences in the message, by altering the positions of subject, predicate, and modifying phrases or clauses in the sentence, and by altering as much as possible the diction by the use of synonyms and synonymous expressions. In this process, deletion rather than expansion of the wording of the message is preferable, because if an ordinary message is paraphrased simply by expanding it along its original lines, an expert can easily reduce the paraphrased message to its lowest terms, and the resultant wording will be practically the original message. It is very important to eliminate repeated words or proper names, if at all possible, by the use of carefully selected pronouns; by the use of the words "former," "latter," "first-mentioned," "second-mentioned"; or by other means. After carefully paraphrasing, the message can be sent in the other key or code.

(*b*) Never send the literal plain text or a paraphrased version of the plain text of a message which has been or will be transmitted in cryptographed form except as specifically provided in appropriate regulations.

(4) *Keys.* Never repeat in a different key or system, without paraphrasing, a cryptographed message which has once been transmitted, unless specifically authorized by the appropriate authority.

(5) *New cipher keys.* Never transmit a new cipher key by means of a message cryptographed in an old key.

(6) *Addresses or signatures.* Never place cryptographed addresses or signatures at the beginning or end of the cryptographed text. Bury them in the body of the message.

(7) *Identifying information.* Include in the address of a cryptographed message only the minimum information necessary for the message to reach the headquarters for which it is intended.

(8) *Replies.* Never reply to a cryptographed message in the clear.

(9) *Short titles.* Never use short titles as system or message indicators in cryptographed messages.

(10) *Dummy letters and padding.* Never use dummy letters or padding unless their use is specifically authorized.

(11) *System indicator.* Never encipher, encode, or disguise in any way the system indicator, unless specifically authorized.

(12) *Notations.* Never place on the cryptographed copy of a message any notations about the system or the subject matter of the message.

(13) *Work tables.* Never allow unnecessary materials such as books, documents, or papers to be on the work table during the process of cryptographing and decryptographing.

(14) *Filing messages.* Never file cryptographic messages and their equivalent plain text together. Work sheets must be destroyed by burning.

(15) *Check for accuracy.* Cryptographed messages should be checked for accuracy by decryptographing the message before transmission. Whenever practicable, this should be done by a cryptographer other than the one who originally cryptographed the message.

(16) *Safeguarding material.* Observe all rules of physical security established to safeguard the cryptographic material and message translations. Utmost care should be taken to prevent the loss or unauthorized sight of the codes or lists of cipher keys in use. It is possible to photograph an entire code in two or three hours. Mere continued possession of the cryptographic material is, therefore, no absolute guaranty that it has not been compromised by photography or some other method of reproduction. The only absolute assurance of its not having been compromised is that it has *never* left the possession of the person into whose care it has been entrusted or the safe in which it is kept when not in use. Even if knowledge that a code or cipher has been compromised follows immediately after such compromise, the amount of time and the difficulties involved in notifying all concerned and distributing new cryptographic material are so great that serious damage is caused by the delay and interruption in communication, not to speak of the danger resulting from the enemy's reading the most recent messages in the compromised system.

(17) *Reporting compromise.* Finally, it must be realized that the compromise or capture of cryptographic material is a most serious matter. If there is any reason to suspect that such material or related documents have been compromised, higher authority should be notified by the fastest means possible. Not only is such material available to the enemy for reading current and old messages, but also the cryptanalytic data afforded thereby become most useful in working on similar systems to replace the compromised one. The failure to notify higher authority promptly, if compromise is suspected, may jeopardize the lives of thousands of soldiers and is therefore more serious than permitting compromise to take place, if it could have been avoided. Regulations for reporting compromise should be carefully observed at all times.

PART TWO

ADVANCED MILITARY CRYPTOGRAPHY

CHAPTER 8

TRANSPOSITION SYSTEMS

Section I.   MONOPHASE TRANSPOSITION SYSTEMS

85. Transposition Systems Employing Geometric Designs

In part one brief mention was made of the use of geometric designs and figures other than rectangles in producing transposition ciphers. It was stated that triangles, trapezoids, and polygons of various symmetrical shapes can be employed. Figures of these types form connecting links between the methods that use simple rectangular designs and the more complicated methods that use figures in which transposition takes place along diagonals.

86. Trapezoidal Designs

a. A trapezoid or, more accurately, a truncated triangle, of pre-arranged dimensions as regards the number of cells (which in this case are rhombs into which it is to be partitioned, is constructed. There will be left on one side of the design a series of small triangles which are not to be used for inscribing letters, and are therefore crossed off in the design, as shown in figure 24. Only two agreements are necessary in order to fix the dimensions of the design: a keyword or keyphrase to determine the number of cells at the base of the design, and an understanding as to the height of the design expressed in number of cells. The successive horizontal rows of cells will decrease by one in number from bottom to top of the design. In figure 24, the keyphrase NO CANDY FOR ISSUE is used as a basis for deriving a numerical key of 15 elements, and it is assumed that by prearrangement it was agreed that the height of the design should be eight cells. Therefore, the bottom row has 15 cells, the next one upwards, 14, the next, 13, and so on, to the last, with 8 cells. The inscription may follow any route agreed upon; in the example, it follows the normal manner of writing. The transcription follows the numerical key order, yielding this cryptogram:

87

ODAIK AEDME HPODV ITEIP NHUET BOBRO
HDTFS EISNI ETBEF BCBTM ESHGA RTORD
IRERE AWARR ERTNS IEPVR VASEO FTEDL
NA

b. Decryptographing is merely the reverse of cryptographing, there being no difficulties provided that the design has been correctly constructed. For this purpose cross-section paper will be found useful. The analysis of such a cryptogram is somewhat complicated by the presence of columns having varying numbers of letters; it may be further complicated by following complex routes in inscription. It is also possible

7—9—2—1—8—3-15—5-10-11—6-12-13-14—4

N O C A N D Y F O R I S S U E
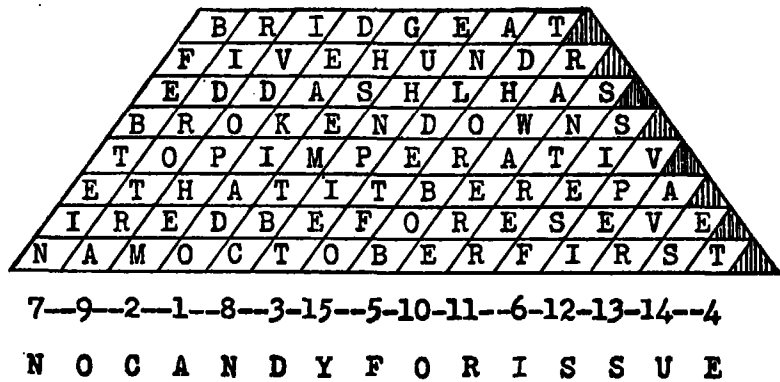
Figure 24.

to follow a numerical key in the inscription of the plain text in horizontal lines; this additional procedure would further complicate and delay solution.

87. Triangular Designs

a. The simplest way of drawing up a triangle for cryptographing is to take cross-section paper, draw a square the side of which is equal to the length agreed upon as expressed in the number of cells, and then draw a diagonal cutting the large square into two equal triangles. This is shown in figure 25, where the length agreed upon is nine, that is, nine cells per side. The letters of the plain text are inscribed in accordance with any prearranged route, the one illustrated in figure 26 being a simple method wherein the letters are inscribed in horizontal lines in the normal manner. When so inscribed, the letters in the diagram will form $2n - 1$ columns where n is the number of cells forming one of the sides of the square from which the triange has been constructed. The total number of letters that can be inscribed within
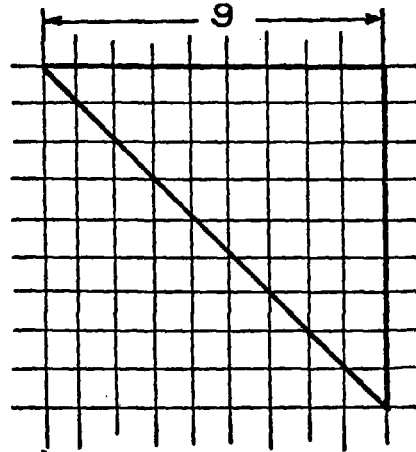
Figure 25.

the triangle is the sum of $n + (n - 1) + (n - 2 + (n - 3) + \ldots + 1$. For a triangle based upon a side of 9 cells, the sum is $9 + 8 + 7 + 6 + 5 + 4 + 3 + 2 + 1 = 45$. The letters may then be transcribed to form the cryptogram by following another route, or by following a derived numerical key applied to the base of the triangle. A simple method of deriving a key of $2n - 1$ elements from a key of n elements or letters is exemplified herewith. Let the key be DIAGONALS, a word of nine letters. Extend this key to $2n - 1$ places by repetition, and then assign numerical values as usual:

$$n = 9; \qquad\qquad\qquad\qquad 2\,n - 1 = 17$$

```
              1-2-3-4—5—6-7—8—9-10-11-12-13-14-15-16-17
Keyword:      D I A G O N A L S D I A G O N A L
Numerical key: 5-9-1-7-15-13-2-11-17—6-10—3—8-16-14—4-12
```

This numerical key is the one that has been employed in enciphering the message in Figure 26.

5--9--1--7-15-13--2-11-17--6-10--3--8-16-14--4-12
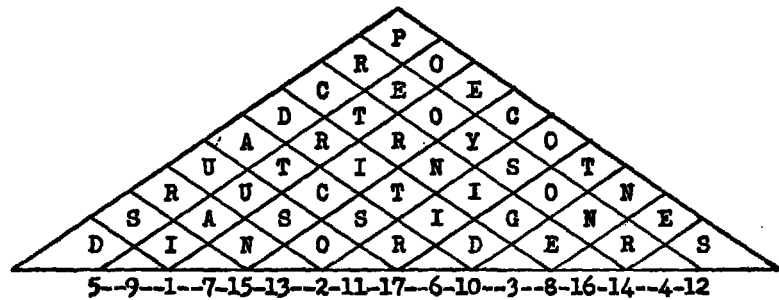
Cryptogram:

RICRC OCSGE DOONI UAOOE
SEYID RTISS DTSNR AUNTN
PERTR

Figure 26.
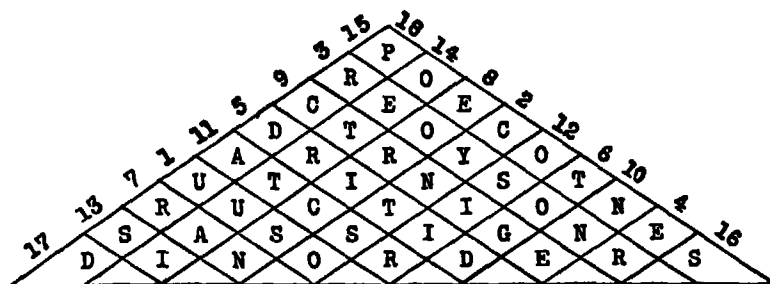
Cryptogram:

```
UUSOC YNTSO REOYS ONRER
DRITI DTOGD RANEO RICSN
CTRNI GENNE ATCSR OSIIR
SOIET RTUAI POECO TNESS
DPRCD AURSD
```

Figure 27.

b. By a slight change in procedure it is possible to encipher a message and produce a text which, for the sake of accuracy in special cases, is double the original length, but which is self-checking. Suppose that instead of applying a single numerical key to the base of the triangle, a double-length key is applied to the legs, as shown in figure 27. Here the key is TRIANGLES, extended to double length by simple repetition, as follows:

```
               1—2-3-4—5-6-7-8—9-10-11-12-13-14-15-16-17-18
Keyword:       T  R I A  N G L E S  T  R  I  A  N  G  L  E  S
Numerical key: 17-13-7-1-11-5-9-3-15-18-14—8—2-12—6-10—4-16
```

This key is applied to the legs of the triangle beginning at the lower left-hand corner. The transcription then follows key-number order, which results in doubling the length of the message but the repeated letters are scattered throughout the whole message. In decryptographing such a message the clerk merely omits the second occurrence of a letter if it agrees (in identity) with its first appearance in the text.

c. Many variations in inscription and transcription can be employed in the case of triangles as well as trapezoids. Some of the variations in the case of triangles are shown in figure 28.

88. Diagonal Methods

a. A method involving diagonal transposition which is reported to have been employed by the French Army in World War I is now to be described. A numerical key is derived from a fairly long word or phrase, and a rectangle is constructed, as in figure 29. The text is inscribed in this rectangle in normal fashion, nulls being employed, if necessary, to complete the last line of the rectangle.
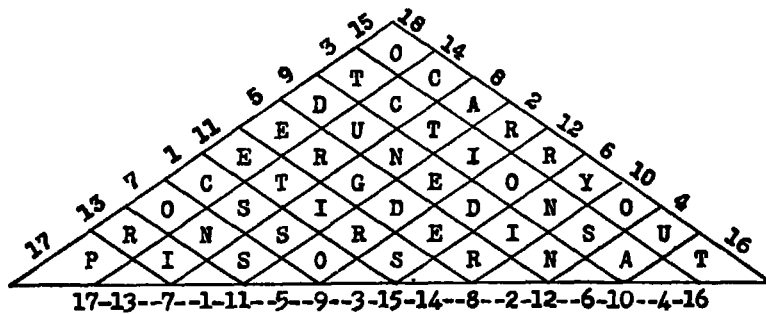
Inscription: Up left side, down right, alternately.

Transcription: (a) In rows from the base line, left to right and right to left, alternately, upwards:

PISOS RNATU SIERS etc.

(b) In diagonals from right leg, in key-number order:

RIEDR OUAYN etc.

(c) In rows from left leg, in key-number order:

CTGEO YTCEU etc.

(d) From columns in key-number order:

CNROI TUGRU etc.

Figure 28.

Message: ENEMY BATTERY LOCATED AT WOODS 1,000 YARDS SOUTHEAST OF MUMMASBURG HEAVY ARTILLERY STOP THEY ARE FIRING AT RATE OF THREE ROUNDS PER MINUTE FOR THE BATTERY X WILLS, MAJ.

Keyphrase: MIDNIGHT RIDE OF PAUL REVERE.

Enciphering diagram:

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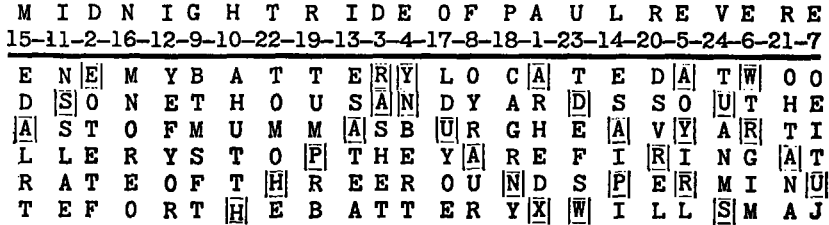
Cryptogram:

```
ADARR SESAR NUANX YAAPH HAURA UWYPW
RHEDO TETFS HETBE RTOIL TGIMO EITJO
YRURB TMSFT AHUTT NSLAE YEFYO RESTE
AESII EDLRT MNORE OLDYO ECAGR YTUMR
BDSVE LOHTN ATOMO ETEFS TANM
```

Figure 29.

b. The correspondents agree beforehand upon several diagonals which run from left to right, and from right to left and which intersect, thus cutting up the design quite thoroughly. In figure 29 let these selected diagonals be those indicated by the numbers from 1 to 6, inclusive, the odd ones indicating diagonals running from left to right. In the transcription, the letters along the indicated diagonals are first set down in groups of five, proceeding in key-number order. Correspondents must also agree beforehand as to whether a letter which lies at the intersection of two diagonals will be taken both times it is encountered or taken only once and, if so, whether on its first or second appearance. After all these letters have been written down, one then proceeds with the remaining letters in the usual columnar manner, omitting the letters which have already been taken. The cryptographing process will become clear upon the study of the example in figure 29.

89. Interrupted Keyword Transposition

a. This method of transposition is a development of a more simple method wherein the transposition follows a numerical key. The latter must first be described. A keyword or keyphrase of fair length is selected and a numerical key derived from it. Let this key be the phrase UNIFORMITY OF METHOD.

Keyphrase: U N I F O R M I T Y O F M E T H O D
Numerical key: 17-10-6-3-11-14-8-7-15-18-12-4-9-2-16-5-13-1

The plain text is then written out in horizontal lines corresponding to the length of the key; then transposition is effected *within each row*, according to the sequence of numbers applicable, as shown in figure 30.

Message: ADMINISTRATIVE ORDERS MUST BE COMPLETED AND READY TO ACCOMPANY FIELD ORDERS NOT LATER THAN 5:00 P.M. THIS DATE.

Enciphering diagram:

```
         17-10-6-3-11-14-8-7-15-18-12-4-9-2-16-5-13-1
         A  D  M  I  N  I  S  T  R  A  T  I  V  E  O  R  D  E
         R  S  M  U  S  T  B  E  C  O  M  P  L  E  T  E  D  A
         N  D  R  E  A  D  Y  T  O  A  C  C  O  M  P  A  N  Y
         F  I  E  L  D  O  R  D  E  R  S  N  O  T  L  A  T  E
         R  T  H  A  N  F  I  V  E  P  M  T  H  I  S  D  A  T
         E
```

Cryptogram:

```
         EEIIR MTSVD NTDIR OAAAE UPEME BLSSM
         DTCTR OYMEC ARTYO DACND OPNAE TLNAE
         DROID STOEL FRTIA TDHVI HTNMA FESRP
         E
```

Figure 30.

b. In the foregoing case the encipherment takes place only by transposition within rows, but it is possible to complicate the method by transposing, in addition, the rows as a whole, employing the same key or only a portion of it, as much as is required. Thus, if the message contained 18 rows of 18 letters each, then the transposition of rows could be effected according to key-number order, the last row being taken first (since the number 1 of the numerical key happens in this case to be at the end of the numerical key), the 14th row being taken second (since the number 2 of the numerical key is the 14th number), and so on. Where the message does not contain as many complete rows as there are numbers in the key, the transposition takes place in key-number order nevertheless, the rows being taken in the numerical order of the numbers present. Using the same key and message as in the foregoing case, the encipherment would be as shown in figure 31.

Enciphering diagram:

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

17:	A	D	M	I	N	I	S	T	R	A	T	I	V	E	O	R	D E
10:	R	S	M	U	S	T	B	E	C	O	M	P	L	E	T	E	D A
6:	N	D	R	E	A	D	Y	T	O	A	C	C	O	M	P	A	N Y
3:	F	I	E	L	D	O	R	D	E	R	S	N	O	T	L	A	T E
11:	R	T	H	A	N	F	I	V	E	P	M	T	H	I	S	D	A T
14:	E																

Cryptogram:

```
ETLNA EDROI DSTOE LFRYM ECART YODAC
NDOPN AAEUP EMEBL SSMDT CTROT IATDH
VIHTN MAFES RPEEE IIRMT SVDNT DIROA
A
```

Figure 31

c. From the preceding method it is but a step to the method of interrupted key transposition now to be described. Instead of writing the text in regular-length groups corresponding to the length of the key, it is written out in irregular groups the lengths of which vary according to some prearranged plan. For example, note the basis of the variable grouping in figure 32, which uses the same message and key as in *a* above.

d. This method may be combined with that shown in *b* above, thus further complicating the system. In decryptographing such a message it is best to use cross-section paper, block out the cells to be occupied by letters in the deciphering diagram, and indicate the key numbers applicable to each line. This will facilitate the process materially and help eliminate errors.

Enciphering diagram:

```
17-10—6—3-11-14—8—7-15-18-12—4—9—2-16—5-13—1
A  D  M  I  N  I  S  T  R  A  T  I  V  E  O  R  D  E
R  S  M  U  S  T  B  E  C  O  M  P  L  E  T  E  D  A
N  D  R  E  A  D  Y  T  O  A  C  C  O  M  P  A  N  Y
F  I  E  L  D  O  R  D  E  R  S  N  O  T  L  A  T  E
R  T  H  A  N  F  I  V  E  P  M  T  H  I  S  D  A  T
E
```

```
17-10—6—3-11-14—8—7-15-18-12—4—9—2-16—5-13—1
A  D  M  I  N  I  S  T  R  A  T  I  V  E  O  R  D  E
R  S  M  U  S  T  B  E  C  O  M  P  L  E  .  .  .  .
T  E  D  A  .  .  .  .  .  .  .  .  .  .  .  .  .  .
N  D  R  E  A  D  Y  T  O  A  C  C  .  .  .  .  .  .
O  M  P  A  N  Y  F  I  E  L  D  O  R  D  E  R  .  .
S  N  O  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
T  L  A  T  E  R  T  H  .  .  .  .  .  .  .  .  .  .
A  N  F  I  V  E  P  .  .  .  .  .  .  .  .  .  .  .
M  T  H  I  S  D  A  T  E (L  C  E  P)*. .  .  .  .
```

(*The four final letters LCEP are nulls, to complete the row.)

Cryptogram (columnar transposition in key-number sequence):

```
EEEDI UAEAT IIIPC OERRM MDRPO AFHTE
TIHTS BYFTP AVLRP DSEDM NLNTN SANEV
STMCD CDITD YREDR COEEO EARTN OSTAM
AOALL
```

Figure 32.

e. Another method of interrupted transposition is that which employs a rather long sequence of digits to control the interruption. In order to avoid the necessity of carrying around such a written sequence, it is possible to agree upon a number whose reciprocal when converted by actual division into its equivalent decimal number will give a long series of digits. For example, the reciprocal of 7, or 1/7, yields a repeating sequence of *six* digits: 142857142857 . . .; the reciprocal of 49, 1/49, yields a repeating sequence of 42 digits, etc. Zeros, when they appear, are omitted from the sequence. Suppose the number 19 is agreed upon, the reciprocal of which yields the sequence (0)52631578947368421. On cross-section paper mark off sets of cells corresponding in number to the successive digits. Thus:

```
   5        2      6       3   1      5
|_|_|_|_|X|_|X|_|_|_|_|_|X|_|_|X|_|X|_|_|_|_|
```
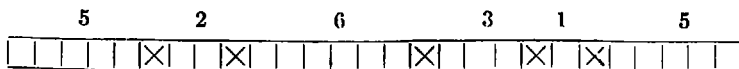
Let the message be ATTACK HAS BEEN POSTPONED.

Encipherment:

```
   5        2      6       3   1      5
|A|H|E|S|O|X|T|A|X|T|S|N|T|N|D|X|A|B|P|X|C|X|K|E|O|P|E|
```
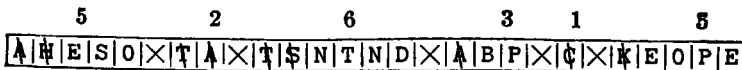
Cryptogram:

```
AHESO TATSN TNDAB PCKEO PE
```

f. To decryptograph such a message, the cryptogram is written down in a series of cross-section cells, which are then blocked off in sets according to the numerical key:

5	2	6	3	1	5

A|H|E|S|O|X|T|A|X|T|S|N|T|N|D|X|A|B|P|X|C|X|K|E|O|P|E
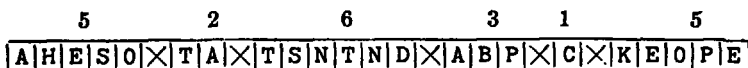
Taking the letters in consecutive order out of the successive sets, and crossing them off the series at the same time as they are being written down to construct the plain text, the message is found to begin with the following two words:

5	2	6	3	1	5

A|H|E|S|O|X|T|A|X|T|S|N|T|N|D|X|A|B|P|X|C|X|K|E|O|P|E
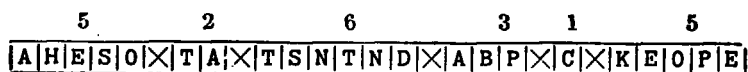
ATTACK HAS . . .

g. Preparatory to cryptographing, it is necessary to find the length of the message to be enciphered and then to mark off as many cells as will be required for encipherment. Nulls are used to fill in cells that are not occupied after enciphering the whole message. The secrecy of the method depends, of course, upon the reciprocal selected, but there is no reason why any fraction that will yield a long series of digits cannot be employed. If the selection of key numbers were restricted to reciprocals, the secrecy would be more limited in scope than is actually necessitated by the method itself.

90. Permutation Method

a. An old method, known in literature as the *aerial telegraphy method,*[1] forms the basis of this system. A set of permutations of 3 4, . . . 9 digits is agreed upon and these permutations are listed in a definite series. As an example, let these permutations be made of the digits 1 to 5, selecting only four of the possible 120. Suppose those selected are the following, set down in successive lines of the diagram in figure 33a:

Permutation

	2	3	1	5	4
2 3 1 5 4	2	3	1	5	4
3 2 5 1 4	3	2	5	1	4
1 5 3 2 4	1	5	3	2	4
4 3 1 5 2	4	3	1	5	2

Figure 33a.

[1] So named because it was first devised and employed in messages transmitted by a system of semaphore signaling in practical usage in Europe before the electrical telegraph was invented.

95

The letters of the plain text, taken in sets of fives, are distributed within the sections of the diagram in accordance with the permutations indicated above the sections and also at the left. Thus, the first five letters of the text, supposing them to be the initial letters of. the word RECOMMENDATIONS, are inserted in the following positions:

Permutation

2 3 1 5 4	2	3	1	5	4
	E	C	R	M	O

The next five letters are inscribed in the second line of the diagram in the sections indicated by the permutation above and at the left of the line. Thus:

Permutation

2 3 1 5 4	2	3	1	5	4
	E	C .	R	M	O
3 2 5 1 4	3	2	5	1	4
	N	E	A	M	D

This process is continued for each line and for as many lines as there are permutations indicated at the left. In the foregoing case, after twenty letters have been inserted, one inserts a second set of five letters again on the first line, placing the letters of this second set immediately to the right of those of the first set, respectively in key-number order. The succeeding lines are treated in similar fashion until the whole message has been enciphered. The following example will illustrate the process:

Message: RECOMMENDATIONS FOR LOCATION OF NEW BALLOON POSITIONS MUST BE SUBMITTED BEFORE 12TH AIRDROME COMPANY CHANGES COMMAND POST TOMORROW.

Enciphering diagram:

Permutation

2 3 1 5 4	2	3	1	5	4
	EASEOM	CTIDMA	RCOTRM	MOIECD	OITBEN
3 2 5 1 4	3	2	5	1	4
	NOSRPS	ESNOMO	ANUTNT	MNOFOP	DFMEAT
1 5 3 2 4	1	5	3	2	4
	TESWYO	SLSTNR	OBBLHO	IWTECM	NAEFAR
4 3 1 5 2	4	3	1	5	2
	LNIRCB*	ROMISC*	FLUHGO	OPTDOD*	OOBAEW

* The letters B, C, and D are nulls, to complete the figure.

Figure 33b.

The letters of the cipher text are taken from the diagram according to any prearranged route, the most simple being to transcribe the lines of letters in groups of fives, thus:

```
EASEO MCTID MARCO TRMNO IECDO ITBEN
NOSRP SESNO MOANU TNTMN OFOPD FMEAT
TESWY OSLST NROBB LHOIW TECMN AEFAR
LNIRC BROME SCFLU HGOOP TDODO OBAEW
```

b. The foregoing method when employed in its most simple form does not yield cryptograms of even a moderate degree of security; but if the method of inscription and transcription is varied and made more complex, the degree of security may be increased quite noticeably. It is possible to use longer permutations, based on sets of 6, 7, 8, or 9 digits, but in every case the successive permutations must be prearranged as regards both their exact composition and their order or arrangement in the diagram.

91. Transposition Method Using Special Figures

a. The method now to be described is useful only in special cases where the correspondence is restricted to brief communications between a very limited number of persons. It is necessary to agree in advance on certain particulars, as will be seen. Let the message to be enciphered be the following:

FOUR TRANSPORTS WILL BE COMPLETED BY END OF APRIL AND SIX MORE BY END OF JULY.

Note the following figures and encipherment:
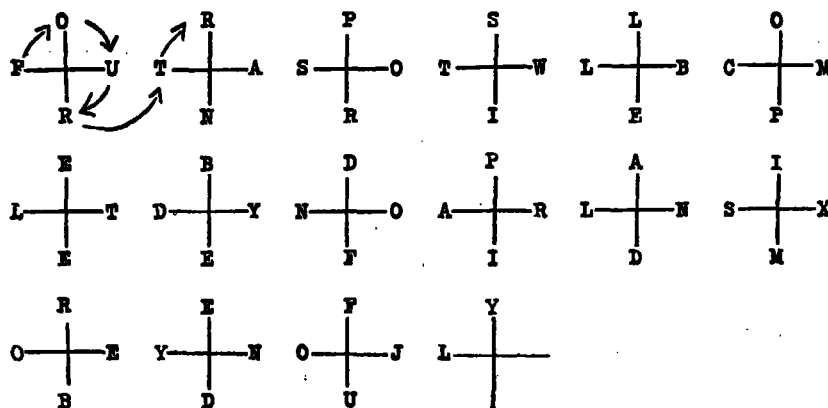
Cryptogram:

```
ORPSL OFUTA SOTWL BCMRN RIEPE BDPAI
LTDYN OARLN SXEEF IDMRE FYOEY NOJLB
DU
```

Figure 34.

b. It will be noted that it is essential to agree in advance not only upon the nature of the figure but also upon the *number* of figures per line.

c. The next series is a modification of the preceding. The same message will be employed, with a double-cross figure, five figures per line.
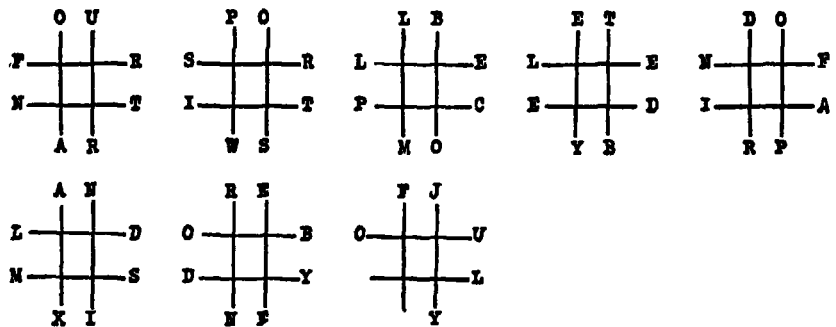
Cryptogram:

OUPOL BETDO FRSRL ELENF NTITP CEDIA
ARWSM OYBRP ANREF JLDOB OUMSD YLXIN
EY

Figure 35.

d. Still another series may be formed, as follows:
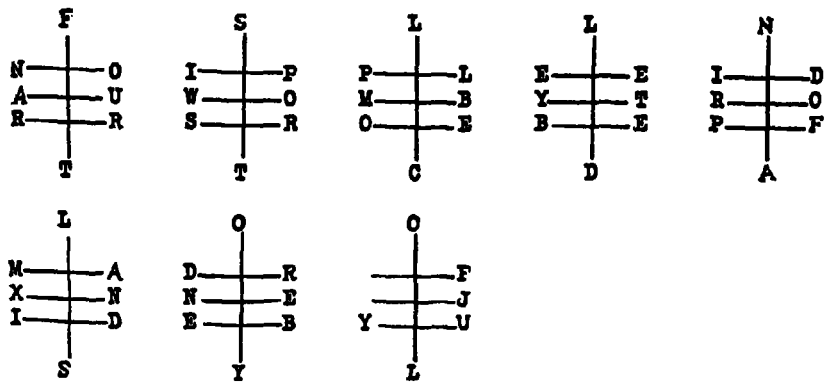
Cryptogram:

FSLLN NOIPP LEEID AUWOM BYTRO RRSRO
EBEPF TTCDA LOOMA DRFXN NEJID EBYUS
YL

Figure 36.

e. A figure of different form than the preceding forms the basis of the next type.

O O E D R T O Y R W P N N L E

F P B E U R C B T S M E A I L D S L T

F N R O P S B J I X E L
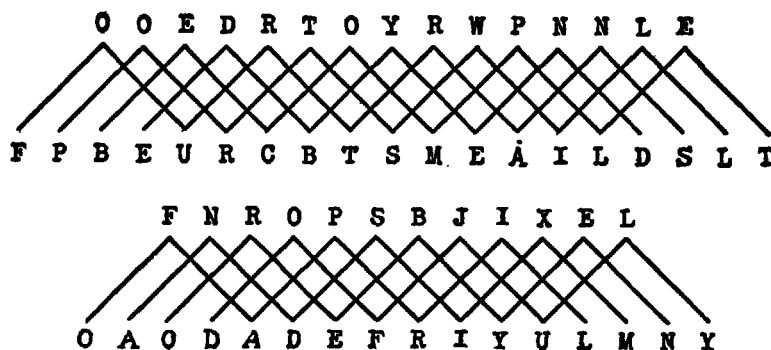
O A O D A D E F R I Y U L M N Y

Cryptogram:

OOEDR TOYRW PNNLE FPBEU RCBTS
MEAIL DSLTF NROPS BJIXE LOAOD
ADEFR IYULM NY

Figure 37.

f. From the foregoing examples, it is obvious that many other figures may be used for effective transpositions of this kind, such as stars of varying numbers of points, polygons of various symmetrical shapes, etc. It is merely necessary to agree upon the figures, the number of figures per line, the starting points of the inscription and transcription processes.

g. The method lends itself readily to combination with simple monoalphabetic substitution, yielding cryptograms of a rather high degree of security.

Section II. POLYPHASE TRANSPOSITION SYSTEMS

92. Polyphase Transposition Methods in General

a. In paragraph 33, brief mention was made of transposition systems in which two or more processes of rearrangement are involved. It was stated that only a very limited number of such transposition methods are practicable for military use, but that the degree of security afforded by them is considerably greater than that afforded by certain much more complicated substitution methods. The methods referred to are those which involve two or more successive transpositions, and merely for purposes of brevity in reference they will here be called *polyphase transposition methods* to distinguish them from the single monophase methods thus far described.

b. It is obvious that a polyphase transposition method may involve 2, 3, . . . successive transpositions of the letters of the plain text. To describe these methods in general terms, one may indicate that the letters resulting from a first transposition, designated as the T–1

transposition, form the basis of a second, or T–2 transposition. If the process is continued, there may be T–3, T–4 . . . transpositions, and each may involve the use of a geometric figure or design. For convenience, the design involved in accomplishing the T–1 transposition may be designated as the D–1 design; that involved in accomplishing the T–2 transposition as the D–2 design, etc. However, it may as well be stated at this point, that so far as military cryptography is concerned, methods which involve more than D–2 and T–2 elements are entirely impractical and often those which involve no more than D–2 and T–2 elements are also impracticable for such use.

93. True and False Polyphase Transpositions

a. It is possible to perform two or more transpositions with the letters of a text and yet the final cryptogram will be no more difficult to solve than if only a single transposition had been effected. The equivalent of this in the case of substitution ciphers is to encipher a monoalphabetic cryptogram by means of a second single alphabet; the final result is still a monoalphabetic substitution cipher. Likewise, if a message had been enciphered by a simple form of route transposition and a second and similar or approximately similar form of simple route transposition is again applied to the text of the first transposition, the final text is still that of a monophase transposition cipher. Again, two transpositions may be accomplished without really affecting a more thorough scrambling of the letters composing the original text. Examples will serve to clarify the differences between false and true polyphase transposition.

b. Note the following simple columnar transposition cipher prepared according to the method described in paragraph 27:

Message: DELIVER ALL AMMUNITION TO 4TH DIVISION DUMP

Keyword: SCHEDULE $= \dfrac{\text{S C H E D U L E}}{\text{7-1-5-3-2-8-6-4}}$

Enciphering rectangle:

7	1	5	3	2	8	6	4	
D	E	L	I	V	E	R	A	
L	L	A	M	M	U	N	I	
T	I	O	N	T	O	F	O	D–1
U	R	T	H	D	I	V	I	
S	I	O	N	D	U	M	P	

Cryptogram (T–1):

ELIRI VMTDD IMNHN AIOIP LAOTO RNFVM
DLTUS EUOIU

Figure 38.

100

In producing the foregoing cryptogram only the columns were transposed. Suppose that by prearrangement, using the keyword BREAK (derived numerical key = 2–5–3–1–4), the horizontal lines of the foregoing enciphering rectangle were also to be transposed. For example, let the horizontal lines of the rectangle D–1 be transposed immediately before taking the letters out of the columns of the design (in key-number order) to form the cipher text. Thus:

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

D–1

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

D–2
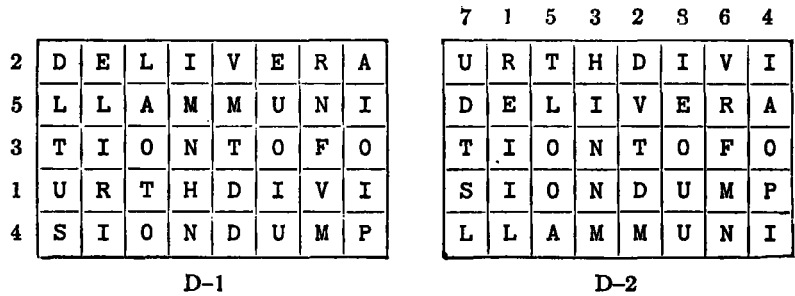
Cryptogram (T–2):

REIIL DVTDM HINNM IAOPI TLOOA VRFMN
UDTSL IEOUU

Figure 39.

c. The foregoing, however, is not a case of true polyphase or so-called *double* transposition. The same final result may be accomplished in a way which will at first glance appear quite different but is in reality one that accomplishes the same two operations by combining them in one operation. Let the message be inscribed as before, but this time with both numerical keys applied to the top and side of the rectangle. Then let another rectangle of the same dimensions, but with numbers in straight sequence instead of key-number sequence, be set alongside it. Thus:

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

D–1

	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								

D–2
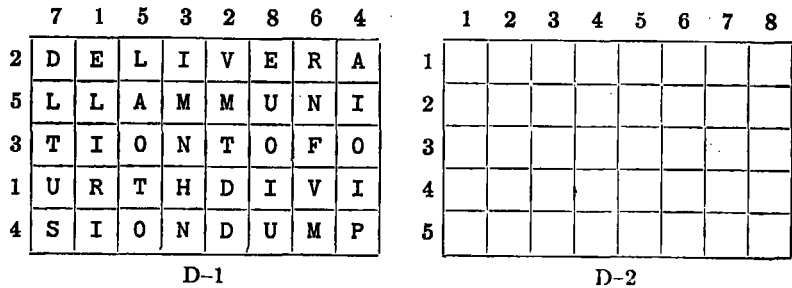
Figure 40.

Each letter D–1 is now transferred to that cell in D–2 which is indicated by the row and column indicators of the letter in D–1. For example, the first letter, D, of D–1, has the indicators 2–7 and it is placed in

the 2–7 cell in D–2; the second letter of D–1, which is E, is placed in the 2–1 cell of D–2, and so on. The final result is as follows:

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

D–1

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

D–2

Figure 41.

It will be seen that if the columns of D–2 are now read downwards in straight order from left to right the final cryptogram is identical with that obtained in figure 39: REIIL DVTDM, etc.

d. The foregoing cipher, often called the Nihilist Cipher, is referred to in some of the older literature as a double transposition cipher because it involves a transposition of both columns and rows; and indeed as described in *b* above it seems to involve a double process. It is, however, not an example of true double transposition. When the mechanism of this cipher is compared with that now to be described, the great difference in the cryptographic security of the two methods will become apparent.

94. True Double Transposition

In the form of the false double transposition described above, it is only entire columns and entire rows that are transposed. The disarrangement of the letters is after all not very thorough. In true double transposition this is no longer the case, for here the letters of columns and rows become so thoroughly rearranged that the final text presents a complete scrambling almost as though the letters of the message had been tossed into a hat and then drawn out at random.

Section III. TRUE DOUBLE TRANSPOSITION

95. True Double Transposition of the Columnar Type

a. It is by what is apparently a simple modification of certain of the columnar methods already described that an exceedingly good true double transposition can be effected. Let a numerical key be derived from a keyword in the usual manner and let the message be written out under this key to form a rectangle in the usual manner for columnar transposition. The length of the message itself determines the exact dimensions of the rectangle thus formed, and whether or not it is completely or incompletely filled.

b. In its most effective form the double transposition is based upon an incompletely filled rectangle; that is, one in which one or more cells in the last line remain unfilled. An example of the method now follows: Let the keyword be INTERNATIONAL; the message to be enciphered, as follows:

OUR ATTACK SLOWING UP IN FRONT OF HILL 1000 YARDS SOUTHEAST OF GOLDENVILLE STOP REQUEST PROMPT REENFORCEMENT.

Keyword: I N T E R N A T I O N A L
Derived numerical key: 4-7-12-3-11-8-1-13-5-10-9-2-6

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

D–1

4	7	12	3	11	8	1	13	5	10	9	2	6
A	N	N	D	G	O	P	N	O	T	U	T	N
U	N											

D–2

Figure 42a.

The first, or D-1, rectangle is inscribed in the usual manner of simple numerical key columnar transposition. It is shown as D-1 in the accompanying figure. *The letters of T-1 transposition* are then inscribed in the second, or D-2, rectangle *in the normal manner of writing,* that is, from left to right and from the top downwards. This is shown in D-2 of figure 42a for the first two columns of D-1 (in numerical key order) after transfer of their letters into D-2. The letters of the remaining columns of D-1 are transferred in the same manner into D-2, yielding the following rectangle:

4—7—12–3—11–8—1—13–5–10–9—2—6

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

Figure 42b.

For the T-2 text the letters are transcribed from the D-2 rectangle, reading down the columns in key-number order, and grouping the letters in fives. The cryptogram is as follows:

PTRUT OGTTI RLOPP DUSVO SOSAU AOREA
CORSH EEDNF WTULC NNEST QOFOY KFFHR
PUORA NTLTE LNLES GLOER OMONA IHIES
ENETN MDIT

e. In paragraph 29 a variation of the simple columnar key method of transposition was described. If the process therein indicated is repeated, double transposition is effected. The following example will serve to illustrate the method, using the same message and key as were used in the paragraph 29:

Message: REQUEST IMMEDIATE REENFORCEMENTS

Keyword: P R O D U C T
Derived numerical key: 4-5-3-2-7-1-6

Encipherment:

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

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

Cryptogram:

EREEE REFNM TASET SEIQO TMEIR
DUCMN

d. In some respects this modified method is simpler for the novice to perform correctly than is that employing rectangles. Experience has shown that many inexpert cryptographic clerks fail to perform the two transpositions correctly when D-1 and D-2 rectangles are employed in the work.

96. General Remarks on True Polyphase Transposition

a. The cryptographic security of the true double transposition method deserves discussion. Careful study of a cryptogram enciphered by the double transposition method set forth in paragraph 95 *b* and *c* will indicate that an extremely thorough scrambling of the letters is indeed brought about by the method. Basically, its principle is the splitting up of the adjacent or successive letters constituting the plain text by *two* sets of "cuts", the second of which is in a direction that is perpendicular to the first, with the individual "cuts" of both sets arranged in a variable and irregular order. It is well adapted for a regular and voluminous exchange of cryptograms between correspondents, because even if many messages in the same key are intercepted, *so long as no two messages are identical in length,* they can only be cryptanalyzed after considerable effort.

b. Triple and quadruple transpositions of the same nature are possible but not practical for serious usage. Theoretically, a continuation or repetition of the tranposition process will ultimately bring about a condition wherein the D-n rectangle is identical with the D-1 rectangle; in other words, after a certain number of transpositions the rectangle produced by a repetition of the *cryptographing* process results finally in *decryptographing* the message. Exactly how many repetitive transpositions intervene in such cases is extremely variable and depends upon factors lying outside the scope of this text.

c. In the example of cryptographing given in paragraph 95*b*, the D-1 and D-2 rectangles are identical in dimensions, and identical numerical keys are applied to effect the T-1 and T-2 transpositions. It is obvious, however, that it is not necessary to maintain these identities; D-1 and D-2 rectangles of different dimensions may readily be employed, and even if it is agreed to have the dimensions identical, the numerical keys for the two transpositions may be different. Furthermore, it is possible to add other variable elements. (1) The direction or manner of inscribing the letters in the D-1 rectangle may be varied; (2) the direction of reading off or taking the letters out of the D-1 rectangle in effecting the T-1 transposition, that is, in transferring them into the D-2 rectangle, may be varied; (3) the direction of inscribing these letters in the D-2 rectangle may be varied; (4) the direction of reading off or taking the letters out of the D-2 rectangle in effecting the T-2 transposition may be varied.

d. The solution of cryptograms enciphered upon the double transposition principle is often made possible by the presence of certain plain-text combinations, such as QU and CH (in German). For this reason, careful cryptographers substitute a single letter for such combinations, as decided upon by preagreement. For example, in one case the letter Q was invariably used as a substitute for the compound CH, with good effect.

Section IV. GRILLES AND OTHER TYPES OF MATRICES

97. Type of Cryptographic Grilles

Broadly speaking, cryptographic grilles[2] are sheets of paper, cardboard, or thin metal in which perforations have been made for the uncovering of spaces in which letters (or groups of letters, syllables, entire words) may be written on another sheet of paper upon which the grille is superimposed. This latter sheet, usually made also of cross-section paper, will hereafter be designated for purposes of brevity in reference as the *grille grid*, or *grid*. Its external dimensions are the same as those of the grille. Grilles are of several types depending upon their construction and manner of employment. They will be treated here under the titles of (1) simple grilles, (2) revolving grilles, (3) non-perforated grilles, and (4) "post card" grilles.

98. Simple Grilles

a. These consist usually of a square in which holes or apertures have been cut in prearranged positions. When the grille is superimposed upon

---

[2] Also often called "stencils." The general term *matrix* (plural, *matrices*) is very useful in referring to a geometric figure or diagram used for transposition purposes. Other terms in common use are *cage, frame, box,* etc.

the grid, these apertures disclose cells on the grid, in which cells letters, groups of letters, syllables, or entire words may be inscribed. An example is shown in figure 43. The four sides of the obverse surface of the grille are designated by the figures 1, 2, 3, 4; the four sides of the reverse surface, by the figures 5, 6, 7, 8. These figures are employed to indicate the position of the grille upon the grid in encipherment.

    b. (1) In cryptographing a message the grille is placed upon the grid, in one of the eight possible positions: Obverse surface up, with figure 1, 2, 3, or 4 at the top left; or reverse surface up, with
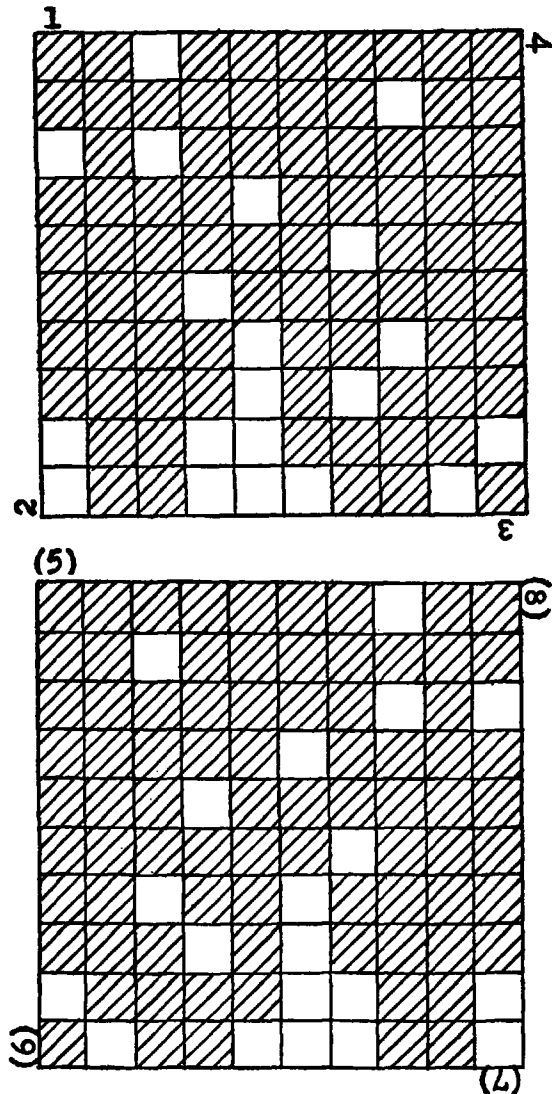
Figure 43.

figure 5, 6, 7, or 8 at the top left. The letters of the plain text are then inscribed in the cells disclosed by the apertures, following any prearranged route. In figure 44, the normal manner of writing, from left to right, and from the top downwards, has been followed in the inscription, the message being ALL DESTROYERS OUTSIDE.
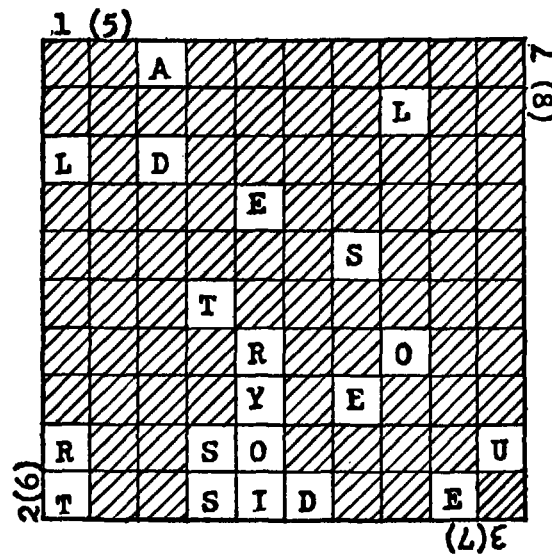
Figure 44.

(2) The transcription process now follows. The cipher text is written down, the letters being taken by following any pre-arranged route, which must be perpendicular to the route of inscription, otherwise the letters will follow in plain-text order. In the following, the route is by columns from left to right.

Cryptogram:

LRTAD TSSER YOIDS ELOEU

(3) If the number of letters of the plain-text message exceeds the number of cells disclosed by one placement of the grille, the letters given by this placement are written down (in cryptographic order), and then the grille is placed in the next position on a fresh grid; the process is continued in this manner until the entire message has been cryptographed. The several sections of the cipher letters resulting from the placements of the grille on successive grids merely follow each other in the final cryptogram. In this manner of employment it is only necessary for the correspondents to agree upon the initial position of the grille and its successive positions or placements.

c. It is obvious that by the use of a simple grille the letters of a message to be cryptographed may be distributed within an enveloping message consisting mostly of "dummy" text, inserted for purposes of enabling the message to escape suppression in censorship. For example, suppose the grille shown in figure 43 is employed in position 1 and the message to be conveyed is ALL DESTROYERS OUTSIDE. The letters of this message are inscribed in their proper places on the grid, exactly as shown in figure 44. An "open" or disguising text is now to be composed; the latter serving as an envelope or "cover" for the letters of the secret text, which remain in the positions in which they fall on the grid. The open or disguising text, in other words, is built around or superimposed on the secret text. Note how this is done in figure 45, with an apparently innocent message reading:

I HAVE WORKED VERY WELL ALL DAY, TRYING TO GET
EVERYTHING STRAIGHTENED UP BEFORE GOING ON MY
NEXT TRIP SOUTH, BUT INSIDE TEN DAYS . . .

1 (5)

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

4 (8)

2 (6)

3 (7)

Figure 45.

d. The foregoing method naturally requires the transmission of considerably more text than is actually necessary for conveying the message intended. Where questions of censorship are not involved, the method is therefore impractical. A modification of the method suggests itself in the use of a transparent sheet of paper superimposed upon a square or other figure in which the individual cells are irregularly numbered and the inscription process follows the sequence of numbers. An example is shown in figure 46, using the message ROCK CREEK BRIDGE WILL BE DESTROYED WHEN TAIL HAS CROSSED.

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

a

W	C	T	E	H	O	E	E
R	I	E	S	R	R	S	W
E	L	R	B	S	B	Y	G
N	I	E	C	D	K	E	L
O	T	E	D	C	S	R	I
O	L	D	H	D	A	A	K

b

Figure 46.

The transcription may now follow any prearranged route. The normal method of reading would produce the cryptogram beginning WCTEH OEERI, etc. It is obvious that the correspondents must possess designs with identically numbered cells.[3]

99. Revolving Grilles

a. In this type of grille (see fig. 47a) the apertures are also formed by perforating a sheet of cross-section paper according to prearrangement, but these apertures are so distributed that when the grille is turned four times successively through angles of 90° and set in four *grille positions* on the grid, all the cells on the grid are disclosed in turn. (The preparation of such grilles is discussed in par. 103.) If letters are inserted in the cells so disclosed, then after a complete revolution of the grille every one of the cells of the grid will contain a letter and thus the grid will be completely filled. For this reason such a grille is also called a *self-filling,* or an *automatic-completion* grille. The secrecy of messages enciphered by its means is dependent upon the distribution or position of the apertures, the sequence of grille positions on the grid, that is, whether in the order 1, 2, 3, 4 clockwise; or 1, 3, 4, 2 etc.), and the route followed in inscribing and transcribing the letters in the cells of the grid. For each position of the grille, one-fourth the total number of letters of the text is inscribed; hence it is convenient to refer to "sections" of the text, it being understood that each section consists of one-fourth the total number of letters.

b. There are two possible procedures so far as the inscription-transcription sequence is concerned. (1) The letters of the plain text may be inscribed in the cells of the grid through the apertures disclosed by the grille and then, when the grid has been completely filled, the grille removed, and the letters transcribed from the grid according to a prearranged route; or, (2) the letters of the plain text may first be inscribed in the cells of the grid according to a prearranged route and then the grille applied to the completely-filled grid to give the sequence of letters

---

[3] The system employed by the French Army in 1886 was of the nature here described.

REF ID:A56932
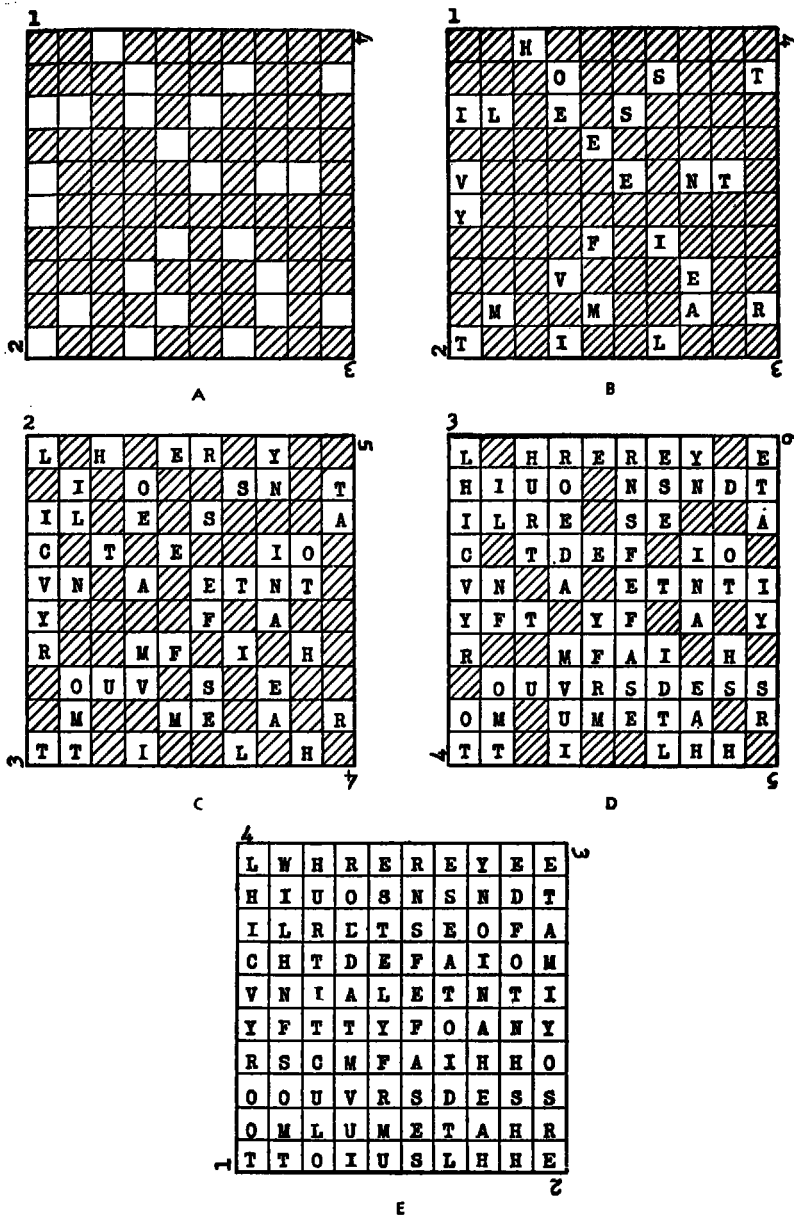
Cryptogram:

```
LHICV YROOT WILHN FSOMT
HURTI TCULO ROEDA TMVUI
ESTEL YFRMU RNSFE FASES
ESEAT OIDTL YNOIN AHEAH
EDFOT NHSHH ETAMI YOSRE
```

Figure 47.

111

forming the cipher text of the transcription process. The first method will be described in *c* below; the second in *e* below.

c. Taking the simplest manner of inscribing the letters, that is, from left to right and from the top downwards, the letters of the first section of the text are inscribed in the cells disclosed by the apertures, the grille being in the first position. This is shown in b of figure 47. The grille is then given ¼ turn clockwise, bringing figure 2 to the top left. If the grille has been correctly prepared, none of the cells disclosed in the second grille position on the grid will be occupied by a letter. The letters of the second section are then inscribed, this being shown in c of figure 47. In d and e of figure 47, the results of inscribing the third and fourth sections, respectively, are shown. The letters of the cryptogram are then taken out of the completed grid by following any prearranged route of transcription. The cryptogram below has been transcribed by following down the columns in succession from left to right.

d. To decryptograph such a message, the cipher letters are inscribed columnwise in a grid 10 by 10 (that is, one composed of 100 cells, 10 per side) and then the grille applied to the square in four consecutive positions corresponding to those used in cryptographing. The letters disclosed by each placement of the grille are written down as they appear, section after section.

e. The second manner of employing a revolving grille is merely the reciprocal of the first. The procedure followed in the first method to *decryptograph* a message is followed in the second method to *cryptograph* a message; and the procedure followed in the first method to cryptograph is followed in the second method to decryptograph.

100. Grilles of Other Geometric Forms

Grilles are not limited to square-shaped figures. They may be equilateral triangles, pentagons, hexagons, and so on. Any figure which can be pivoted upon a central point and which when revolved upon this pivot can be placed in a succession of homologous positions over a grid corresponding to the grille will serve equally well. A triangle affords three grille positions, a pentagon, five, and so on.

101. Polyphase Transposition by Grilles

One grille may be employed to inscribe the letters of the message on the grid, and a second, and different, grille employed to transcribe them from the grid to form the final text of the cryptogram. This would constitute a real double transposition method of great complexity. Polyphase transposition by a series of grilles is of course possible.

112

102. Increasing the Security of Revolving Grilles

a. The total number of letters which a grille will exactly encipher is termed its *capacity*. If the number of letters of a message is always equal to the total capacity of the grille, this information is of great aid in solution by the enemy. For example, a message of 64 letters indicates a grille 8 by 8 with 16 apertures; one of 144 letters, a grille 12 by 12 with 36 apertures, and so on. There are, however, methods of employing a grille so that it will serve to encipher messages the lengths of which are greater or less than the capacity of the grille.

b. When the total number of letters is less than the capacity of the grille, no modification in method of use is necessary. Encipherment of such a message comes to a close when the last plain-text letter has been inscribed. In decryptographing such a message, the recipient must strike out, on the grid upon which he is to inscribe the cipher text, a number of cells corresponding to the difference between the number of letters of the text as received and the total capacity of the grille. The location of the cells to be thus eliminated must be prearranged, and it is best usually to strike them off from the final positions of the grid.
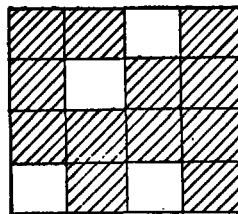
15	29	1	30	19	33	5	
42	2	16	43	46	6	20	
17	44	31	18	21	47	34	
3	32	4	45	7	35	8	
25	38	11	39	22	36	9	
50	12	26	51	48	10	23	
27	52	40	28	24	49	37	
13	41	14					

a

b

Figure 48.

c. When the total number of letters is equal to or greater than the capacity of the grille, a grid of greater capacity than that of the grille can be prepared, on which the grille may be positioned several times, thus forming a large or composite grid composed by the juxtaposition of the several small grids. If there are a few cells in excess of the actual number required, these may be struck off from the large grid at prearranged points, for example, from the last column and row, as shown in b of figure 48. The grille is then placed in its first position in turn on each of the component grids, then in its second position, and so on. An example will serve to illustrate. A message of fifty-two letters is to be

enciphered with the grille shown in a of figure 48, the capacity of which is sixteen letters. The number of letters of the message being greater than three times sixteen, the composite grid must be composed of four small grids containing a total of sixty-four cells. Therefore, twelve of these cells must be eliminated. These are shown in b of figure 48, together with the number indicating the positions occupied by the letters of the text.

103. Construction of Revolving Grilles

a. There are several ways of preparing revolving grilles, of which the one described below is the most simple. All methods make use of cross-section paper.

b. Suppose a revolving grille with a capacity of 100 letters is to be constructed. The cells of a sheet of cross-section paper 10 by 10 are numbered consecutively in *bands* from the outside to the center, in the manner shown in a of figure 49. It will be noted that in each band, if n is the number of cells forming one side of the band, the highest number assigned to the cells in each band is $n - 1$.

c. It will be noted that in each band there is a quadruplication of each digit; the figure 1 appears four times, the figure 2 appears four times, and so on. From each receding band there is to be cut out $(n-1)$ cells: from the outermost band, therefore, nine cells are to be cut out; from the next band, seven; from the next, five; from the next, three; and from the last, one cell. In determining specifically what cells are to be cut out in each band, the only rules to be observed are these: (1) One and only one cell bearing the figure 1 is to be cut out, one and only one cell bearing the figure 2 is to be cut out, and so on; (2) as random a selection as possible is to be made among the cells available for selection for perforation. In b of figure 49 is shown a sample grille prepared in this way.

d. If the side of the grille is composed of an odd number of cells, the innermost band will consist of but one cell. In such case this central cell must not be perforated.

e. It is obvious that millions of differently perforated grilles may be constructed. Grilles of fixed external dimensions may be designated by indicators, as was done by the German Army in 1915 when this system was employed. For example, the FRITZ grille might indicate a 10 by 10 grille, serving to encipher messages of about 100 letters; the ALBERT grille might indicate a 12 by 12 grille, serving to encipher messages of about 144 letters, and so on. Thus, with a set of grilles of various dimensions, all constructed by a central headquarters and distributed to lower units, systematic use of grilles for messages of varying lengths can be afforded.

f. A system for designating the positions of the perforated cells of a grille may be established between correspondents, so that the necessity

114

for physical transmission of grilles for intercommunication is eliminated. An example of a possible system is that which is based upon the co-ordinate method of indicating the perforations. The columns from left to right and the rows from bottom to top are designated by the letters A, B, C, . . . Thus, the grille shown in b of figure 49 would have the following formula:

ADG; BBEH; CDJ; DEG; EACH; FFI; GE; HBDHJ; IDG; JABFI.

1	2	3	4	5	6	7	8	9	1
9	1	2	3	4	5	6	7	1	2
8	7	1	2	3	4	5	1	2	3
7	6	5	1	2	3	1	2	3	4
6	5	4	3	1	1	2	3	4	5
5	4	3	2	1	1	3	4	5	6
4	3	2	1	3	2	1	5	6	7
3	2	1	5	4	3	2	1	7	8
2	1	7	6	5	4	3	2	1	9
1	9	8	7	6	5	4	3	2	1

a
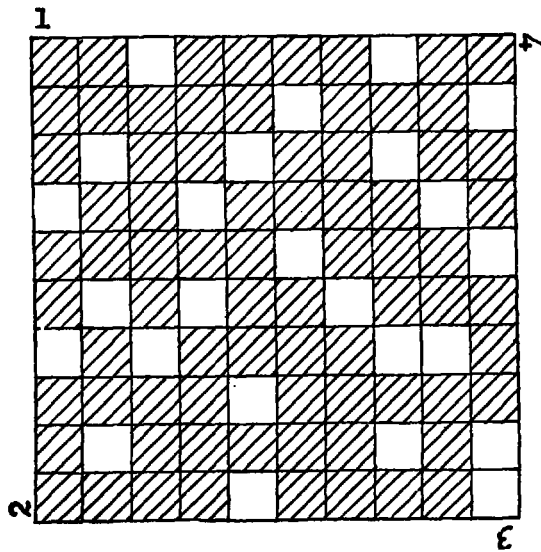
b

Figure 49.

g. Given the formula, the eight corners of the grille can be labeled in various ways by prearrangement; but the simplest method is that shown in connection with b of figure 49. Then the initial position of the grille can be indicated by the number which appears at the upper left-hand corner when the grille is placed on the grid, ready for use. Thus, position 1 indicates that the grille is in position with the figure 1 at the upper left-hand corner; position 3, with the figure 3 at the upper left-hand corner, etc.

h. The direction of revolving the grille can be clockwise or counter-clockwise, so that correspondents must make arrangements beforehand as to which direction is to be followed.

i. Revolving grilles can be constructed so that they have two operating faces, an obverse and a reverse face. They may be termed *revolving-reversible* grilles. The principles of their construction merely involve a modification of those described in connection with ordinary revolving grilles. A revolving-reversible grille will have eight possible placement indicators; usually positions 1 and 5, 2 and 6, and so forth, correspond in this obverse-reverse relationship, as shown in figure 43.

j. The principles of construction described above apply also to grilles of other shapes, such as triangles, pentagons, and so forth.

104. Nonperforated Grilles

a. All the effects of a grille with actual perforations may be obtained by the modified use of a nonperforated grille. Let the cells that would normally be cut out in a grille be indicated merely by crosses thereon, and then on a sheet of cross-section paper let the distribution of letters resulting from each placement of the grille on a grid be indicated by inserting crosses in the appropriate cells, as shown in figure 50.

Grille   Grille Position
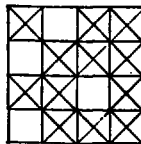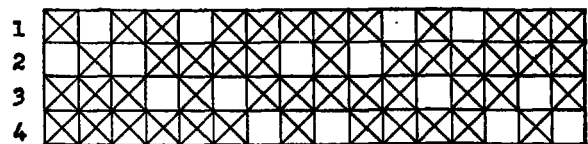
Figure 50a.   *Figure 50b.*

b. Note should be made of the fact that in figure 50b the distribution of crosses shown in the third row of cells is the reverse of that shown in the first; the distribution shown in the fourth row is the reverse of that shown in the second. This rule is applicable to all revolving grilles and is of importance in solution.

c. If the letters of the text are now inscribed (normal manner of writing) in the cells not eliminated by crosses, and the letters transcribed

from *columns* to form the cryptogram, the results are the same as though a perforated grille had been employed. Thus:

Cryptogram:

EWCRA EOLDA RDDAT Y

Figure 50c.

d. It is obvious that a numerical key may be applied to effect a columnar transposition in the foregoing method, giving additional security.

e. The method is applicable to grilles of other shapes, such as triangles, pentagons, hexagons, octagons, etc.

f. In figure 50c it is noted that there are many cells that might be occupied by letters but are not. It is obvious that these may be filled with nulls so that the grid is completely filled with letters. Long messages may be enciphered by the superposition of several diagrams of the same dimensions as figure 50c.

105. Rectangular or "Post Card" Grilles

a. The grille shown in figure 51 differs from the ordinary revolving grille in that (1) the apertures are rectangular in shape, and are greater in width, thus permitting of inscribing several letters in the cells disclosed on the grid by each perforation of the grille; and (2) the grille itself admits of but two positions with its obverse side up and two with its reverse side up. In figure 51 the apertures are numbered in succession from top to bottom in four series, each applying to one position of the grille; the numbers in parentheses apply to the apertures when the grille is reversed; the numbers at the corners apply to the four positions in which the grille may be placed upon the grid.

b. One of the ways in which such a grille may be used is to write the first letter of the text at the extreme left of the cell disclosed by aperture 1, the second letter, at the extreme left of the cell disclosed by aperture 2, and so on. The grille is retained in the same position and the 17th letter is written immediately to the right of the 1st, the 18th immediately to the right of the 2d, and so on. Depending upon the width of the aperture, and thus of the cells disclosed on the grid, 2, 3, 4 . . . letters may be inserted in these cells. When all the cells have been filled, the grille may then be placed in the second position, then the third, and finally, the fourth.

117
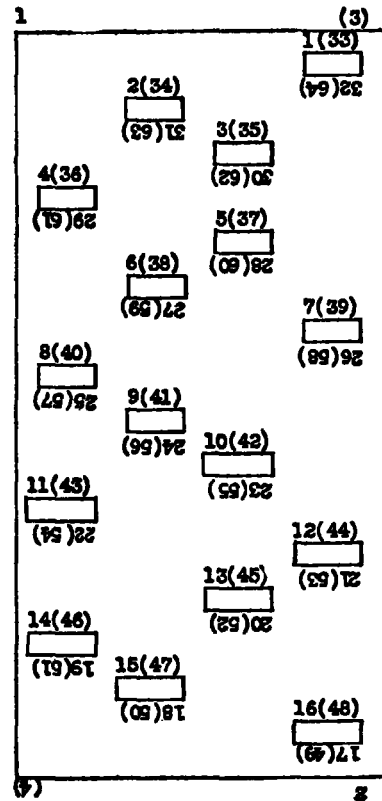
Figure 51.

c. Another way in which the grille may be used is to change the position of the grille after the 16th letter has been inserted, then after the 32d, 48th, and 64th; the 65th letter is then inserted to the right of the 1st, the 81st, to the right of the 17th, and so on until the grid is completed.

d. Whole words may, of course, be inserted in the cells disclosed by the apertures, instead of individual letters, but the security of the latter method is much lower than that of the former.

e. The text of the grid may be transcribed (to form the cryptogram) by following any prearranged route.

f. The successive positions of a post card grille may be prearranged. The order 1, 2, 3, 4 is but one of 24 different sequences in which it may be superimposed upon the grid.

g. A modification of the principles set forth in paragraph 103, dealing with the construction of revolving grilles, is applied in the construction of rectangular or "post card" grilles. Note the manner in which the cells in a of figure 51 are assigned numbers; homologous cells in each band receive the same number. In a of figure 52 there are three bands,

118

numbered from 1 to 8, 9 to 16, and 17 to 24. Then in each band one
and only one cell of the same numbered set of four cells is cut out. For
example, if cell 1a is selected for perforation from band 1 (as indicated
by the check mark in that cell), then a cross is written in the other three
homologous cells, 1b, c, and d, to indicate that they are not available for
selection for perforation. Then a cell bearing the number 2 in band 1
is selected, for example, 2c, and at once 2a, b, and d are crossed off as
being ineligible for selection, and so on. In c of figure 52 is shown a
grille as finally prepared, the nonshaded cells representing apertures.

h. The grille, c of figure 52, is a "six-column" one, that is, the cells
form six columns. It is obvious that grilles with any even number of
columns of cells are possible. The number of apertures in each band
should be equal and this number multiplied by the number of bands and
then by 4 should equal the capacity of the grille. In the case of the one
shown in c of figure 52, the capacity is 8 by 3 by 4 or 96 cells; this is
the same as is obtained merely by multiplying the height (in cells) by the

Figure 52.

number of columns, 16 × 6 = 96. If four letters are inscribed in each rectangle, the capacity of the grille in terms of letters is 384. The grid in this case would, after completion, present 24 columns of letters, to which a numerical key for a second transposition can be applied in transcription to produce the final text of the cryptogram.

106. Indefinite or Continuous Grilles

a. In his *Manual of Cryptography,* Sacco illustrates a type of grille which he has devised and which has elements of practical importance. An example of such a grille is shown in figure 53. This grille contains 20 columns of cells, and each column contains 5 apertures distributed at random in the column. There are therefore 100 apertures in all, and this is the maximum number of letters which may be enciphered in one position of the grille. The plain text is inscribed vertically, from left to right, using only as many columns as may be necessary to inscribe the complete message. A 25-letter message would require but 5 columns. To form the cryptogram the letters are transcribed *horizontally* from the rows, taking the letters from left to right as they appear in the apertures. If the total number of letters is not a multiple of 5, sufficient nulls are added to make it so. In decryptographing, the total number of letters is divided by 5, this giving the number of columns employed. The cipher text is inscribed from left to right and top downwards in the apertures in the rows of the indicated number of columns and the plain text then reappears in the apertures in the columns, reading downward and from left to right. (It is, of course, not essential that nulls be added in the encipherment to make the length of the cryptogram an exact multiple of 5, for the matter can readily be handled even if this is not done. In decipherment the total number of letters divided by 5 will give the number of complete columns; the remainder left over from the division will give the number of cells occupied by letters in the last column on the right.)
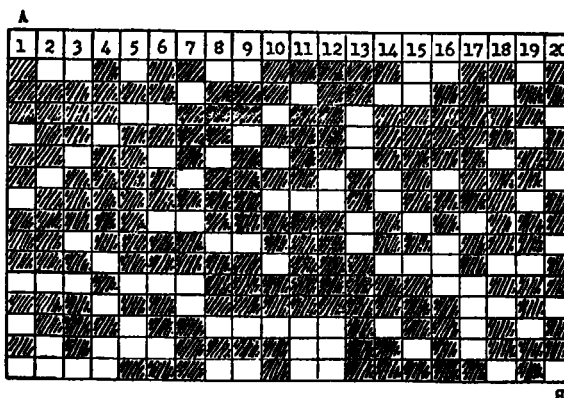
Figure 53a.

b. Such a grille can assume 4 positions, two obverse and two reverse. Arrangements must be made in advance as to the sequence in which the various positions will be employed. That is why the grille shown in figure 53a has the position-designating letter "A" in the upper left-hand corner and the letter "B" (upside down) in the lower right-hand corner. On the obverse side of the grille would be the position-designating letters "C" and "D."

c. Figure 53b shows how a message is enciphered.

Message:

AM RECEIVING HEAVY MACHINE GUN FIRE FROM HILL SIX TWO ZERO.

Figure 53b.

Cryptogram:

EGIIX FNNEA YTHFL RIRMO IOLWE MERVA ERMAH EGSOA ICUEC NVHIZ.

(The letters E and A in the 10th column are nulls. Columns 11 to 20 are not used at all, the irregular right-hand edge of the grille merely indicating that this portion of the grille remains vacant.)

Section V. MISCELLANEOUS TRANSPOSITION SYSTEMS

107. Complex Route Transposition

a. In figure 54 a route for inscribing letters within a rectangle is indicated by a sequence of numbers. The initial point may be at any of the four corners of the rectangle, or it may be at any other point, as prearranged. The letters may be inscribed to form the rectangle by following the route indicated and then transcribed from the rectangle to form the cryptogram by following another route; or the letters may be inscribed according to one route and transcribed accordingly to the numerical route indicated.

b. A variation of the foregoing is that illustrated in figure 55, wherein the inscription follows the route shown by the arrows. The initial point

of inscription is indicated by the figure 1, and the final point, by the figure 2.

c. In the foregoing case, the route is a succession of the moves made by the king in the game of chess; it forms the so-called "king's tour", in which the playing piece makes a complete or reentrant journey covering all cells of the chessboard, each cell being traversed only once. A route composed of a succession of moves made by the knight, or the so-called "knight's tour", is also possible, but in order to be practical a grid with the cells numbered in succession would have to be prepared for the correspondents, since millions of different reentrant knight's tours can be constructed[4] on a chessboard of the usual 64 cells.

90	61	60	31	30	1
2	29	32	59	62	89
88	63	58	33	28	3
4	27	34	57	64	87
86	65	56	35	26	5
6	25	36	55	66	85
84	67	54	37	24	7
8	23	38	53	68	83
82	69	52	39	22	9
10	21	40	51	70	81
80	71	50	41	20	11
12	19	42	49	72	79
78	73	48	43	18	13
14	17	44	47	74	77
76	75	46	45	16	15

Figure 54.
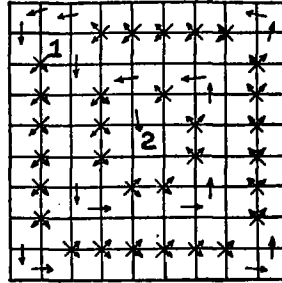
Figure 55.

108. Transposition of Groups of Letters, Syllables, and Words

There is nothing in the previously described methods which precludes the possibility of their application to pairs of letters, sets of three or more letters, or even syllables and whole words. Nor, of course, is their use limited to operations with plain text they may be applied as secondary steps after a substitutive process has been completed (see sec. I, ch. 10).

109. Disguised Transposition Methods

a. The system often encountered in romances and mystery stories, wherein the message to be conveyed is inserted in a series of nonsignificant words constructed with the purpose of avoiding or evading suspicion, is a species of this form of "open" cryptogram involving transposition. The "open" or enveloping, apparently innocent text may be designated as the *external text;* the secret or cryptographic text may be designated as the *internal text.* A complicated example of external or open and internal or secret text is that shown in paragraph 98.

---

[4] See Ball, W. W. R., Mathematical Recreations and Essays, London, 1928.

b. Little need be said of the method based upon constructing external text the letters of which, at prearranged positions or intervals, spell out the internal text. For example, it may be prearranged that every fourth letter of the external text forms the series of letters for spelling out the internal text, so that only the 4th, 8th, 12th ... letters of the external text are significant. The same rule may apply to the complete words of the external text, the *n*, *2n*, *3n*, ... words form the internal text. The preparation of the external text in a suitable form to escape suspicion *is not so easy as might be imagined,* when efficient, experienced, and vigilant censorship is at work. Often the paragraph or passage containing the secret text is sandwiched in between other paragraphs added to pad the letter as a whole with text suitable to form introductory and closing matter to help allay suspicion as to the presence of secret, hidden text.

c. A modification of the foregoing method is that in which the 1st, 3d, 5th, ... words of a secret message are transmitted at one time or by one agency of communication, and the 2d, 4th, 6th, ... words of the message are transmitted at another time or by another agency of communication. Numerous variations of this scheme will suggest themselves, but they are not to be considered seriously as practical methods of secret intercommunication.

d. Two correspondents may agree upon a specific size of paper and a special diagram drawn upon this sheet, the lines of which pass through the words or letters of the internal text as they appear in the external text. For example, the legs of an equilateral triangle drawn upon the sheet of paper can serve for this purpose. This method is practicable only when messages can be physically conveyed by messenger, by the postal service, or by telephotographic means. Many variations of this basic scheme may perhaps be encountered in censorship work.

110. Cipher Machines for Effecting Transposition

These may be dismissed with the brief statement that if any exist today they are practically unknown. A few words are devoted to the subject in paragraph 147.

CHAPTER 9

SUBSTITUTION SYSTEMS

Section I. POLYGRAPHIC SYSTEMS

111. General

a. It will be recalled that chapter 3 dealt with the various types of cipher alphabets, simple monoalphabetic substitution, monoalphabetic substitution with variants, the more simple varieties of polyalphabetic substitution, cipher disks, and cipher tables. The following material on substitution is a continuation of the former, a thorough understanding of which is a requisite to the examination of the more complex types of substitution now to be set forth.

b. First it will be advisable to explain several terms which will be used. Substitution methods in general may be described as being *monoliteral* or *polyliteral* in character. In the former there is a strict letter-for-letter replacement, or, to include numerical and symbol methods, there is a "one-to-one" correspondence between the length of the units of the plain text and those of the cipher text, no matter whether the substitution is monoalphabetic or polyalphabetic in character. In polyliteral methods, however, this "one-to-one" correspondence no longer holds. A combination of two letters, or of two figures, or of a letter and a figure, may represent a single letter of the plain text; there is here a "two-to-one" correspondence, two characters of the cipher text representing one of the plain text. The methods described in chapter 3, fall under the latter designation; the cipher equivalents there shown are, properly speaking, bipartite in character. Tripartite cipher equivalents are also encountered. Polyliteral methods, therefore, are said to employ *polypartite alphabets,* of which the bipartite type is by far the most common. Further on in this text, polyliteral methods of greater complexity than those illustrated in chapter 3 will be discussed. Attention now will be directed more particularly to a different type of substitution designated as *monographic* and *polygraphic* substitution.

112. Monographic and Polygraphic Substitution

a. All the methods of substitution heretofore described are monographing in nature, that is, in the enciphering process the individual units subjected to treatment are single letters; there is a letter-for-letter substitution, or, to include numerical and symbol methods, there is, as in the

case of monoliteral substitution, a "one-to-one" correspondence between units of the plain text and those of the cipher text. In polygraphic substitution, however, *combinations* of letters of the plain text, considered as indivisible compounds, constitute the units for treatment in encipherment. If the units consist of pairs of plain-text letters, the encipherment is pair-for-pair, and is said to be *digraphic* in character; if the units consist of sets of three letters, it is *trigraphic* in character, and so on. There is still a "one-to-one" correspondence involved, but the units in these cases are composite in character and the individual elements composing the units affect the cipher equivalents *jointly*, rather than separately. The basic important factor in true polygraphic substitution is that *all* the letters of the group participate in the determination of the cipher equivalent of the group; the identity of *each* letter of the plain-text group affects the composition of the *whole* cipher group. Thus, in a certain digraphic system AB_p may be enciphered as XP_c, and AC_p, on the other hand, may be enciphered as NK_c; a difference in the identity of but one of the letters of the plain-text pair here produces a difference in the identity of *both* letters of the cipher pair.

b. For practical usage polygraphic substitution is limited to the handling of digraphs and trigraphs, although very occasionally groups of more than three letters may be employed for special purposes.

c. The fundamental purpose of polygraphic substitution is the suppression or rather the elimination of the frequency characteristics of ordinary plain text. It is these frequency characteristics which lead, sooner or later, to the solution of practically all substitution ciphers. When the substitution involves only individual letters in a monoalphabetic system, the cryptogram can be solved very quickly; when it involves individual letters in a polyalphabetic system, the cryptogram can usually be solved, but only after a much longer time and much more study, depending upon the complexity of the method. The basic principle in the solution, however, is to reduce the polyalphabetic text to the terms of monoalphabetic ciphers and then to solve the latter. In true polygraphic substitution on the other hand, the solution does not rest upon the latter basis at all because it is not a question of breaking up a complex text into simpler elements; it rests, as a rule, upon the possibility of analysis on the basis of the frequency of the polygraphic units concerned. If the substitution is digraphic, then the units are pairs of letters and the normal frequencies of plain-text pairs become of first consideration; if the substitution is trigraphic, the units are sets of three letters and the normal frequencies of plain-text trigraphs are involved. In the last two cases the data that can be employed in the solution are meager, and are far from definite or unvarying in their significance, and that is why solution of polygraphic substitution ciphers is often extremely difficult.

d. Just as in typography, when certain combinations of letters, such as fi, fl, and ffi, are mounted on one and the same piece of type, they are

called logotypes or ligatures, so in cryptography, when combinations of two or more letters are to be treated as a unit in a cryptographic process, they may also be called ligatures and can be conveniently indicated as being so by placing a bar across the top of the combination. Thus, $\overline{CO}_p$ represents the digraph CO of the plain text. It will also be convenient to use the Greek letter θ to represent a letter of the alphabet, without indicating its identity. Thus, instead of the circumlocution "any letter of the plain text", the symbol θ_p will be used; and for the expression "any letter of the cipher text", the symbol θ_c will be used. The symbol $\overline{\theta\theta}_p$ then means "any plain-text digraph"; the symbol $\overline{\theta\theta}_c$ "any cipher-text diagraph." To refer specifically to the 1st, 2d, 3d . . . member of a ligature, the exponent 1, 2, 3 . . . will be used. Thus, θ^2_p of $\overline{REM}_p$ is the letter E; θ^3_c of $\overline{XRZ}_c$ is Z.

TABLE I

(Showing only a partially filled table)

Final Letter (θ^2_p)

	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	A
B	NY	DC	NB	ZI	XX	DX						...				B
C				AH				AB				...		ND		C
D			BB		YA					AY		...	BF			D
E	AX					AI						...				E
F		AG				NZ		AZ				...	AA			F
N		BC		CY								...		BA	FE	N
X					AC					AJ		...	BE			X
Y	DE					AF						...		AD		Y
Z	AE								BD			...	AK			Z
	A	B	C	D	E	F	G	H	I	J	K		X	Y	Z	

Initial letter (θ^1_p)

113. Polygraphic Substitution by Means of Tables

a. The most simple method of effecting polygraphic substitution involves the use of tables similar to that shown in table I. This table merely presents equivalents for digraphs and is to be employed upon the coordinate system, θ^1_p of $\overline{\theta^1\theta^2}_p$ being sought in the column at the left or right, θ^2_p in the row at the top or bottom. The cipher pair, $\overline{\theta^1\theta^2}_c$, is

then found at the intersection of the row and column thus indicated. For example, $\overline{AF}_p = \overline{YG}_c$; $\overline{FH}_p = \overline{AZ}_c$, etc.

b. Table I is reciprocal in nature; that is, $\overline{AF}_p = \overline{YG}_c$ and $\overline{YG}_p = \overline{AF}_c$. Thus, a single table serves for enciphering as well as for deciphering. The word DEFEND would be enciphered as YA NZ CY, and then grouped in fives: YANZC Y . . . . When a final single letter occurs, a null is added in order to make a pair of letters capable of being enciphered by the method. Reciprocity is, however, not an essential factor and for greater security nonreciprocal tables are more advisable. In such cases an enciphering table must have its complementary deciphering table.

c. Until the amount of text enciphered by means of such a table becomes great enough to disclose the cipher equivalents of the most frequently used digraphs, such as EN, ER, RE, TH, ON, etc., crypto-grams based upon the table are relatively secure against solution.

d. A simple method for preventing the establishment of the frequencies characterizing these commonly used digraphs and thus eliminating the principal basis for their identification is given in paragraph 134*e*.

e. The factor that contributes most to the relatively high degree of security of the digraphic method described in *a* and *b* above is the absence of symmetry in the table employed; for this table is constructed by random assignment of values and shows no symmetry whatsoever in its arrangement of contents. Hence, even if θ^1_p in a first case of $\overline{\theta^1\theta^2}_p = \overline{\theta^1\theta^2}_c$ is identical with θ^1_p in a second case, $\overline{\theta^1\theta^2}_c$ in the first case is wholly different from $\overline{\theta^1\theta^2}_c$ in the second case. For example, table I shows that $\overline{AC}_p = \overline{XE}_c$ and $\overline{AD}_p = \overline{YY}_c$; the cipher resultants fail to give any hint that the plain-text pairs contain an identical letter.

f. If, however, the latter is not the case and the table exhibits symmetry in its arrangement of contents, solution is somewhat facilitated. Note table II, for example, in which two mixed sequences are employed to form the cipher equivalents. One mixed sequence is based upon the keyphrase WESTINGHOUSE AIR BRAKE; the other, upon the keyphrase GENERAL ELECTRIC COMPANY. The word FIRE would be enciphered as KIQA.

g. A cursory examination of table II shows that when θ^2_p is identical in two cases then θ^2_c is identical in these cases, so that in reality the encipherment is by no means truly digraphic in character. Described in cryptographic terms, the encipherment of θ^1_p is polyalphabetic in character whereas that of θ^2_p is monoalphabetic. A more obvious picture of this condition is brought out in the rearrangement of table II.

h. By a slight modification in arrangement but with no change in basic principle, the encipherment can be made monoalphabetic so far as θ^1_p is concerned, and polyalphabetic so far as θ^2_p is concerned. Note table IV.

TABLE II

θ^2_D

	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	HX	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	PW	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

i. The results given by table III or table IV may be duplicated by using sliding alphabets, as shown in figures 56 and 57. In the former, which corresponds to table III, alphabets I and IV are fixed, II and III are mounted upon the same strip, which is movable. To use these alphabets in encipherment, θ^1_p of $\overline{\theta^1\theta^2}_p$ is located on alphabet II and alphabets II–III are shifted so that θ^1_p is beneath A on alphabet I; θ^2_p is now sought in alphabet I and $\overline{\theta^1\theta^2}_c$ will be found under it on alphabets III and IV, respectively. Thus, for the word FIRE the successive positions of the alphabet strips are as shown below, yielding the cipher resultant KIQA.

$$\overline{FI}_p = \overline{KI}_c$$

I—ABCDEFGHIJKLMNOPQRSTUVWXYZ ....Fixed alphabet
II—FGHIJKLMNOPQRSTUVWXYZABCDE
III—NGHOUARBKCDFJLMPQVXYZWESTI } ....Movable alphabet
IV—GENRALCTIOMPYBDFHJKQSUVWXZ ....Fixed alphabet

$$\overline{RE}_p = \overline{QA}_c$$

I—ABCDEFGHIJKLMNOPQRSTUVWXYZ ....Fixed alphabet
II—RSTUVWXYZABCDEFGHIJKLMNOPQ
III—JLMPQVXYZWESTINGHOUARBKCDF } ....Movable alphabet
IV—GENRALCTIOMPYBDFHJKQSUVWXZ ....Fixed alphabet

Figure 56.

TABLE III

θ^2_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	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z
B	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W
C	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E
D	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S
E	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T
F	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I
G	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N
H	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G
I	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H
J	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O
K	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U
L	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A
M	B	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R
N	K	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B
O	C	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K
P	D	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C
Q	F	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D
R	J	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F
S	L	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J
T	M	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L
U	P	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M
V	Q	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P
W	V	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q
X	X	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V
Y	Y	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X
Z	Z	W	E	S	T	I	N	G	H	O	U	A	R	B	K	C	D	F	J	L	M	P	Q	V	X	Y

θ^2_c G E N R A L C T I O M P Y B D F H J K Q S U V W X Z

j. To correspond with table IV the alphabet strips are arranged as shown in figure 57. Here alphabets I and II are fixed, III and IV are mounted upon the same movable strip. To use these alphabets in encipherment, θ^2_p of $\overline{\theta^1\theta^2}_p$ is located on alphabet IV and alphabets III–IV are shifted so that θ^2_p (I_p) is beneath A on alphabet I; θ^1_p (F_p) is now sought in alphabet I and $\overline{\theta^1\theta^2}_c$ will be found under it on alphabets II and III, respectively. Thus, for the word FIRE, the successive positions of the alphabet strips are as shown below, yielding the cipher resultant NBJU.

$$\overline{FI}_p = \overline{NB}_c$$

I—ABCDEFGHIJKLMNOPQRSTUVWXYZ.............Fixed alphabet
II—WESTINGHOUARBKCDFJLMPQVXYZ.............Fixed alphabet
III—IOMPYBDFHJKQSUVWXZGENRALCT ⎫
IV—IJKLMNOPQRSTUVWXYZABCDEFGH ⎬ ....Movable alphabet

$$\overline{RE}_p = \overline{JU}_c$$

I—ABCDEFGHIJKLMNOPQRSTUVWXYZ.............Fixed alphabet
II—WESTINGHOUARBKCDFJLMPQVXYZ.............Fixed alphabet
III—ALCTIOMPYBDFHJKQSUVWXZGENR ⎫
IV—EFGHIJKLMNOPQRSTUVWXYZABCD ⎬ ....Movable alphabet

Figure 57.

TABLE IV

θ^2_p

$\theta^1_p \, \theta^1_c$	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
A W	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z
B E	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G
C S	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E
D T	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N
E I	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R
F N	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A
G G	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L
H H	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C
I O	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T
J U	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I
K A	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O
L R	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M
M B	Y	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P
N K	B	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y
O C	D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B
P D	F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D
Q F	H	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F
R J	J	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H
S L	K	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J
T M	Q	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K
U P	S	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q
V Q	U	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S
W V	V	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U
X X	W	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V
Y Y	X	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W
Z Z	Z	G	E	N	R	A	L	C	T	I	O	M	P	Y	B	D	F	H	J	K	Q	S	U	V	W	X

k. Neither table III nor table IV presents the possibilities such tables might afford for digraphic substitution. They may, however, be rearranged so as to give results that will approach more closely to the desired ideal as to nonrelationship between cipher equivalents of plain-text pairs having an identical letter in common. Note that in table V, which is based upon the same primary alphabets as table III and table IV, the cipher equivalents are the same as in the latter tables, but they have been so distributed as to eliminate the undesirable and externally obvious relationship referred to. (In any table of this nature there can be only 676 different pairs of equivalents, since the table presents merely the permutations of the 26 letters taken two at a time. It is the distribution of the pairs which is important.)

l. Table V still shows symmetry in its construction, and a suspicion of its existence formed during the preliminary stages of cryptanalysis would aid materially in hastening final solution.

m. The foregoing tables have all been digraphic in nature, but a kind of false trigraphic substitution may also be accomplished by means of such tables, as illustrated in the accompanying table VI, which is the same as table V with the addition of one more alphabet at the top of the table.

n. In using this table, θ^1_p is located in alphabet I, and its equivalent, θ^1_c, taken from alphabet II; θ^2_p is located in alphabet III, and its equivalent, θ^2_c, taken from alphabet IV; θ^3_c is the letter lying at the intersection of the row indicated by θ^3_p in alphabet I and the column determined by θ^2_p. Thus, FIRE LINES would be enciphered NNZ IEQ KOV. It is obvious, however, that only the encipherment of θ^3_p is polyalphabetic in character; θ^1_p and θ^2_p are enciphered purely monoalphabetically. Various other agreements may be made with respect to the alphabets in which the plain-text letter will be sought in such a table, but the basic crypto-graphic principles are the same as in the case described.

o. Digraphic tables employing numerical equivalents instead of letter equivalents are, of course, possible but in this case the number of equivalents required, 676, means that combinations of three figures must be used.

TABLE V

$$\theta^2_p$$

θ^3_p

Each cell below contains two letters (upper/lower). They are written here as upper/lower.

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

TABLE VI

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

Section II. MATRIX[5] DIGRAPHIC SUBSTITUTION

114. Disadvantages of Large Tables

Digraphic substitution by means of tables such as those illustrated in tables I, II, and V is impractical for military use because of the relatively large size that the table takes, and the inconvenience in their production, change, distribution, and handling. Just as it has been noted in section VI, chapter 3, that simple sliding alphabet strips can replace large quadricular tables, so it will be found that small matrices similar to a checkerboard can replace the large quadricular tables in digraphic substitution.

115. Four-Alphabet Matrix

a. The simple or single-alphabet matrix consists of a square 5 by 5, containing 25 cells in which the letters of a 25-element alphabet (I and J

---

[5] The word *matrix* as herein employed refers to "checkerboard" diagrams smaller than the quadricular tables illustrated in section I. These matrices usually comprise sections of 25 cells each.

being interchangeable) are inserted in any prearranged order. When four such matrix alphabets are arranged in a large square as shown in figure 58, the latter may be employed for digraphic substitution to yield the same cipher results as does the much larger table I. In this square, θ^1_p of $\overline{\theta\theta}_p$ is sought in section 1; θ^2_p, in section 2. Thus, θ^1_p and θ^2_p will always form the northwest-southeast corners of an imaginary rectangle delimited by these two letters as located in these two sections of the square. Then θ^1_c and θ^2_c are, respectively, the letters at the northeast-southwest corners of this same rectangle. Thus, $\overline{TG}_p = \overline{TK}_c$; $\overline{WD}_p = \overline{TX}_c$; $\overline{OR}_p = \overline{PS}_c$; $\overline{UR}_p = \overline{WP}_c$, etc. In decryptographing, θ^1_c and θ^2_c are sought in sections 3 and 4, respectively, and their equivalents, θ^1_p and θ^2_p, noted in sections 1 and 2, respectively. It may, of course, be prearranged that θ^1_p should be sought in the section now labeled 3, θ^2_p, in that labeled 4, whereupon θ^1_c would be located in the section now labeled 1, θ^2_c, in that now labeled 2.

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

Sec. 1 (θ^1_p) — Sec. 3 (θ^1_c) — Sec. 4 (θ^2_c) — Sec. 2 (θ^2_p)

Figure 58.

b. It is possible to construct a digraphic substitution matrix that shows reciprocity in its $\overline{\theta\theta}_p = \overline{\theta\theta}_c$ relationship so that if $\overline{AB}_p = \overline{XY}_c$, for example, then $\overline{XY}_p = \overline{AB}_c$. Two conditions are essential to assure reciprocity. These are taken into consideration in the establishment of the $\overline{\theta^1\theta^2}_c$, or deciphering sections, and an example will serve to explain the process.

c. Two enciphering alphabets are first constructed; one in section 1 for θ^1_p, the other in section 2 for θ^2_p, as shown in figure 59a. The alphabet in section 3 is now to be constructed. Any horizontal row of section 1 is taken, for example, the row labeled 1, consisting of the letters BWGRM, and these letters are written on any horizontal row of section

Sec. 1 (θ^1_p) ... **Sec. 3 (θ^1_c)**

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

Sec. 4 (θ^2_c) ... **Sec. 2 (θ^2_p)**, bottom columns 1 2 3 4 5

Figure 59a.

Sec. 1 (θ^1_p) ... **Sec. 3 (θ^1_c)** — top order 1 2 3 4 5 | 5 2 4 1 3

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

Sec. 4 (θ^2_c) ... **Sec. 2 (θ^2_p)**, bottom columns 1 2 3 4 5

Figure 59b.

3, in any transposed order, which is immediately written at the top of section 3, as shown in figure 59b.

Row 1 of section 1 was inserted in row 4 of section 3. The reciprocal permutation of 1 4 is 4 1, and therefore row 4 of section 1 must now be inserted in row 1 of section 3, and in the transposed order 5–2–4–1–3, as indicated at the top of section 3. The result is shown in figure 59c. Then

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

Sec. 1 (θ^1_D) — Sec. 3 (θ^1_c) — Sec. 4 (θ^2_c) — Sec. 2 (θ^2_D)

Figure 59c.

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

Sec. 1 (θ^1_D) — Sec. 3 (θ^1_c) — Sec. 4 (θ^2_c) — Sec. 2 (θ^2_D)

Figure 59d.

row 2 of section 1 is transferred to another row of section 3, for example, the fifth, and the letters inserted in the already indicated transposed order. Immediately thereafter, in order to continue the reciprocal permutation relationship, row 5 of section 1 becomes row 2 of section 3. This leaves row 3 of section 1 to become also row 3 of section 3, and to be reciprocal to itself. The result is shown in figure 59d, where section 3 is

completely constructed. The foregoing principle of permutation reciprocity applies equally to the rows of section 4. Suppose the permutation 3-5-1-4-2 is decided upon for the rows of section 4. This means that rows 1 and 3 of section 2 become rows 3 and 1 of section 4; rows 2 and 5 of section 2 become 5 and 2 of section 4; row 4 of section 2 becomes row 4 of section 4. As regards the transposed order within the rows of section 4, the following rule applies: The letters forming a complete column from the top of section 3 to the bottom of section 2, whatever their order, must also form a complete column from the top of section 1 to the bottom of section 4. For example, the column designated by the number 5 of section 3 contains the letters OHKMECOSGT; column 5 of section 1 contains five of these letters, MEKOH; therefore, the completed column must contain the letters, COSGT but in the transposed order given by the permutation selected for the rows of section 4, namely, 3-5-1-4-2.

The completed matrix is then as shown in figure 59e, and exhibits reciprocity throughout. Example: $\overline{BB}_p = \overline{LW}_c$, and $\overline{LW}_p = \overline{BB}_c$.

	1	2	3	4	5	5	2	4	1	3	
1	B	W	G	R	M	O	P	A	U	L	4
2	N	Y	V	X	E	H	Z	Q	D	F	5
Sec. 1 (θ^1_p) 3	S	I	C	T	K	K	I	T	S	C	3 Sec. 3 (θ^1_c)
4	U	P	L	A	O	M	W	R	B	G	1
5	D	Z	F	Q	H	E	Y	X	N	V	2
3	W	A	L	E	S	C	X	K	P	B	1
5	F	H	U	I	T	O	M	Y	D	V	2
Sec. 4 (θ^2_c) 1	P	X	B	K	C	S	A	E	W	L	3 Sec. 2 (θ^2_p)
4	N	Z	R	Q	G	G	Z	Q	N	R	4
2	D	M	V	Y	O	T	H	I	F	U	5
	4	2	5	3	1	1	2	3	4	5	

Figure 59e.

d. The total number of reciprocal permutations of five elements is 25, as follows:

Base 12345

(1) 12354	(6) 14325	(11) 21354	(16) 34125	(21) 45312
(2) 12435	(7) 14523	(12) 21435	(17) 35142	(22) 52341
(3) 12543	(8) 15342	(13) 21543	(18) 42315	(23) 52431
(4) 13245	(9) 15432	(14) 32145	(19) 43215	(24) 53241
(5) 13254	(10) 21345	(15) 32154	(20) 42513	(25) 54321

137

Since the row permutations of sections 2 and 4 are independent, the total number of different four-alphabet matrices as regards row permutations is $25^2 = 625$. Taking into account the column permutations, $5 \times 4 \times 3 \times 2 \times 1$ in number, it is therefore possible to have 625×120 or 75,000 different, four-alphabet matrices of this nature, based upon the same two alphabets in sections 1 and 3. With changes in the latter, the number, of course, becomes very much greater.

116. Two-Alphabet Matrices

a. It is possible to effect digraphic substitution with a matrix consisting of but two sections by a modification in the method of finding equivalents. In the checkerboard shown in figure 60, $\theta^1{}_p$ of $\overline{\theta^1\theta^2}{}_p$ is located in the square at the left, $\theta^2{}_p$, in the square at the right.

$\theta^1{}_p\theta^2{}_c$

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

$\theta^2{}_p\theta^1{}_c$

Figure 60.

When $\overline{\theta^1{}_p\theta^2}{}_p$ are at the opposite ends of the diagonal of the imaginary rectangle defined by the letters, $\overline{\theta^1\theta^2}{}_c$ are at the opposite ends of the other diagonal of the same rectangle, just as in the preceding case. For example, $\overline{AL}_p = \overline{TT}_c$; $\overline{DO}_p = \overline{GA}_c$; $\overline{AT}_p = \overline{TA}_c$; $\overline{EH}_p = \overline{HE}_c$.

b. Reciprocity may be imparted to the two-alphabet matrix by reciprocal permutation of the rows of the squares, no attempt being made to effect any reciprocal permutation of columns. Figure 61 shows such a matrix. Here, for example, $\overline{AW}_p = \overline{OT}_c$ and $\overline{OT}_p = \overline{AW}_c$; $\overline{BA}_p = \overline{DL}_c$ and $\overline{DL}_p = \overline{BA}_c$, etc.

c. In two-alphabet matrices in which one section is directly above the other, reciprocity already exists without special preparations for its

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

Figure 61.

M	A	N	U	F
C	T	R	I	G
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
C	D	F	G	H
K	N	P	Q	R
V	W	X	Y	Z

Figure 62.

production. In figure 62, $MO_p = UA_c$ and $UA_p = MO_c$; $MA_p = MA_c$ and $MA_c = MA_p$. When both $\theta^1{}_p$ and $\theta^2{}_p$ happen to be in the same column, there is no encipherment[6], a fact which constitutes an important disadvantage of this method. This disadvantage is only slightly less obvious in the preceding cases where the cipher equivalent of such a case of $\overline{\theta^1\theta^2}_p$ consists merely of the plain-text letters in reversed order, yielding $\overline{\theta^2\theta^1}_c$.

117. One-Alphabet Matrices; Playfair Cipher

a. Limiting the matrix to one alphabet and modifying the method of finding equivalents gives the basis for a well-known system called the Playfair Cipher, which was not invented by Lord Lyon Playfair but by Sir Charles Wheatstone. It was used for many years as a field cipher in the British Army. For a short time, 1917–18, it was prescribed as a field cipher for use in the United States Army. The modification in the method of finding cipher equivalents has been found useful in imparting a greater degree of security than that afforded in the preceding types of matrix methods. Figure 63 shows a typical Playfair square. The usual method of encipherment can be best explained by examples given under four categories:

(1) Members of the plain-text pair, $\theta^1{}_p$ and $\theta^2{}_p$, are at opposite ends of the diagonal of an imaginary rectangle defined by the two letters; the members of the cipher-text pair, $\theta^1{}_c$ and $\theta^2{}_c$, are at the opposite ends of the other diagonal of this imaginary rectangle. Examples: $\overline{MO}_p = \overline{AL}_c$; $\overline{MI}_p = \overline{UC}_c$; $\overline{LU}_p = \overline{QM}_c$; $\overline{VI}_p = \overline{YC}_c$.

[6] Actually, the plain-text digraph is self-enciphered, in that $\overline{\theta^1\theta^2}_p = \overline{\theta^1\theta^2}_c$.

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

Figure 63.

(2) θ^1_p and θ^2_p are in the same row; the letter immediately to the right of θ^1_p forms θ^1_c, the letter immediately to the right of θ^2_p forms θ^2_c. When either θ^1_p or θ^2_p is at the extreme right of the row, the first letter in the row becomes its θ_c. Examples: $\overline{MA_p} = \overline{AN_c}$; $\overline{MU_p} = \overline{AF_c}$; $\overline{AF_p} = \overline{NM_c}$; $\overline{FA_p} = \overline{MN_c}$.

(3) θ^1_p and θ^2_p are in the same column; the letter immediately *below* θ^1_p form θ^1_c, the letter immediately below θ^2_p forms θ^2_c. When either θ^1_p or θ^2_p is at the bottom of the column, the top letter in that column becomes its θ_c. Examples: $\overline{MC_p} = \overline{CB_c}$; $\overline{AW_p} = \overline{TA_c}$; $\overline{WA_p} = \overline{AT_c}$; $\overline{QU_p} = \overline{YI_c}$.

(4) θ^1_p and θ^2_p are identical; they are to be separated by inserting a null, usually the letter X or Q. For example, the word BATTLES would be enciphered thus:

BA TX TL ES
DM RW CO KP

b. The Playfair square is automatically reciprocal so far as encipherments of type (1) above are concerned; but this is not true of encipherments of type (2) or (3).

118. Rectangular Designs

a. It is not essential that matrices for digraphic substitution be in the shape of perfect squares; rectangular designs will serve equally well, with little or no modification in procedure. In four-alphabet and two-alphabet rectangles reciprocity can be produced by following the method indicated in paragraph 115.

b. In figures 64 and 65 are shown two examples of such rectangles, together with illustrations of encipherments. Since the English alphabet consists of 26 letters, a number which can only form an impracticable rectangle 2 by 13, and since the addition of any symbols such as the digits 1, 2, 3 . . . to augment the number of elements to 27, 28, 30, 32, 35, or 36 characters would result in producing cryptograms containing intermixtures of letters and figures, the only practicable scheme is to reduce the alphabet to 24 letters as shown in the figures, where I serves also for J and U also for V,

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

Sec. 1 (θ^1_p) Sec. 3 (θ^1_c)
Sec. 4 (θ^2_c) Sec. 2 (θ^2_p)

Figure 64.

Examples:
  Plain: TH ER EA RE BE TT ER CR YP TO GR AM
  Cipher: YX BE BK CR ER LX BE RE HC ZX RH IB

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

Sec. 1 (θ^1_p) Sec. 3 (θ^1_c)
Sec. 4 (θ^2_c) Sec. 2 (θ^2_p)

Figure 65.

Examples:
  Plain: TH ER EA RE BE TT ER CR YP TO GR AM
  Cipher: BS ME MS PR TM FQ ME HN DN BQ XE WE

141

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

Figure 66.

c. Two-alphabet rectangles are also possible; it is thought unnecessary to demonstrate them by specific examples. The general examples shown in b above are considered sufficient.

d. It is possible, however, and it may be practicable to extend the alphabet to 28, 30, or more characters by the subterfuge now to be explained. Suppose one of the letters of the alphabet is omitted from the set of 26 letters, and suppose it is replaced by 2, 3, or more *pairs* of letters, each pair having as one of its members the omitted single letter. Thus, in the case of a one-alphabet Playfair design of rectangular shape, in which the letter K is omitted as a single letter, and the number of characters in the rectangle is made a total of 30 by the addition of five combinations of K with other letters, the rectangle shown in figure 66 may be constructed. An interesting consequence of this modification is that certain irregularities are introduced in the cryptogram, consisting in (1) the occasional replacement of $\overline{\theta^1\theta^2}_p$ by $\overline{\theta^1\theta^2\theta^3}_c$, that is, of a digraph by a trigraph, (2) less frequently, the replacement of $\overline{\theta^1\theta^2\theta^3}_p$ by $\overline{\theta^1\theta^2\theta^3\theta^4}_c$, that is, of a trigraph by a tetragraph, and (3) the appearance of variant values. For example, $\overline{AM}_p = \overline{HKU}_c$; $\overline{GL}_p = \overline{OKO}_c$; $\overline{JK}_p = \overline{KAKE}_c$; $\overline{CK}_p = \overline{BKE}_c$, or $\overline{DKE}_c$, or $\overline{GP}_c$, or $\overline{TP}_c$. So far as the decryptographing is concerned, there would be no difficulty, because the operator always considers any K occurring in the cipher test as invariably forming a ligature with the succeeding letter, taking the pair of letters as a unit. In decryptographing a set of letters, such as $\overline{GP}_c$, he obtains $\overline{CKO}_p$; he disregards the O.

e. As a final note it may be added that it is, of course, possible to insert the letters within a matrix in a less systematic order than that indicated in the various examples. *The letters may be inserted at random or by following the principles of systematically-mixed alphabets, so that no definite sequence is apparent in the matrix.*

119. Combined Alphabetical and Numerical Matrix

a. Figure 67 shows a 4-section matrix which presents a rather interesting feature in that it makes possible the substitution of 3-figure com-

binations for digraphs in a unique manner. To encipher a message one proceeds as usual to find the numerical equivalents of a pair, and then these numbers are added together. Thus:

```
Plain text:   PR    OC    EE    DI    NG
              275   350   100   075   325
                9    13    24    18     7
              ───   ───   ───   ───   ───
Cipher text:  284   363   124   093   332
```

Sec. 1 (θ^1_p)

Sec. 4 (θ^2_c)

A	B	C	D	E	000	025	050	075	100
F	G	H	I	K	125	150	175	200	225
L	M	N	O	P	250	275	300	325	350
Q	R	S	T	U	375	400	425	450	475
V	W	X	Y	Z	500	525	550	575	600
0	1	2	3	4	V	Q	L	F	A
5	6	7	8	9	W	R	M	G	B
10	11	12	13	14	X	S	N	H	C
15	16	17	18	19	Y	T	O	I	D
20	21	22	23	24	Z	U	P	K	E

Sec. 3 (θ^1_c)

Sec. 2 (θ^2_p)

Figure 67.

b. To decipher such a cryptogram, take the greatest multiple of 25 contained in the group of three digits; this multiple and its remainder form the elements for determining the plain-text pair in the usual manner. Thus, 284 = 275 + 9 = PR.

Section III.   COMPLEX SUBSTITUTION SYSTEMS

120. General

In paragraph 64, brief reference was made to more complex substitution systems. It was stated that there are certain polyalphabetic methods in which periodicity is absent; there are other methods in which the external manifestation of periodicity in cryptograms is prevented, or in which it is suppressed or disguised. Slight hints were then given as to the nature of some of these methods. This and the next two sections give a more detailed description and discussion of the methods indicated, which, as a class, may be designated as *aperiodic* systems, as contrasted with the previously described, more simple *periodic* systems.

143

121. Continuous or Nonrepeating-Key Systems

a. One of the simplest methods of avoiding periodicity occasioned by the employment of more than one substitution alphabet is to use as the key for the encipherment of one or more messages a series of letters or characters that does not repeat itself. The running text of a book, identical copies of which are in possession of the correspondents, may serve as the key for this purpose. It is only necessary for the correspondents to agree as to the starting point of the key, or to arrange a system of indicating this starting point in the text of the cryptogram. Such a system is called a continuous-key system. Other names applied to it are *nonrepeating, running,* or *indefinite-key* systems. Telephone directories, the Bible, standard reference works, etc., are often used as source books for such keys.

b. Various types of cipher alphabets may be employed in this system, direct or reversed standard alphabets, mixed alphabets drawn up at random, or secondary mixed alphabets resulting from the interaction of two primary sliding mixed components.

c. As an example of the method of cryptographing, suppose the following message is to be enciphered on the continuous key principle, using as the key the text of this subparagraph, beginning AS AN EXAMPLE . . . , and reversed standard alphabets:

HEAVY INTERDICTION FIRE FALLING AT . . . .

Key text: ASANE XAMPL EOFTH EMETH ODOFC RYPTO . . .
Plain text: HEAVY INTER DICTI ONFIR EFALL INGAT . . .
Cryptogram: TOASG PNTLU BGDAZ QZZLQ KYOUR JLJTV . . .

122. Auto-Key Systems

a. The cipher letters of a cryptogram may serve as keyletters, thus automatically furnishing a key. Suppose, for example, that two correspondents agree to use the word TRUE as an initial key, and suppose the message to be enciphered (with the obsolete U. S. Army cipher disk) is as follows:

HEAVY INTERDICTION FIRE FALLING AT . . . .

The first four letters are enciphered as shown:

Key text: TRUE
Plain text: HEAVY INTER DICTI ONFIR EFALL INGAT . . .
Cryptogram: MNUJ

The cipher letters MNUJ now form the keyletters for enciphering the next four plain-text letters, YINT, yielding OFHQ. The latter then form the keyletters for enciphering the next four letters, and so on, yielding the following:

144

CRITICAL

Key text:	TRUEM NUJOF HQKOE IIVWU VQODR LOSGD . . .
Plain text:	HEAVY INTER DICTI ONFIR EFALL INGAT . . .
Cryptogram:	MNUJO FHQKO EIIVW UVQOD RLOSG DBMGK . . .

b. Instead of using the cipher letters in sets, as shown, the last cipher letter given by the use of the keyword may become the keyletter for enciphering the plain-text letter; the cipher resultant of the latter then becomes the keyletter for enciphering the following letter, and so on to the end of the message. Thus:

Key text:	TRUEJ LDQXT CZRPW OANIA JFAAP EWJDA . . .
Plain text:	HEAVY INTER DICTI ONFIR EFALL INGAT . . .
Cryptogram:	MNUJL DQXTC ZRPWO ANIAJ FAAPE WJDAH . . .

c. It is obvious that an initial keyword is not necessary; a single pre-arranged letter will do.

d. The plain text itself may serve as a key, after an initial group or an initial letter. This is shown in the following example, wherein the text of the message itself, after the prearranged initial keyword TRUE, forms the key text:

Key text:	TRUEH EAVYI NTERD ICTIO NFIRE FALLI . . .
Plain text:	HEAVY INTER DICTI ONFIR EFALL INGAT . . .
Cryptogram:	MNUJJ WNCUR KLCYV UPOAX JAIGT XNFLP . . .

e. Although reversed standard alphabets have been used in all the foregoing examples, it is obvious that various types of alphabets may be employed, as prearranged.

f. The following method, although it may at first appear to be quite different, is in reality identical with those just described. A mixed sequence is prepared and its elements numbered in sequence. Let the mixed sequence be derived from the keyword PERMUTABLY:

```
6 3 7 5 9 8 1 2 4 10

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

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

Let the message be the same as before, and let the first letter be its own cipher equivalent. Each cipher letter from that point on is produced in turn by finding the sum of the numerical equivalents of the preceding cipher letter and the plain-text letter to be enciphered. When this total exceeds 26, the latter amount is deducted and the letter equivalent of the remainder is taken for the cipher letter. Thus:

```
Key text:            0 23  2  3 21 20 14 23 16 21 11 17 11 25 18 12 12
Plain text:          H  E  A  V  Y  I  N  T  E  R  D  I  C  T  I  O  N
Numerical value: 23  5  1 18 25 20  9 19  5 16  6 20 14 19 20 26  9
Keyed value:        28  3 21 46 40 23 42 21 37 17 37 25 44 38 38 21
(less 26 or 52 if
  necessary):     23  2  3 21 20 14 23 16 21 11 17 11 25 18 12 12 21
Cipher text:        H  J  B  Z  I  C  H  R  Z  G  F  G  Y  V  W  W  Z
Key text:          21 12  6 22  1 18 19  1  9  3 12 23 24
Plain text:          F  I  R  E  F  A  L  L  I  N  G  A  T
Numerical value: 17 20 16  5 17  1  8  8 20  9 11  1 19
Keyed value:        38 32 22 27 18 19 27  9 29 12 23 24 43
(less 26 or 52 if
  necessary):     12  6 22  1 18 19  1  9  3 12 23 24 17
Cipher text:        W  D  U  A  V  T  A  N  B  W  H  X  F
```

g. In the foregoing example the successive cipher letters form the successive keyletters; but, as noted in *d* above, the successive plain-text letters may serve as the successive keyletters.

h. The same results can be obtained by the use of sliding strips bearing the mixed alphabet. Study the following diagram showing the successive positions of the movable strip and compare the results with those obtained in *f* above.

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

i. One serious objection to such autokey systems is that the results of errors are cumulative; one error affects all the succeeding letters, and if several errors are made, the messages are difficult to decryptograph. It is possible that this disadvantage can be minimized by the use of automatic cipher devices suitably constructed to accomplish the encipherment with speed and accuracy.

123. Progressive-Alphabet Systems

a. The special characteristic of these systems is that the members of a whole set of cipher alphabets are employed one after the other in progression and in a definite sequence. These systems are periodic in nature and the length of the period is usually equal to the total number of different cipher alphabets employed in the system. The sequence in which the various cipher alphabets are used may or may not change with each message; if it does, this constitutes an additional element of secrecy.

b. To illustrate what is meant by a progressive system a simple example will be given, employing the obsolete U. S. Army Cipher Disk. Starting with the disk so that $A_{\phi} = A_c$ (or with any other prearranged initial setting), the first letter of the message is enciphered; the revolving alphabet is then moved one step clockwise (or counter-clockwise) and the second letter is enciphered, and so on. After 26 letters have been enciphered, the disk has returned to its initial starting point and a second cycle begins (if the message is longer than 26 letters). Thus, the period in this case is 26 letters. It is obvious that the displacement of the revolving disk may occur after every 2, 3, 4 . . . . letters, as prearranged, in which case the period increases correspondingly in length. The displacement may, however, be more complicated than this, and may occur after a constantly varying number of letters has been enciphered, whereupon periodicity is suppressed.

c. Two sliding mixed components may be employed, producing a set of 26 secondary mixed alphabets.

d. Another variation is more complicated. Suppose the correspondents draw up a set of 100 random-mixed cipher alphabets, each accompanied by a designating number from 00 to 99, and a set of numerical keys composed of randomized sequences of numbers from 00 to 99. Each such numerical key is designated by an indicator of some sort. To encipher a message, a key sequence is selected and the cryptogram is prepared by means of the sequence of alphabets indicated by the key sequence. If the message is 100 or less letters in length, the alphabets do not repeat; if it is more than 100 letters long, either the sequence of alphabets may repeat or else a new sequence is selected, as prearranged. It is possible to operate the system by means of indicators inserted in the text of the cryptogram.

124. Interrupted or Variable-Key Systems

In certain of the foregoing systems it was noted that periodicity is entirely avoided by the use of a key which is so long that it does not repeat itself; often such a system is referred to as operating in connection with an *indefinite, infinite,* or *unlimited* key as contrasted with one that operates in connection with a *definite, finite,* or *limited* key. But periodicity may also be avoided by special manipulation of a limited key. Several such methods are explained below.

125. Suppressing Periodicity by Encipherment of Variable-Length Groupings of the Plain Text

a. A keyword, though limited in length, may nevertheless be applied to variable or invariable-length sections of the plain text. When, for example, each letter of the key serves to encipher a single letter of the plain text, the encipherment is said to be *invariable* or *fixed* in this respect. The same is true even if a single letter of the key serves to encipher regular sets of letters of the plain text; for example, each letter of the key may serve to encipher 2, 3, 4 . . . . letters of the text. In these cases periodicity would be manifested externally by the cryptograms, providing there is a sufficient amount of text to be examined. But if each letter of the key serves to encipher *irregular* or variable-length groupings of the plain text, then periodicity cannot appear except under rather remote contingencies. Suppose, for example, that so simple a scheme as letting each letter of the key serve to encipher a *complete word* of the text is used; since words are of irregular lengths and there is little or no regularity whatever in the sequence of words with respect only to their lengths, periodicity cannot appear. An example of encipherment will be useful.

b. In the following example the simple cipher disk (direct sequence sliding against reversed sequence) is used, with the key word DEBARK, to encipher the following message, according to the scheme described above. Study it carefully.

```
Key:          D       E      B         A     R     K
Plain text:   COLLECT ALL STRAGGLERS STOP SEND THEM
Cipher:       BPSSZBK ETT JIKBVVQXKJ IHML ZNEO RDGY

Key:          D       E   B
Plain text:   FORWARD AT ONCE
Cipher:       YPMHDMA EL NOZX

Cryptogram:   BPSSZ BKETT JIKBV VQXKJ IHMLZ NEORD
              GYYPM HDMAE LNOZX
```

c. Instead of enciphering according to natural word lengths, the irregular groupings of the text may be regulated by other agreements. For

example, suppose that it is agreed that every keyletter will encipher a number of letters corresponding to the numerical value of the keyletter in the normal alphabet. The foregoing example then becomes as follows:

Key: D   E   B A   R
Plain text: COLL ECTAL LS T RAGGLERSSTOPSENDTH
Cipher: BPSS ACLET QJ H ARLLGNAZZYDCZNEOYK

Key: K   D
Plain text: EMFORWARDAT ONCE
Cipher: GYFWTOKTHKR PQBZ

Cryptogram: BPSSA CLETQ JHARL LGNAZ ZYDCZ NEOYK
             GYFWT OKTHK RPQBZ

d. The foregoing example employed reversed standard alphabets, but mixed alphabets of all types may readily be used.

e. If the keyword is short, and the message long, periodicity may creep in despite the irregular groupings in the encipherment. Sufficient evidence may even be obtained to lead to a disclosure of the length of the key. But if the key consists of a long word, or of a complete phrase or sentence, the text would have to be very long in order that sufficient evidences of periodicity be found to make possible the determinaton of the length of the key.

126. Suppressing Periodicity by Encipherment by Variable-Length Groupings of the Key

a. In paragraph 125*b* periodicity was suppressed by enciphering variable-length groupings of the text; in this paragraph it will be shown how periodicity may be suppressed by enciphering by variable-length groupings of the key. The method consists in *interrupting* the key.

b. Given a keyword, it can become a variable-length key by interrupting it according to some prearranged plan, so that it becomes equivalent to a series of keys of different lengths. Thus, the single keyword UNPREPAREDNESS may be expanded to a sequence of irregular lengths, such as UNPREP/UNP/UNPREPAR/UNPR/UNPRE-PARE/UNPREPAREDN/U/UNPRE, etc. Various schemes for indicating or determining the interruptions may be adopted. For example, suppose it may be agreed that the interruption will take place immediately after and every time that the letter R occurs in the plain text. The key would then be interrupted as shown in the following example:

Key: UNPUN UNPRE PARED UNPRE UNPRU NP . . .
Plain text: OURFR ONTLI NESAR ENOWR EPORT ED . . .

c. It is possible to apply an interrupted key to variable-length groupings of the plain text. In illustrating this method, an indicator, the letter

X, will be inserted in the plain text to show when the interruption takes place. The plain text is enciphered by natural word lengths.

Key: U   N   U   N   P   U
Plain text: OUR FRONTX LINES ARE NOWX REPORTED

d. It is also possible to interrupt the key regularly, cutting it up into equal length sections as, for example, with the keyword EXTINGUISH-ER: EXT/XTI/TIN/ING/NGU/GUI/UIS/ISH/SHE/HER. Each set of three keyletters may serve to encipher a set of three plain-text letters. But it is possible to make each set of three keyletters apply to more than three plain-text letters, or to irregular groupings of plain-text letters. For example, suppose a numerical key be derived from the keyword:

$$E \quad X \quad T \quad I \quad N \quad GU \quad I \quad S \quad H \quad E \quad R$$
$$1\text{-}12\text{-}10\text{---}5\text{---}7\text{---}3\text{-}11\text{---}6\text{---}9\text{---}4\text{---}2\text{---}8$$

Let this numerical sequence determine how many letters will be enciphered by each grouping of the key. The example below will illustrate (reversed standard alphabets are used):

Numbers: 1   12   10   5
Key: E   XTIXTIXTIXTI   TINTINTINT   INGIN
Plain text: C   OLLECTALLSTR   AGGLERSSTO   PSEND
Cipher: C   JIXTRPXIXFAR   TCHIEWBQUF   TVCVK

Numbers: 7   3   11
Key: NGUNGUN   GUI   UISUISU
Plain text: THEMFOR   WAR   DATONCE
Cipher: UZQBBGW   KUR   RIZGVQQ

Cryptogram: CJIXT RPXIX FARTC HIEWB QUFTV
             CVKUZ QBBGW KURRI ZGVQQ

e. Another simple method of prearranging the interruption of a keyword or of plain text is to employ the sequence of numbers given by reducing an incommensurate fraction to decimals. For example, the fraction $\frac{1}{7}$ yields the sequence 142857142857 . . . This fraction may be represented by the indicator letter H given as the initial letter of the cryptogram.

127. Cipher Devices in Which Periodicity Is 'Avoided

There are certain cipher devices which operate in such a manner that periodicity is avoided or suppressed. Some of them are discussed in section I, chapter 11. Among them one of the most interesting is that invented by Sir Charles Wheatstone in 1867. As a rule, however, cipher devices, by their very nature, can hardly avoid being cyclic in operation, thus causing periodicity to be exhibited in the cryptograms.

CHAPTER 10
REPETITIVE AND COMBINED SYSTEMS

Section I. REPETITIVE SYSTEMS

128. Superencipherment

a. When, for purposes of augmenting the degree of cryptographic security, the plain text of a message undergoes a first or primary encipherment and the resulting cipher text then undergoes a second or secondary encipherment, the system as a whole is often referred to as one involving superencipherment. If the two or more processes are well selected, the objective is actually reached, and the resulting cryptograms present a relatively great degree of cryptographic security; but sometimes this is not accomplished and the augmented security is of a purely illusory character. The final cryptographic security may, in fact, be no greater in degree than if a single encipherment had been effected, and in unusual cases it may even be less than before.

, *b.* It is impossible to describe all the combinations that might be employed; only a very few typical cases can here be treated, and these will be selected with a view to illustrating general principles. It is possible to pass a message through 2, 3, . . . successive processes of substitution; or through 2, 3, . . . successive processes of transposition; or substitution may be followed by transposition or vice versa. An example of each type will be given.

c. It will be convenient to adopt the symbol C to represent the cipher text produced by any unspecified process of encipherment. The symbols C_1, C_2, C_3, . . . , will then represent the successive texts produced by successive processes in superencipherment. The subscript letter *s* or *t* may be prefixed to the C to indicate that a given process is one of substitution or of transposition. Thus, the steps in a system where a first substitution is followed by a second substitution can be represented symbolically by $sC_1 \rightarrow sC_2$. In a similar manner, $tC_1 \rightarrow tC_2$ represents double transposition. The symbol $sC_1 \rightarrow tC_2$ means that the text from a first process of substitution undergoes transposition as a second process.

129. Repetitive Transposition Systems

These have been dealt with in Chapter 8, Sections II and III, and need no further discussion at this point. It was there shown that properly

151

selected transposition methods, when repetitive in character, can produce cryptograms of very great security.

130. Repetitive Monoalphabetic Substitution Systems

Suppose a message undergoes a primary encipherment by means of a single-mixed, nonreciprocal alphabet, and the primary cipher text undergoes a secondary encipherment by means of the same or a *different* mixed alphabet. The resulting cryptogram is still monoalphabetic in character, and presents very little, if any, augmentation in the degree of security (depending upon the type of alphabet employed). Here an entirely illusory increase in security is involved and an ineffectual complexity is introduced; the process may indeed be repeated indefinitely without producing the desired result. This is because the fundamental nature of monoalphabetic substitution has not been taken into consideration in the attempts at superencipherment; $sC_1 \rightarrow sC_2 \rightarrow sC_3$ . . . , still remains monoalphabetic in character.

131. Repetitive Polyalphabetic Substitution Systems

a. If the primary encipherment is by means of the repeating-key principle, with standard alphabets, and the secondary encipherment is similar in character, with similar alphabets, and a key of similar length, the final cryptogram presents no increase in security at all. Thus, if the key BCDE is used in the primary encipherment (Vigenère Method) and the key FGHI is used in the secondary encipherment, the final result is the same as though the key GIKM had been used in a single encipherment.

b. If mixed alphabets are used, and if those of the primary and the secondary encipherment belong to the same series of secondary alphabets resulting from the sliding of two primary sequences against each other, the results are similar in character to those described in *a* above. They are identical with those that would be obtained by an equivalent single encipherment by the appropriate secondary alphabets.

c. If the key for the secondary encipherment is of a different length from that for the primary encipherment, the results are, however, somewhat different, in that the period of the resultant cryptogram becomes the least common multiple of the two key lengths. For example, if the length of the key for the primary encipherment is 4, that for the secondary 6, the result is the same as though a key of 12 elements had been employed in a single encipherment. This can be demonstrated as follows, using the keys 4-1-2-3 and 5-2-6-1-4-3:

```
4 1 2 3 4 1 2 3  4 1 2 3 | 4 1 2 3 4 1 2 3  4 1 2 3 | 4 1 2 3 . . .
5 2 6 1 4 3 5 2  6 1 4 3 | 5 2 6 1 4 3 5 2  6 1 4 3 | 5 2 6 1 . . .
9 3 8 4 8 4 7 5 10 2 6 6 | 9 3 8 4 8 4 7 5 10 2 6 6 | 9 3 8 4 . . .
```

d. The degree of cryptographic security is, without doubt, increased by such a method. If the key lengths are properly selected, that is, if they present no common multiple less than their product, the method may give cryptograms of great security. For example, two keys that are 17 and 16 characters in length would give a cryptogram that is equivalent in period to that of a cryptogram enciphered once by a key 17 × 16, or 272 elements in length. The fundamental principle of an excellent, though complicated, printing telegraph cipher system is this very principle.

Section II. COMBINED SYSTEMS

132. Combined Monoalphabetic and Polyalphabetic Substitution Systems

a. If a message undergoes a primary encipherment by the repeating-key method, using standard alphabets, and the primary cipher text then undergoes a secondary encipherment by means of a single-mixed alphabet, the degree of cryptographic security is increased to the same extent that it would be if the original message had undergone the same primary encipherment with secondary alphabets resulting from the sliding of a mixed primary sequence against the normal sequence. This increase in security is not very great.

b. The same is true if the primary encipherment is monoalphabetic and the secondary encipherment is polyalphabetic by the method described.

c. In general, this also applies to other types of polyalphabetic and monoalphabetic combinations. The increase in security is not very great, and is, indeed, much less than the uninitiated suspect.

133. Combined Substitution-Transposition in General

Combinations of substitution and transposition methods can take many different forms, and only a few examples can be illustrated herein. It is possible of course, to apply substitution first, then transposition, or transposition first, then substitution. The most commonly encountered systems, however, are of the former type, that is $sC_1 \rightarrow tC_2$. Furthermore, it can be stated that as a rule practicable systems in which both processes are combined use methods that are relatively simple in themselves, but are so selected as to produce cryptograms of great security as a result of the combination. To give a very rough analogy, in certain combinations the effect is much more than equivalent to the simple addition of complexities of the order X and Y, giving $X+Y$; it is more of the order XY, or even X^2Y^2.

134. Monoalphabetic and Polyalphabetic Substitution Combined with Transposition

a. A message may undergo simple monoalphabetic substitution or complex polyalphabetic substitution and the resulting text passed through a simple transposition. Obviously, either standard or mixed alphabets may be employed for the substitution phase and for the transposition phase any one of the simple varieties of geometric-design methods may be applied.

b. As an example, note the following simple combination, using the message ALL ACTION AT LANDING BEACH HAS CEASED. 1st step: sC_1 (monoalphabetic, by mixed alphabet) :

```
Plain:   ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher:  TDRAMOBNILPEZYXWVUSQKJHGFC
```

```
Message: ALLAC TIONA TLAND INGBE ACHHA SCEAS ED
Cipher:  TEETR QIXYT QETYA IYBDM TRNNT SRMTS MA
```

2d step: tC_2 (as prearranged between correspondents) :

```
TEETRQIX    (For the inscription; a rectangle of eight columns.)
YTQETYAI
YBDMTRNN    (For the transcription; counterclockwise route beginning
TSRMTSMA      at lower right hand corner.)
```

Cryptogram: ANIXI QRTEE TYYTS RMTSM NAYTE QTBDM TR

c. A simple subterfuge often adopted between correspondents is to write the substitution text backwards to form the final cryptogram (a case of simple reversed writing).

d. An extremely simple and yet effective transposition method (when its presence is not suspected) sometimes employed as a preliminary to substitution is that in which the text of a message is first divided into halves; the second being placed under the first as in rail-fence writing. Thus:

```
P O E D O O T F M A K T O
R C E T P R O E B R A I N
```

Then encipherment by simple monoalphabetic methods may be effected and the cipher text taken from the two separate lines. Thus, if a standard alphabet one letter in advance were used, the text would be as follows:

```
Q P F E P P U G N B L U P
S D F U Q S P F C S B J O
```

Cryptogram: QPFEP PUGNB LUPSD FUQSP FCSBJ O

154

e. A simple variation of the foregoing method which is frequently effective with true digraphic methods of substitution is to write $\theta^2{}_p$ under $\theta^1{}_p$ and then encipher the sets of juxtaposed $\overline{\theta^1\theta^1}{}_p$ letters digraphically, then the sets of juxtaposed $\overline{\theta^2\theta^2}{}_p$ letters. Thus, let the message be WILL RETURN AT ONCE; it would be written down as follows:[7]

<div align="center">

WLRTRAOC
ILEUNTNE

</div>

Then the following pairs would be enciphered: $\overline{WL}_p$, $\overline{RT}_p$, $\overline{RA}_p$, $\overline{OC}_p$, $\overline{II}_p$, etc. The foregoing message enciphered in this manner by means of the Playfair Square shown in figure 63, for example, yields the following cryptogram:

Plain text: WL RT RA OC IL EU NT NE
Cipher: VO IR TN LT CQ HN AR RP
Cryptogram: VOIRT NLTCQ HNARR P

f. Naturally the transposition process may involve groups of letters; a simple type of disarrangement is to reverse the order of the letters in 5-letter groups, or within 5-letter groups a transposition such as 3–2–1–4–5 or 2–1–5–3–4 (any of 120 different arrangements) is possible.

g. Columnar transposition methods lend themselves especially well to combination with substitution methods. An excellent example will be considered under the next section.

135. Polyliteral Substitution Combined with Transposition

In paragraph 111*b* the essential nature of polyliteral substitution as contrasted with monoliteral substitution was discussed. Polyliteral methods make use of polypartite alphabets in which the cipher equivalents are composed of two or more parts. This being the case it is a natural extension of cryptographic processes to *separate* these parts or to distribute them throughout the cipher text so that the components or, so to speak, fractional parts of the cipher equivalents are thoroughly disarranged and distributed evenly or irregularly throughout the text.

136. Fractionating Systems

a. A simple example will first be shown. Let the following bipartite cipher alphabet be drawn up by assigning numerical equivalents from 01 to 26 in mixed sequence to the letters of the normal sequence. Thus:

---

[7] In preparing the text for encipherment, the clerk must bear in mind that if the normal Playfair system is to be used no doublets can be enciphered. The message WE WILL LEAVE . . would be arranged thus:

<div align="center">

WXILXEV
EWLXLAE

</div>

A	B	C	D	E	F	G	H	I	J	K	L	M
02	11	06	12	13	05	10	14	09	15	16	17	01

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
03	18	19	20	08	21	07	04	22	23	24	25	26

Each letter is represented by a combination of two digits; in preparing the message for cryptographing, the two digits comprising the cipher equivalent of a letter are written one below the other, thus:

Plain text: **ONE PLANE REPORTED LOST**

Cipher $\begin{cases} \theta^1_c: \textbf{101 11001 01110011 1120} \\ \theta^2_c: \textbf{833 97233 83988732 7817} \end{cases}$

By recombining the single digits in pairs, reading from horizontal lines, and writing down the pairs in unchanged numerical form, one obtains the following:

$$10 \quad 11 \quad 10 \quad 01 \quad 01 \quad 11 \quad 00 \quad 11 \quad 11 \quad 20$$
$$83 \quad 39 \quad 72 \quad 33 \quad 83 \quad 98 \quad 87 \quad 32 \quad 78 \quad 17$$

b. The foregoing cipher text can be transmitted in 5-figure groups, or it can be reconverted into letters by one means or another, but some difficulties are encountered in the latter case because every one of 100 different pairs of digits has to be provided for, thus necessitating a 2-letter substitution, which would make the cipher text twice as long as the plain text.

c. In the methods to follow presently, these difficulties are avoided by a simple modification. This modification consists in the employment of true *polyfid cipher alphabets,* that is, polypartite alphabets in which the plain component is the normal sequence and the cipher component consists of a sequence of equivalents composed of all the permutations of 2, 3, 4, . . . symbols taken in definite groups. For example, a *bifid alphabet*[8] composed of permutations of five digits taken two at a time can be constructed, yielding a set of 25 equivalents for a 25-letter alphabet (I and J being usually considered as one letter). A *trifid alphabet* of 27 equivalents can be constructed from *all* the permutations of the digits 1, 2, 3, taken three at a time; an extra character must, however, be added to represent the 27th element of the alphabet. It is convenient to represent the parts of a bifid equivalent by the symbols θ^1_c and θ^2_c, the parts of a trifid equivalent, by the symbols θ^1_c, θ^2_c and θ^3_c.

---

[8] Such an alphabet should be clearly differentiated from a *biliteral alphabet.* In the latter, two and only two elements are employed, in groups of fives, yielding 25 or 32 permutations. The Biliteral Cipher of Sir Francis Bacon and the Baudot Alphabet of modern printing telegraph systems are based upon alphabets that are typical examples of biliteral alphabets. The designation *digraphic alphabet* will be applied to one in which the cipher equivalents are composed of any number of symbols, *n,* taken simply in groups of two, these symbols not being permuted in systematic fashion to produce a complete set of 2^n equivalents.

d. Polyfid cipher alphabets may be systematically-mixed alphabets based upon keywords and keyphrases. For example, note how the following bifid alphabet is derived from the keyphrase XYLO-PHONIC BEDLAM:

X	Y	L	O	P	H	N	I	C	B	E	D	A
11	12	13	14	15	21	22	23	24	25	31	32	33

M	F	G	K	Q	R	S	T	U	V	W	Z
34	35	41	42	43	44	45	51	52	53	54	55

The same principle may be applied to trifid alphabets, employing the permutations of the three digits 1, 2, and 3, taken in groups of three.

e. Note the following bifid alphabet and the example of its use in enciphering a message:

A	B	C	D	E	F	G	H I-J	K	L	M
12	31	21	32	33	15	25	34 24	35	41	11

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	42	43	44	23	45	22	14	51	52	53	54	55

Message:		ONE PLANE REPORTED LOST
Cipher	θ^1_c:	413 44113 23442233 4442
	θ^2_c:	233 31233 33323232 1252

The bifid elements, θ^1_c and θ^2_c, are now recombined horizontally in pairs and the pairs are reconverted into letter equivalents of the basic alphabet which, for the sake of convenience, is here arranged in the form of a deciphering alphabet:

11	12	13	14	15	21	22	23	24	25	31	32	33
M	A	N	U	F	C	T	R	I	G	B	D	E

34	35	41	42	43	44	45	51	52	53	54	55
H	K	L	O	P	Q	S	V	W	X	Y	Z

Cryptogram: LHLNR QTEQO REAEE DDDAW

f. It will be noted that there are four basic steps involved in the foregoing encipherment: (1) A process of decomposition, substitutive in character, in which each θ_p is replaced by a bipartite θ_c, composed of two parts, θ^1_c and θ^2_c, according to a bifid alphabet; (2) a process of separation, transpositive in character, in which each θ^1_c is separated from the θ^2_c with which it was originally associated; (3) a process of recombination, also transpositive in character, in which each θ^1_c is combined with a θ^2_c with which it was not originally associated; and finally (4) a process of recomposition, substitutive in character, in which each new θ^1_c θ^2_c combination is given a letter value according to a bifid alphabet. In the foregoing example (*e* above), the alphabet for the recomposition was the same as that for the decomposition; this,

157

of course, is not an inherent necessity of the system; the decomposition and recomposition alphabets may be entirely different. This is shown in the example in paragraph 137d.

137. Comparison of Foregoing Fractionating System with Certain Digraphic Systems

a. The method described in paragraph 136e can be identified with some of the digraphic substitution systems discussed in chapter 9, section I.

b. Take the message of paragraph 136e and let a slight modification in the method of recombining θ^1_c and θ^2_c be made. Specifically, let the first halves and the second halves of the bifid equivalents of the plain-text letters be combined in the following manner, using the bifid alphabet of paragraph 136e:

```
Message:  ONE PLANE REPORTED LOST
       ON    EP    LA    NE    RE    PO    RT    ED
      41=L  34=H  41=L  13=N  23=R  44=Q  22=T  33=E
      23=R  33=E  12=A  33=E  33=E  32=D  32=D  32=D

                         LO    ST
                        44=Q  42=O
                        12=A  52=W
```

Cryptogram: LRHEL ANERE QDTDE DQAOW

If the cryptogram given in paragraph 136e were split in the middle into two sections, and the letters taken alternately, the result would be identical with that obtained in this subparagraph. The identification referred to in a above is demonstrated in c below.

c. Note the two alphabet matrix shown in figure 68. If the same message is now enciphered by its means, a cryptogram identical with that obtained in b above will be obtained. Thus:

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

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

Message:

ONE PLANE REPORTED LOST

Substitution of pairs:

$ON_p = LR_c$; $EP_p = HE_c$; $LA_p = LA_c$; $NE_p = NE_c$;
$RE_p = RE_c$; etc.

Cryptogram:

LRHEL ANERE etc.

Figure 68.

158

d. In the example in paragraph 136*e*, the same bifid alphabet was used for the recomposition as for the decomposition. Instead of converting the combined θ^1_c θ^2_c elements into letters by means of the original bifid alphabet, suppose a second bifid alphabet specifically drawn up for this recomposition is at hand (see par. 136*f*). Thus:

11=A	21=B	31=C	41=K	51=V
12=U	22=I	32=D	42=N	52=W
13=T	23=L	33=F	43=P	53=X
14=O	24=E	34=G	44=Q	54=Y
15=M	25=S	35=H	45=R	55=Z

The encipherment of the message is then as follows:

Message: **ONE PLANE REPORTED LOST.**

Alphabet for decomposition		Alphabet for recomposition	
A=12	N=13	11=A	34=G
B=31	O=42	12=U	35=H
C=21	P=43	13=T	41=K
D=32	Q=44	14=O	42=N
E=33	R=23	15=M	43=P
F=15	S=45	21=B	44=Q
G=25	T=22	22=I-J	45=R
H=34	U=14	23=L	51=V
I-J=24	V=51	24=E	52=W
K=35	W=52	25=S	53=X
L=41	X=53	31=C	54=Y
M=11	Y=54	32=D	55=Z
	Z=55	33=F	

Encipherment:

```
 ON     EP     LA     NE     RE     PO     RT     ED
41=K  34=G  41=K  13=T  23=L  44=Q  22=I  33=F
23=L  33=F  12=U  33=F  33=F  32=D  32=D  32=D

                     LO     ST
                    44=Q  42=N
                    12=U  52=W
```

Cryptogram: KLGFK UTFLF QDIDF DQUNW

e. Now encipher the same plain-text message by means of the four-alphabet matrix shown in figure 69. The results are as follows:

Message: **ONE PLANE REPORTED LOST.**

Plain text: ON EP LA NE RE PO RT ED LO ST

Cipher pairs: KL GF KU TF LF QD ID FD QU NW

Cryptogram: KLGFK UTFLF QDIDF DQUNW

The results are identical with those obtained in *d* above.

```
┌─────────────┬─────────────┐
│ M A N U F   │ A U T O M   │
│ C T R I G   │ B I L E S   │
│ B D E H K   │ C D F G H   │
│ L O P Q S   │ K N P Q R   │
│ V W X Y Z   │ V W X Y Z   │
├─────────────┼─────────────┤
│ A B C K V   │ M C B L V   │
│·U I D N W   │ A T D O W   │
│ T L F P X   │ N R E P X   │
│ O E G Q Y   │ U I H Q Y   │
│ M S H R Z   │ F G K S Z   │
└─────────────┴─────────────┘
```

Figure 69.

f. If the successive letters of the cryptogram of *b* above are enciphered monoalphabetically by means of the following alphabet, the results again coincide with those obtained in *d* and *e* above.

Alphabet

C_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
C_2:U C B D F M S G E H K A T N P Q L R I O V W X Y Z

First cryptogram: LRHEL ANERE QDTDE DQAOW
Final cryptogram: KLGFK UTFLF QDIDF DQUNW

138. Fractionating Systems as Forms of Combined Substitution and Transposition

In studying the various types of substitution discussed in chapter 9, section II, it was not apparent, and no hint was given, that these systems combine both substitution and transposition methods into a single method. But the analysis presented in paragraph 137 shows clearly that there is a kind of transposition involved in digraphic methods involving the use of matrices.

139. Fractionation and Recombination within Regular or Variable Groupings of Fractional Elements

a. This method is an extension or modification of that illustrated in paragraph 136*e*. Let the text be written out in groups of 3, 4, 5, . . . letters, as prearranged between the correspondents. Suppose groupings of five letters are agreed upon; a bifid alphabet (that in par. 136*e*) is used for substitution; thus:

Message: ONEPL ANERE PORTE DLOST
                    41344 11323 44223 34442
                    23331 23333 32323 21252

Then, let the recombinations be effected *within* the groups horizontally. Thus, for the first group the recombinations are 41, 34, 42, 33, and 31. The entire message is as follows:

41.34.4	11.32.3	44.22.3	34.44.2
2.33.31	2.33.33	3.23.23	2.12.52

Recomposition (using the same bifid alphabet as was used for the decomposition) yields the cryptogram:

<div align="center">LHOEB MDDEE QTERR HQTAW</div>

b. As indicated, other groupings may be employed. Furthermore, a different bifid alphabet for the recomposition may be used than was employed for the original substitution or decomposition. It is also clear that sequences of variable-length groupings may also be employed, as determined by a subsidiary key.

c. Trifid alphabets also lend themselves to these methods. Note the following example:

Alphabet for decomposition			*Alphabet for recomposition*		
A=222	J=312	S=131	111=I	211=U	311=V
B=322	K=112	T=122	112=K	212=N	312=J
C=121	L=231	U=211	113=W	213=H	313=$\overline{ZB}$
D=133	M=323	V=311	121=C	221=X	321=E
E=321	N=212	W=113	122=T	222=A	322=B
F=123	O=333	X=221	123=F	223=Y	323=M
G=332	P=233	Y=223	131=S	231=L	331=Q
H=213	Q=331	Z=132	132=$\overline{ZA}$	232=R	332=G
I=111	R=232	?=313	133=D	233=P	333=O

Message: H A S   A I R P L A N E   R E T U R N E D   Y E T ?

```
H A S A I    R P L A N    E R E T U    R N E D Y    E T ?
2 2 1.2 1    2 2 2.2 2    3 2 3.1 2    2 2 3.1 2    3 1 3
1.2 3 2.1    3.3 3 2.1    2.3 2 2.1    3.1 2 3.2    2 2 1
3 2.1 2 1    2 3.1 2 2    1 2.1 2 1    2 2.1 3 3    1 2 3
```

Cipher text[9]: XUR$\overline{ZA}$C AYGFT MTBKC YFFAD $\overline{ZB}$XF

Final cryptogram: XURZA CAYGF TMTBK CYFFA DZBXF

---

[9] The reason for the regrouping shown in the final cryptogram requires a consideration of the fact that a trifid alphabet involves the use of 27 characters. Since our alphabet contains but 26 letters, either an extra symbol would have to be used (which is impractical) or some subterfuge must be adopted to circumvent the difficulty. This has been done in this case by using $\overline{ZA}$ and $\overline{ZB}$ to represent two of the permutations in the recomposition alphabet. In decryptographing, when the clerk encounters the letter Z in the text, it must be followed either by A or by B; according to the alphabet here used, ZA represents permutation 132, and ZB represents permutation 313. In order not to introduce a break in the regulation 5-letter groupings of cipher text, the final cryptogram is regrouped strictly into fives.

d. Bifid and trifid alphabets may be combined within a single system with appropriate groupings, but such combinations may be considered as rather impracticable for military usage.

140. Fractionation Combined with Columnar Transposition

a. An excellent system of combined substitution-transposition that has stood the test of practical, war-time usage is that now to be described. Let a 36-character bipartite alphabet square be drawn up, and a message enciphered, as follows:

```
      M  O  N  T  H  S
   ┌─────────────────────┐
W  │ H  8  A  1  I  9 │
I  │ L  C  3  O  U  M │
N  │ B  2  P  Y  N  D │
T  │ 4  E  5  F  6  G │
E  │ 7  J  ∅  K  Q  R │
R  │ S  T  V  W  X  Z │
   └─────────────────────┘
```

(Key for internal alphabet: HAIL COLUMBIA HAPPY LAND. Digits are inserted immediately after each letter from A to J, A being followed by 1, B, 2, etc.)

Message:

ADVANCE PROGRESSING SATISFACTORILY OVER 400 PRIS-
ONERS AND 5-75 MM GUNS CAPTURED. SECOND OBJECTIVE
REACHED AT 5:15 P. M.

Substitution:

```
 A  D  V  A  N  C  E  P  R  O  G  R  E  S  S
WN NS RN WN NH IO TO NN ES IT TS ES TO RM RM
 I  N  G  S  A  T  I  S  F  A  C  T  O  R  I
WH NH TS RM WN RO WH RM TT WN IO RO IT ES WH
 L  Y  O  V  E  R  4  ∅  ∅  P  R  I  S  O  N
IM NT IT RN TO ES TM EN EN NN ES WH RM IT NH
 E  R  S  A  N  D  5  7  5  M  M  G  U  N  S
TO ES RM WN NH NS TN EM TN IS IS TS IH NH RM
 C  A  P  T  U  R  E  D  S  E  C  O  N  D  O
IO WN NN RO IH ES TO NS RM TO IO IT NH NS IT
 B  J  E  C  T  I  V  E  R  E  A  C  H  E  D
NM EO TO IO RO WH RN TO ES TO WN IO WM TO NS
 A  T  5  1  5  P  M
WN RO TN WT TN NN IS
```

The C_1 text is now inscribed in a rectangle of predetermined dimensions. Transposition rectangle (columnar, based on key HAIL COLUMBIA HAPPY LAND) (see figure 70).

b. One of the important advantages of this type of cipher is that it affords accuracy in transmission since the text is composed of a

```
H   A   I   L   C   O   L   U   M   B   I   A   H   A   P   P   Y   L   A   N   D
8—1—10—12—6—17—13—20—15—5—11—2—9—3—18—19—21—14—4—16—7
```

```
W  N  N  S  R  N  W  N  N  H  I  O  T  O  N  N  E  S  I  T  T
S  E  S  T  O  R  M  R  M  W  H  N  H  T  S  R  M  W  N  R  O
W  H  R  M  T  T  W  N  I  O  R  O  I  T  E  S  W  H  I  M  N
T  I  T  R  N  T  O  E  S  T  M  E  N  E  N  N  N  E  S  W  H
R  M  I  T  N  H  T  O  E  S  R  M  W  N  N  H  N  S  T  N  E
M  T  N  I  S  I  S  T  S  I  H  N  H  R  M  I  O  W  N  N  N
R  O  I  H  E  S  T  O  N  S  R  M  T  O  I  O  I  T  N  H  N
S  I  T  N  M  E  O  T  O  I  O  R  O  W  H  R  N  T  O  E  S
T  O  W  N  I  O  W  M  T  O  N  S  W  N  R  O  T  N  W  T  T
N  N  N  I  S
```

Cryptogram:

```
NEHIM  TOION  ONOEM  NMRSO  TTENR  OWNIN
ISTNN  OWHWO  TSISI  OROTN  NSEMI  STONH
ENNST  WSWTR  MRSTN  THINW  HTOWN  SRTIN
ITWNI  HRMRH  RONST  MRTIH  NNIWM  WOTST
OWSWH  ESWTT  NNMIS  ESNOT  TRMWN  NHETN
RTTHI  SEONS  ENNMI  HRNRS  NHIOR  ONRNE
OTOTM  EMWNN  OINT
```

Figure 70.

limited number of letters. In fact, if the horizontal and vertical coordinates of the cipher square are the same letters, then the cryptographic text is composed of permutations of but six different letters, thus aiding very materially in correct reception. Indeed, it is even possible to reconstruct completely a message that has been so badly garbled that only half of it is present. This cipher system was used with considerable success by the Germany Army in 1917–18, and was known to the Allies as the ADFGVX Cipher, because these were the letters used as horizontal and vertical coordinates of the cipher square, and consequently the cipher text consisted solely of these six letters.

c. The cipher text of the foregoing message is, of course, twice as long as the plain text, but it can be reduced to exactly the original plain-text length by combining the distributed or transposed θ^1_c and θ^2_c elements in pairs, referring to the original (or a different) polypartite square, and recomposing the pairs into letters. In this case, the horizontal and vertical coordinates must be identical in order to permit of finding equivalents for all possible pairs.

CHAPTER 11

CIPHER DEVICES AND CIPHER MACHINES

Section I.   CIPHER DEVICES

141. General

The cipher systems previously described by no means exhaust the category of complex systems, but it is impossible to describe them all. Furthermore, each one presents innumerable possibilities for modification in minor respects and for combination with other methods. In the paragraphs to follow, the principles upon which certain of the more simple cipher devices have been based are described.

142. Wheatstone Cipher[10]

a. The device is a little more than four inches in diameter, and consists of a dial with two hands, as shown in figure 71. The dial is composed of two independent circles of letters. In the outer circle the letters progress clockwise in normal alphabetic sequence, but there is an extra character between the Z and the A, making a total of 27 characters. Some of the spaces also have digits inscribed in them, for enciphering numbers. In the inner circle the letters are arranged in mixed alphabetic sequence and are inscribed either on a surface which permits of erasure, or on a detachable cardboard circle which can be removed and replaced by another circle bearing a different sequence. In figure 71 this inner sequence is a systematically mixed sequence derived from the keyword FRANCE, as follows:

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

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

---

[10] Credit for the invention of the device and system described in this paragraph belongs not to Sir Charles Wheatstone, as has until recently been thought, but to an American, Decius Wadsworth, who in 1817 constructed a device identical in principle with that described on pp. 342-347 of *The Scientific Papers of Sir Charles Wheatstone*, published by the Physical Society of London in 1879. The Wheatstone device used a 27-element outer alphabet (26 letters

b. The two hands are pivoted concentrically, as are the hour and minute hands of a clock. Now, in a clock, the minute hand makes a complete revolution, while the hour hand makes only $\frac{1}{12}$ of a complete revolution; the action in the case of this device, however, is somewhat different. The short hand is free to move independently of the long one, although the motion of the latter affects the former. Since the outer circle has 27 spaces and the inner one only 26, by a simple mechanical contrivance each complete revolution of the long hand causes the short hand to make $1\frac{1}{26}$ revolutions, thus causing the short hand to point one place in advance of where it pointed at the end of the preceding revolution of the long hand. For example, when the long hand is over B of the outer circle and the short hand points to R of the inner circle, if the long hand is pushed clockwise around the dial, making a complete revolution, the short hand will also make a complete revolution clockwise plus one space, thus pointing to D.

c. To encipher a message, the long hand and the short hand are set to prearranged initial positions. It is usual to agree that the plain-text letters will be sought in the outer circle of letters, their cipher equivalents in the inner circle; and that the long hand is invariably to be moved in the same direction, usually clockwise.
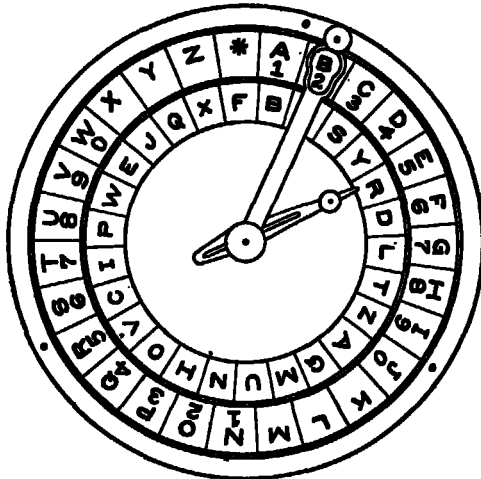

Figure 71.

Suppose the message to be enciphered is SEND AMMUNITION FORWARD. The long hand is moved clockwise until it is directly

and a word-separator), and a 26-element inner alphabet; the Wadsworth device used a 33-element outer alphabet (26 letters and the digits 2–8, inclusive), and a 26-element inner alphabet. Also, whereas in the Wheatstone device only the cipher component could be varied, in the Wadsworth device both components could be varied according to identical or non-identical mixed sequences.

over S on the outer sequence. The letter to which the short hand points is the cipher equivalent of S and is written down. Then the long hand is moved clockwise to a position over E, the letter to which the short hand points is noted and written down. When a double letter occurs in the plain text, as in the case of the double M of AMMUNITION, some infrequently used letter, such as Q, must be substituted for the second occurrence of the letter. To decipher a message, the hands are returned to their initial prearranged position, and then the long hand is moved clockwise until the short hand points to the first cipher letter; the long hand is then directly over the plain-text letter. The process is continued until all the letters have been deciphered.

d. A consideration of the foregoing details shows that the encipherment of a message depends upon a combination of the following variables:

(1) The sequence of letters in the outer circle. In the case just considered, this sequence must be regarded as a known sequence, since it consists merely of the normal alphabet plus one character.

(2) The sequence of letters in the inner circle.

(3) The initial juxtaposition of the two sequences.

(4) The exact composition of the text to be enciphered, since this will determine the number of revolutions of the long hand required to encipher a given number of letters of the message.

e. It is obvious that if the outer alphabet is made a mixed alphabet, as well as the inner, both being different, the cryptograms will be made the more secure against cryptanalysis.

f. The same results as are obtained by using the device can be obtained by using sliding strips of paper, providing the operator will bear in mind that every time a θ_p on the plain component is situated to the left of the preceding θ_p, he must displace the cipher component one interval to the left, if the correspondents have agreed upon a clockwise movement of the long hand, or to the right, if they have agreed upon a counterclockwise movement of the long hand.

143. Jefferson Cipher

a. Credit for the invention of the cipher system and device now to be described belongs to Thomas Jefferson,[11] the original inventor,

---

[11] The late John M. Manly, Ph. D., formerly Captain, Military Intelligence Division, U. S. A., discovered, in 1922, a description of the device among Jefferson's Papers in the Library of Congress (vol. 232, item 41575, Jefferson's Papers). For a photographic reproduction of this historically interesting item, see pp. 189-91 of *Articles on Cryptography and Cryptanalysis Reprinted From The Signal Corps Bulletin*, Signal Security Service Publication, OCSigO, Washington, 1942.

although it was independently invented many years later (1891) by a French cryptographer, Commandant Bazeries, and still later (1914) by Captain Parker Hitt, U. S. Army (now Colonel, U. S. Army, Ret.). Because it was first described in print (1901) by Bazeries, the principle upon which the cipher system is based is usually referred to in the literature as the Bazeries principle; for the sake of historical accuracy, however, it is herein called the Jeffersonian principle.

b. The basis of this principle is the use of a set of 20 (or more, if desired) mixed alphabets arranged in a sequence that can readily be changed; these can be used in the encipherment of a whole set of 20 letters with one and the same displacement of the alphabets. Successive encipherments are accomplished with different displacements of the alphabets.

c. Whereas Jefferson contemplated a device using a total of 36 different alphabets mounted on revolvable disks, the one Bazeries described used only 20 alphabets mounted in the same manner.

144. The Obsolete U. S. Army Cipher Device, Type M-94

a. This cipher device is based upon the Jeffersonian principle, using 25 mixed alphabets on small aluminum disks. It was widely employed in the U. S. military service and to a more limited extent in other U. S. services until 1942, when it was superseded by better devices.

b. In using the device, the 25 disks were first arranged according to the key for the day (the disks bearing the identifying numbers 1–25, and also the letters B–Z), and then the first twenty-five letters of the plain text were set up along a guide rule. The cipher text consisted of *any* one of the other rows, which would be taken off in five groups of five letters each. This process continued until the entire message was enciphered. To decryptograph, it was merely necessary for the deciphering clerk to set up along the guide rule of the device (properly arranged according to the daily key) the first twenty-five letters of the cipher text, and then by inspection find the one and only one row of letters that constituted plain text, which process would be repeated until the entire message was deciphered.

145. Strip Cipher Systems

a. A modification of the Jeffersonian principle which has found merit in practical cryptography is the strip cipher system. This is nothing more than a series of printed, random-alphabet strips to take the place of the disks of the cylindrical devices. These strips, bearing identifying numbers, slide freely in a strip board which may be made of metal, wood, or plastic. The strips are simpler to produce and more economical to replace than metal disks.

b. It is possible to incorporate modifications of the basic idea of the Jeffersonian principle in using strip systems. For instance, there may be a daily selection of strips from a set consisting of a much larger number; or there may be different sets of strips for messages in the various security classifications; or different sets of strips may be issued to different groups of holders, etc.

Section II. CIPHER MACHINES

146. Importance of Cipher Machines in Modern Cryptographic Communication

The remarks made in paragraph 2 regarding the present trends in the art, are believed to be sufficient to give a clear idea of the importance of a knowledge of the uses and limitations of cipher machines as adjuncts to modern cryptographic communications. However, in this text only observations of a general character can be made, leaving for a future text an exposition of detailed principles involved in the construction and operation of a few typical cipher machines. More and more attention is today being devoted to this phase of cryptography and to a large extent cipher machines have replaced code systems even in lower headquarters, except for small, special-purpose codes.

147. Transposition-Cipher Machines

These are rarely encountered; the files of United States patents disclose but two examples and so far as is known no actual machines have been constructed conforming to the specifications covered therein. It may be said that substitution methods lend themselves so much more readily to automatic encipherment than do transposition methods that the possibilities for the construction of cipher machines for effecting transpositions are almost completely overlooked. Basically it would seem that a machine for effecting transposition would have to include some means for "storing up" the letters until all the plain text has been "fed into the machine," whereupon the transposing process is begun and the letters are finally brought out in what externally appears to be a randomized order. It is conceivable that a machine might be devised in which the disarrangement of the letters is a function merely of the number of letters comprising the message; daily changes in the randomizing machinery could be provided for by resetting the elements controlling the process.

148. Substitution-Cipher Machines

a. The substitution principle lends itself very readily to the construction of cipher machines for effecting it. The cipher devices described in the

168

preceding section, as well as the simpler varieties making use merely of two or more superimposed, concentric disks are in the nature of hand-operated substitution-cipher mechanisms that are difficult to use, cannot be employed for rapid or automatic cryptographic manipulations, and are quite markedly susceptible to errors in their operation. For a long time these defects have been recognized and many men have striven to produce and to perfect devices more automatic in their functioning. However, the would-be inventors have not, as a rule, realized the complexity of the problems confronting them; nor have they approached these problems with the necessary and thorough knowledge of both theoretical and practical cryptography, with its many limitations, and theoretical as well as practical cryptanalysis, with its wide possibilities for the exercise of human ingenuity. However, when the problem of developing and producing a good cipher machine is attacked by a competent cryptographic and cryptanalytic engineering staff, highly efficient cipher machines can be developed. At this writing some very excellent machines are now in actual use for practical secret communications.

b. It is obvious that automatic devices of this nature should be equipped with a keyboard of some kind, resembling or duplicating that of an ordinary typewriter. Furthermore, for rapid manipulation these machines must be actuated by mechanisms affording speed in operation, such as electric or spring motors, compressed air, electromagnets, etc.

149. Machines Affording Only Monoalphabetic Substitution

Little need be said of those machines in which the ordinary keys of the keyboard are merely covered with removable caps bearing other letters or characters. They yield only the simplest type of substitution cipher known and have little to recommend them. Even when the mechanism is such that a whole series of alphabets can be brought into play, if the encipherment is monoalphabetic for a succession of 20 or more letters before the alphabet changes, the degree of cryptographic security is relatively low, especially if the various alphabets are interrelated as a result of their derivation from a limited number of primary components.

150. Machines Affording Polyalphabetic Substitution

a. In recent years there have been placed upon the commercial market several cipher machines of more than ordinary interest, but they cannot be described here in detail. In some of them the number of secondary alphabets is quite limited, but the method of their employment, or rather the manner in which the mechanism operates to bring the cipher alphabets into play is so ingenious that the solution of cryptograms prepared by means of the machine is exceedingly difficult. This point should be clearly recognized and understood: *other things being equal, the manner*

169

of shifting about or varying the cipher alphabets contributes more to cryptographic security than does the number of alphabets involved, or their type. For example, it is quite possible to employ 26 direct-standard alphabets in such an irregular sequence as to yield greater security than is afforded by the use of 1,000 or more mixed alphabets in a regular or an easily-ascertained method. The importance of this point is not generally recognized by inventors.

b. One of the serious limitations upon the development of good cipher machines is that the number of letters in our alphabet, 26, does not lend itself well to mechanical or mathematical manipulation, because it has but the factors 1, 2, and 13; nor is it a perfect square. If the alphabet consisted of 25, 27, or 36 characters, much more could be done. The addition of figures or symbols to the 26-letter alphabet introduces the serious practical difficulty that the cryptograms will contain characters other than letters and the cost of transmitting intermixtures of letters, figures, and symbols by Morse telegraphy is prohibitive. Subterfuges of one sort or another, employed to circumvent this difficulty, are usually impractical and expensive.

151. The Converter M–209

a. This machine, widely used for low-echelon U. S. Army communications, is a small, compact, hand-operated, tape-printing, mechanical cipher machine, weighing 6 pounds, with dimensions $7\frac{1}{4}''$ x $5\frac{7}{16}''$ x $3\frac{1}{2}''$. The cryptographic principle of this machine embodies polyalphabetic substitution, employing a complex mechanical arrangement to generate a long running key which is used in conjunction with reversed standard alphabets for the primary components. Despite the period of 101,405,850 before the keying cycle repeats, nevertheless a high degree of security can be imparted to messages enciphered by means of this converter *only* if the machine is properly used according to authorized instructions and if the messages are drafted with proper regard for security.

b. Space does not permit the inclusion of details of operation, etc., of this machine. However, full instructions as to its use, maintenance, and repair will be found in TM 11–380, "Converter M–209, M–209–A, M–209–B (Cipher)".

152. Advantages and Disadvantages of Cipher Machines

a. The principles underlying the various machines which have thus far been developed are so diverse and complex that no description of them can be undertaken in this text. However, a few remarks of a general character, dealing with the advantages and disadvantages of cipher machines in military communications today, are deemed pertinent.

170

b. Until a few years ago, code methods were predominant in military cryptography within the United States Army but the reverse is now the case. This important change has been the result of advances made within comparatively recent years in the design and construction of cryptographic systems and apparatus. It may be useful to compare code methods in general with methods based upon cipher devices and cipher machines in general to note the advantages and disadvantages of each category of methods.

    c. (1) When designed for keyboard operation and equipped with a standard typewriter keyboard, cipher machines afford much more speed in encipherment and decipherment than do any "hand-operated" cryptographic methods, including codes and certain types of cipher devices. Comparative speed tests gave the following data recently:

Number of groups or words per minute

Method*	Cryptographing	Decryptographing
1	4.04 (4-letter or 4-figure groups)	.... 6.00
2	1.94 (4-letter or 4-figure groups)	.... 2.26
3	1.75 (5-letter groups)	.... 1.78
4	2.74 (5-letter groups)	.... 3.98
5	3.14 (5-letter groups)	.... 3.54
6	30.00 (5-letter groups)	.... 25.00

*Method 1—A 2-part code of 6,000 groups unenciphered.
Method 2—The same code enciphered by a secure system.
Method 3—The obsolete U. S. Army Cipher Device, Type M-94.
Method 4—A small electrical cryptographic machine giving lamp indications but not provided with a typewriter keyboard.
Method 5—The Converter, M-209.
Method 6—An electrical cryptographic machine producing a printed record and provided with a keyboard.

    (2) When properly designed, cipher machines and certain types of "hand-operated" cryptographs afford greater guarantees of cryptographic security than do code methods or hand-operated "pencil and paper" cipher systems, because machines can accurately, speedily, and tirelessly perform far more complex cryptographic operations than can possibly be performed even by the most skillful cryptographers working with code books and cipher tables, or with hand-operated cipher systems.

    (3) Though the initial cost of a cipher machine may compare unfavorably with the initial cost of a code book, the over-all cost of maintaining cryptographic security by means of cipher machines is probably less than that in the case of code systems. Good machines designed by technically qualified experts afford a multiplicity of keying arrangements; once distributed there

171

is no necessity for recalling "old editions" and substituting "new editions," as is the case with code books. Therefore, the labor costs incident to the necessity for repeated preparation, printing, and distribution of code books, together with the labor costs incident to the necessity for repeated accounting operations, correspondence exchanges relative to issue, receipt, etc., in the end overbalance the higher initial cost of cipher machines. In this connection it should be stated that merely the cost of printing an edition of 200 copies of a large 2-part code is well over $25,000. This does not include the cost of the labor involved in the compilation of the code, nor of that involved in preparing, printing, and binding cipher tables for superencipherment, etc.

(4) The security of a cryptographic system involving the use of a properly designed cipher device or cipher machine is not wholly dissipated by the capture or compromise of the machine or device itself, as is the case with a code book.

(5) On the other hand, it must be admitted that, as a general rule, the solution of a very few cryptograms by long and laborious cryptanalysis makes it possible, in the case of a cipher machine, to decryptograph more or less readily many or all other cryptograms enciphered by the same machine with the same (or in certain cases) different "settings," keys, or elements; whereas in the case of a large 2-part code the solution of a few code messages can hardly be accomplished at all, and practical analysis of the code must await the accumulation of a large amount of traffic. Even should the plain text of one or two code messages be obtained by theft or capture, this would not permit the prompt decoding of subsequent messages in the same code; whereas this may be possible in the case of cipher messages.

(6) Again, cipher machines are, as a rule, complicated and delicate mechanisms. They require considerable technical skill for their proper operation by cryptographic clerks, skill which may not always be possessed by such personnel. What is perhaps more important, complicated cipher machines require the skill and services of special personnel for their proper maintenance and repair. They usually require electric current for operation, which may not always be available.

(7) If the cipher machine employed is at all complicated to set up for enciphering and deciphering, errors are easy to make and sometimes call for costly or laborious exchanges of service messages relative to their correction. However, this may be a doubtful point because complex superenciphered code is just as subject to errors as is a complex cipher machine.

(8) As regards administrative communications, cipher cannot compete with code from the point of view of condensation or abbreviation. A cipher message is always at least as long as the original plain-text message, whereas a code message prepared by means of a large code specially compiled to give a high degree of condensation is usually much shorter than the equivalent original plain-text message. This arises, of course, from the fact that in well-constructed code books single groups of 4 or 5 characters may represent long phrases or even whole sentences.

(9) As a rule, cipher devices or machines cannot readily be operated under all sorts of weather conditions. In very damp or in rainy climates, machinery failures are quite common, and it is difficult to keep delicate machines in regular service. Moreover, in hot, humid climates no machines can long survive the disastrous corrosive effects of moisture, vegetable growths, etc., whereas printed matter is hardly affected by these elements. Finally, under field conditions, while a code book can be manipulated outdoors in all sorts of weather, in rain, sleet, or snow, in high altitudes where the temperature is very low, or in the tropics where it is very hot and humid, a cipher machine, especially if electrical, often cannot be operated with success for more than a few minutes or, at most, a few hours.

CHAPTER 12

CODE SYSTEMS

Section I.   GENERAL

153. General

a. Chapter 4 was devoted to a general consideration of code systems and enciphered code. It was there indicated that code systems are systems of substitution where the elements of the substitutive process, comprising letters, syllables, words, phrases, and sentences, are so numerous that it is impossible to memorize them or to reconstruct them at will when necessary, so that printed books containing these elements and their code equivalents must be at hand in order to cryptograph or decryptograph messages. The various types of code groups were indicated, together with methods for their construction by means of permutation tables. One-part and two-part codes were briefly discussed. Finally, a few words were added for the purpose of indicating various types of enciphering code for greater cryptographic security.

b. Practical cryptography must take cognizance of the fact that the texts of governmental as well as commercial and social telegrams must conform to certain standard forms and practices. A subsequent text will go into these matters but at this moment it is only necessary to indicate that international telegraph regulations in the past have exercised an important influence upon the structure of code groups and upon the selection of cryptographic systems for their encipherment.

c. In the subsequent paragraphs, when reference is made to *numerical code groups*, or *number-code groups*, or *figure-code groups*, it will be understood that the code groups are composed of digits; when reference is made to *alphabetical code groups*, or *letter-code groups*, or *letter groups*, it will be understood that the code groups are composed of letters of the alphabet; and when reference is made to *mixed code groups*, or *mixed groups*, it will be understood that the code groups are composed of intermixtures of letters and digits.

154. Intermixtures of Code-Text and Other Kinds of Text

a. Only in commercial code messages is the practice of mixing plain text and code text common in modern communications. In governmental code messages, military, naval, or diplomatic, such intermixtures are today so rare that their presence in telegrams indicates abysmal ignorance

174

of some of the fundamental rules of cryptographic security. Because the plain-text words give definite clues to the meaning of the adjacent code groups, even though the former may apparently convey no intelligibility in themselves (such words as *and, but, by, comma, for, in, period, stop, that, the,* etc.), their presence constitutes a fatal danger, and no cryptographer who is aware of this danger will countenance such intermixtures.

b. It often happens that correspondents employ a code which makes no provision for encoding proper names or unusual words not included in the vocabulary of the code book. Rather than leave the unencodable text in plain language in the message, *since its appearance will surely lead to clues to unauthorized reading of the message,* the correspondents encipher such words and proper names by means of any prearranged cipher system. Also, in some cases, when the code is limited in its vocabulary and the various inflections of words are not represented, the correspondents may suffix the proper inflections ("ed," "ing," "tion," etc.) in cipher. This procedure, however, is not to be recommended, because it considerably reduces the cryptographic security of the whole system.

c. Sometimes correspondents make use of two or more codes within the same message. This is occasionally the case when they are making use of a general or commercial code which does not have all the special expressions necessary for their business, the latter expressions being contained in a small private code. Sometimes, however, the intermixture of code text from several codes is done for the purposes of secrecy, though it is, as a rule, a rather poor subterfuge.

Section II. ENCIPHERED CODE

155. General

a. The purposes of enciphering code have already been explained together with brief indications of methods. The superimposition of a good cipher system upon the code text of a message is a safe and practical method of cryptography for governmental use, where more rapid machine methods are not available.

b. In the subsequent paragraphs, for brevity and ease in reference, the term *placode*[12] will be employed to designate the actual or unenciphered code groups representing the plain-text elements; the term is derived by telescoping the words *plain* and *code.* On the other hand, the term *encicode*[12] will be employed to designate the final product of the superencipherment; it is likewise derived by telescoping the words *enciphered* and *code.*

---

[12] Pronounced "play-code" and "en-sigh'-code."

c. The terms *superenciphered code, superencipherment,* or (British) *reciphered code* and *recipherment* all apply to code text which undergoes a subsequent process of encipherment.

d. The terms *indicator system* and *indicator* are very important in connection with all cryptographic procedures but especially so in connection with enciphering systems as applied to code. The indicator gives information relative to the proper tables to use, or the proper point to begin in such tables, etc. Further information in this regard will be given in subsequent paragraphs.

156. General Types of Methods of Superencipherment

Both transposition and substitution methods may be applied to superencipher code. There are arithmetical methods which at first glance appear to constitute a third category of superencipherment methods since they involve mathematical processes apparently resembling neither transposition nor substitution. However, deeper study will lead to the conclusion that these arithmetical methods are substitutive in character.

157. Transposition Methods

a. Transposition methods wherein whole code groups or series of them are shifted about according to some key are not frequently encountered. Transposition methods applied strictly within the code groups, by rearrainging or shifting about the letters or figures composing them, have been used to a limited extent for a number of years. Prior to January 1, 1934, transposition processes for producing encicode messages, that is, for superenciphering code, were practically never employed in commercial or governmental practice because they destroyed the regular vowel-consonant structure of code groups so that they no longer conformed to the requirements of the international telegraph regulations referred to in paragraph 153*b*. However, the restrictions in this respect were lifted on the date indicated and it may be expected that transposition processes for superenciphering code will be encountered much more frequently than in the past.

b. One of the most commonly used transposition methods for this purpose is simple keyed-columnar transposition, either with special matrices, designs, or forms having nulls and blanks, or without these features. The system as a whole, however, is very subject to error and requires high-grade personnel for its practical operation. It is, of course, wholly unsuited for practical military usage, though it can be employed for other purposes. Solution of such a system if well constructed is a very difficult matter, especially if the basic code book is not known,

158. Substitution Methods

a. GENERAL. All of the methods of substitution applicable in the case
of cipher systems are available for use in superenciphering code.

b. MONOALPHABETIC METHODS. It is, of course, easy to draw up one
or more single-mixed alphabets. When the code book is in possession of
the enemy cryptanalysts and the original or placode groups are therefore
at hand, this method does not yield any security, for reasons not neces-
sary here to indicate. Even when the actual code book is not known, but
it is known that it is one of a set of commerical codes having groups of
the 2-letter difference type, the reconstruction of the cipher alphabets is
not difficult.

c. POLYALPHABETIC METHODS.

(1) A very simple polyalphabetic method is to have 5 alphabets
which are used in succession; or there may be a series of sets
of 5 alphabets, the individual set to be used being determined
by indicators inserted in the message itself.

(2) Any sort of polyalphabetic method may be used. For example,
the repeating-key method, the running or continuous-key
method, the interrupted-key method, etc., can be applied.
Digraphic methods may also be used; also, combinations of
digraphic and monographic methods are frequent.

(3) Tables of various sorts are often employed. For example, using
a table applicable to code groups of 5 figures, a table giving
pronounceable combinations of letters for the combinations of
digits may result in converting a group such as 75152 into the
letter group KOBAL. Tables for substituting combinations of
letters into other combinations of letters are, of course, equally
feasible. The substitution may be strictly digraphic, combining
two 5-letter or 5-figure groups into a series of 10 digraphs; or
it may be a combination of trigraphic and digraphic substitu-
tion, each 5-character group being split up into a 3-character
and a 2-character combination. Other combinations are, of
course, also possible.

(4) In all the foregoing methods the chief objection is that the
advantage of the 2-letter differential feature is more or less
dissipated by the encipherment, but this is true of every sub-
stitutive method that is superimposed on code.

(5) The disadvantage referred to in the preceding subparagraph is
absent in those cases in which the encipherment operates merely
to substitute other code groups of the same book for the mes-
sage code groups. The most common methods of this type
make use of the figure-code groups, the latter being manipulated
in various ways to change them and the resulting groups then

177

being given their letter-code equivalents. Some of these methods are explained below.

159. Arithmetical Methods

These are the most important of the various methods of superenciphering code, and must be dealt with in somewhat greater detail than the foregoing methods. There are several different types of treatment, each of which will be briefly discussed in the subsequent subparagraphs.

160. Single or Fixed Additives

a. If the code groups are numerical, the addition of an arbitrarily selected number to each code group in the code message constitutes a simple form of superencipherment. It may be varied by prearrangement between correspondents, simply by changing the fixed number as frequently as may be deemed necessary, or by some easily arranged system of change. The group of digits composing the number which is added to the placode values is commonly termed an *additive group*, or, more often, an *additive*, or sometimes simply an *adder*. In decipherment, the additive is merely removed from the received encicode groups by subtraction, leaving the placode groups, which can then be decoded by reference to the code book. Often the date or some number derivable from the date is employed as the additive but usually the number is simply an arbitrarily composed group of digits. Because the same number is employed throughout the encipherment of the entire code message, such an additive is called a *fixed additive*.

b. Methods such as the foregoing are particularly weak cryptographically if the basic code book and the code groups embody limitations in construction. For example, should it be employed in connection with a code having only 3,000 groups numbered consecutively from 0000 to 2999, then the initial digits of the groups are limited to the three digits 0, 1, and 2; the application of a fixed additive can therefore produce only three different digits as the initial digits of the encicode text. This phenomenon would, of course, soon lead to the determination of the initial digits of the placode groups.

c. One rather simple scheme involving the use of fixed additives in the case of codes having alphabetical as well as numerical code groups is to apply the fixed additive to the numerical code groups representing the plain-text words or phrases and then take the alphabetical code groups corresponding to the sums as the final encicode groups. In codes of this type the additives may be rather large numbers and the process of finding the alphabetical code groups corresponding to the sums is very easy. But in codes wherein only alphabetical code groups are listed, that is, no figure-code or numerical groups are also given, the additives employed must naturally be rather small numbers. It would be extremely

178

laborious to count 573 groups forward, for example. In cases such as these additives limited to numbers from 1 to 20 or 30 are common.

    d. (1) Instead of *adding* a fixed number in encipherment, the latter may be subtracted, in which case, in decipherment, the fixed number must be added to the encicode groups as received. Such a group may be termed a *subtractive group,* or *subtractor,* because subtraction is the process used in encipherment; in decipherment the group becomes, of course, an additive.

        (2) Addition and subtraction of a fixed numerical group may be alternated within the same message, according to some simple subsidiary key; for example, a series of additive groups corresponding to the keyword BAD might, by prearrangement, consist of the numbers 200, 100, 400. These might be used in repetitive manner. Or the correspondents might agree to use these key numbers alternatively in additive and subtractive manner, such as +200, −100, +400, −200, +100, −400, +200, −100, etc.

    e. Addition without "carrying," or *noncarrying addition,* is just as simple as *normal addition,* that is, addition with "carrying"; and subtraction without "borrowing," or *nonborrowing subtraction,* is just as simple as *normal subtraction,* that is, subtraction with "borrowing." It is merely necessary that the correspondents agree in advance on this point and apply the process consistently throughout a message. In practice, however, it is more common to perform these processes without "carrying" or "borrowing," *so that the operations can be performed from left to right as in normal writing.* Following is an example which will make the matter clear.

Example A

(a) Example of *"noncarrying" addition* in encipherment:

(1) Placode........................	5517	3082	9015	6710	9541
(2) Fixed group for addition.........	5678	5678	5678	5678	5678
(3) Encicode........................	0185	8650	4683	1388	4119

(b) In decipherment, *"nonborrowing" subtraction* is applied:

(1) Encicode........................	0185	8650	4683	1388	4119
(2) Fixed group for subtraction.......	5678	5678	5678	5678	5678
(3) Placode........................	5517	3082	9015	6710	9541

(c) Note that in the *decipherment* process the *encicode* serves as the *minuend,* the additive used in the encipherment serves as the *subtrahend,* and the placode is the *remainder.*

    f. In the foregoing example the additive remains the same throughout the superencipherment but it is obvious that this is only the simplest sort of an arrangement. A *series of different additives* may readily be employed, as will be explained later.

179

g. (1) *Cryptographic procedure.* It is, however, possible to make the cryptographic procedure the same in both encipherment and decipherment, by proper changes in method. *They can both be made either additive or subtractive in nature, thus requiring the learning of but a single process.* Two methods will be explained below.

(2) *Both processes additive.* If in encipherment an additive process is used, and if in decipherment the *complement* of the additive employed in encipherment is then *added* to the encicode groups, the decipherment also becomes an additive process. For example, the complement of the group 5678, on a basis of 10, is 5432. Note the following:

Example B

(a) Example of "noncarrying" addition in encipherment:

(1) Placode.........................	5517	3082	9015	6710	9541
(2) Fixed group for addition.........	5678	5678	5678	5678	5678
(3) Encicode........................	0185	8650	4683	1388	4119

(b) In decipherment, using the complement of the additive used in encipherment, *addition* reproduces the placode:

(1) Encicode........................	0185	8650	4683	1388	4119
(2) Complement of fixed group.......	5432	5432	5432	5432	5432
(3) Placode.........................	5517	3082	9015	6710	9541

(3) *Both processes subtractive.* By a very simple change in procedure it is possible to apply subtraction in *both* encipherment and decipherment, using the *same* numerical groups as *subtractors,* thus making it necessary to learn only one process. If the additive, instead of being in the second line of the three lines shown in the foregoing examples, is placed on the first line, and a subtraction process applied, the proper results are obtained *regardless of whether encipherment or decipherment is involved.* Note the following example:

Example C

(a) Example of "nonborrowing" subtraction in encipherment and decipherment:

(1) Fixed group.....................	5678	5678	5678	5678	5678
(2) Placode.........................	5517	3082	9015	6710	9541
(3) Encicode........................	0161	2696	6663	9968	6137

(b) Decipherment (*subtraction also*):

(1) Fixed group.....................	5678	5678	5678	5678	5678
(2) Encicode........................	0161	2696	6663	9968	6137
(3) Placode.........................	5517	3082	9015	6710	9541

180

(c) Note that in the *encipherment* process the keying group serves as the *minuend,* the *placode* as the *subtrahend,* whereupon the *remainder* becomes the *encicode;* in the *decipherment* process the keying group again serves as the *minuend,* the *encicode* as the *subtrahend,* whereupon the *remainder* becomes the *placode.*

(4) *Explanation.* The explanation involves a consideration of the nature of the processes themselves when looked at from the point of view of simple algebra. Note the following, where the symble x denotes placode, y denotes the fixed group, and z denotes encicode:

In example A (a)... $x+y=z$
Transposing.. $x=z-y$
That is.. $z-y=x$

It is seen here that y must be *subtracted* from z in order to recover x and in order that x may be a positive quantity. Thus, this method involves both addition and subtraction.

But in example C (a)...................................... $y-x=z$
Transposing... $y-z=x,$

which is exactly what is done in Example C (b). Hence it is seen that in the case of this second method only subtraction is involved, *in both processes.*

h. The method illustrated in Example C is becoming more common, because of its simplicity and ease in manipulation. It is termed the *subtractor method* and the numerical groups employed as keying groups are called *subtractors.* In paragraph 162 more will be said about this method.

161. Repeating or Recurring-Key Additives and Subtractors

a. In the foregoing examples the number which was added or subtracted in encipherment was always the same but this need not, of course, be true. It is possible to employ a *sequence* of numbers for addition or subtraction, the sequence being agreed upon in advance or it may be easily derivable from a key phrase, etc. Thus, suppose the placode message is the same as in the previous examples and that the repeating key is 432809721 and that this key is employed according to the subtractor method explained in paragraph 160*g* (3). Note the following:

(a) Encipherment:

(1) Repeating key....................	4328	0972	1432	8097	2143
(2) Placode.........................	5517	3082	9015	6710	9541
(3) Encicode........................	9811	7990	2427	2387	3602

(b) Decipherment:

(1) Repeating key....................	4328	0972	1432	8097	2143
(2) Encicode........................	9811	7990	2427	2387	3602
(3) Placode.........................	5517	3082	9015	6710	9541

b. It is important to note that such a key as the foregoing must be of a length that does not contain a factor in common with the length of the code groups involved in the encipherment, for if it does contain a common factor the period will be abbreviated. For example, in the foregoing case, since the repeating key contains 9 digits and the code groups 4 digits, the length of the enciphering period is 9 groups, that is, two identical placode groups must be at least 9 groups apart before they will produce identical encicode groups. But if the keying sequence were 10 digits in length this phenomenon of cyclic repetition could happen if the identical placode groups were but 5 groups apart, since the common factor 2 cuts the potential keying length in half; and if the keying sequence were 12 digits in length the period would be but 3 groups. In this connection see also paragraph 131 *c.*

162. Nonrepeating Additives and Subtractors

a. When special tables are employed as the source of the adders or subtractors for superenciphering code, a much more secure system is provided. The tables may be contained in a book or document called a *keybook,* an *additive book,* or a *subtractor book.* On each page of such a book groups of numbers are regularly disposed in rows and columns on the page. By applying identifying symbols called *indicators* to the pages, as well as to the rows and the columns on each page of the keybook, it is possible to provide for the safe superencipherment of a large volume of traffic. All correspondents must, of course, be provided with the same basic code book and the same keybook. In employing the keybook the *indicators* tell the recipient of a message what groups were used; that is, where to begin in the decipherment of the encicode. A page from a typical keybook of this sort is shown in figure 72.

b. It should be noted that whether the arbitrary numerical groups in the keybook are employed as *adders* or as *subtractors* has nothing to do with the nature of the groups themselves: the latter may be used either way, provided consistency is observed and the correspondents agree as to whether the groups will be employed throughout the messages in the additive manner (in encipherment) illustrated in Example A (a) in paragraph 160*e,* or in the subtractor manner illustrated in Example C (a), in paragraph 160*g.* In figure 72 are shown two sets of 100 4-digit groups, disposed in numbered blocks each containing 10 columns and 10 rows of groups. To designate a group as the initial one to be employed in encipherment, or decipherment, it is merely necessary to give the block number, the row number and the column number of the group. For example, 0116 is the indicator for the group 8790. It is usual to take the successive groups in the normal order of reading, that is, from left to right and from the top downwards, although any other order of reading may be agreed upon between correspondents. The book from which this

182

BLOCK 00

	1	2	3	4	5	6	7	8	9	0
1	0378	9197	3260	3607	2699	9053	9733	1844	6622	4213
2	7185	0135	6091	2387	4957	3113	7284	0750	3501	1945
3	5037	3365	1294	8261	2149	0718	3678	2510	7238	5268
4	8004	5199	3859	1293	5311	3550	9915	0512	1518	3776
5	9282	6893	4229	9736	0927	1418	1930	9864	0090	8974
6	7259	9399	0769	3144	9801	1378	4732	5134	1435	5282
7	2878	9963	7943	4519	3404	9810	0190	4467	7069	5348
8	1620	5879	0218	1064	9560	5732	6661	0883	1883	2619
9	3868	1905	2500	6654	0824	3710	3875	6332	1503	7259
0	4319	3298	7819	8721	1549	6630	6301	5701	3586	1907

BLOCK 01

	1	2	3	4	5	6	7	8	9	0
1	9328	1135	3871	1549	0839	8790	1771	8251	3274	1173
2	2297	9550	5033	0102	6817	5597	0847	4038	1200	2949
3	3640	3984	3299	1181	3811	8844	2500	4557	4133	0487
4	1456	9614	5520	8372	1941	2417	1098	4039	3943	8282
5	1751	4254	8479	8647	2684	5511	8680	4660	3858	4266
6	3643	0445	4673	6178	5250	4310	9580	0481	1005	4100
7	5875	0710	7652	5415	6851	6001	9668	2109	8471	3276
8	4555	9772	0128	2171	6835	3142	9514	1478	9746	7625
9	0183	2959	3757	7481	4398	4586	8143	8049	7478	8417
0	5072	4405	4128	9068	5023	4374	7741	6373	9454	7733

Figure 72.

183

example was taken consisted of 50 pages each containing 200 groups, making 10,000 in all. The groups themselves, of course, consist merely of digits selected *at random* when the keybook is in preparation.

c. Referring back to the method illustrated in Example B in paragraph 160*g* (2), in which addition is employed in both encipherment and decipherment, it was noted that in decipherment the *complement* of the additive employed in encipherment must be used in order to recover the placode. This principle serves as the basis for preparing keybooks in which half the contents are additives, the other half, their complements. By proper manipulation of indicators it is possible to use any given page of the arbitrary groups for encipherment, whereupon a specific page (containing the complements) must be used for decipherment. This method obviously requires considerable care in preparing the keybooks, so as to insure that complementary pages are present and are properly indicated; it also involves much more care to insure that the groups on complementary pages are accurate, although there are mechanical methods of preparing series of complements of this type.

d. If a keybook for an additive or a subtractor system is used *once and only once,* security of an absolute order is imparted to the messages *even if the basic code book is known to and possessed by the enemy.* It is not even necessary to use indicators except where a question may arise as to the serial order of one of two or more messages arriving at about the same time. In such a case the system is referred to as a *one-time system* and the keybook is called a *one-time pad* because the pages are usually fastened securely in the form of a tablet or pad and are destroyed as soon as it is certain that the recipient of a message has properly deciphered and decoded it. The disadvantages of such a system are two in number, both very serious. In the first place the production and distribution of the pads present very difficult problems in composition, printing, assembly of sheets, etc. For voluminous correspondence many pads are necessary and the mere question of the production, timely distribution, and proper safekeeping of the pads is a serious one. In the second place, a system such as this is suitable for *only two correspondents* and even in this case there usually must be two pads, one for incoming, the other for outgoing messages, otherwise it will occasionally or frequently happen that both correspondents will use the same series of additives or subtractors.

e. The foregoing difficulties make it desirable to modify the system so that while its security may not be absolute it can be employed by a larger number of correspondents, cutting down on the number of pads required and permitting of intercommunication among all correspondents. For such use, indicators are absolutely essential in order to facilitate the prompt decipherment of messages received from several different correspondents.

f. The security of a scheme such as the foregoing is dependent upon the manner in which the indicators are treated in the cryptographing processes. If the indicators are given *in clear*, that is, without disguise of one sort or another, it becomes possible to study a series of encicode messages and perhaps to solve them, even without possession of the code. On the other hand, if the indicators are themselves disguised by enciphering them according to a well-designed method, the system as a whole becomes very secure and may, indeed, be made impregnable against attack for a very long time.

163. Observations on Arithmetical Methods

a. It can be perceived by this time that the foregoing arithmetical methods are, in reality, substitution methods. Where a fixed group is added or subtracted from the placode group this is easy to see. For example, if the fixed additive is 3089 and the placode group is 8752, the encicode group is 1731. This is the same as saying that a 4-alphabet system is involved, and the alphabets are as follows:

Placode...........	1	2	3	4	5	6	7	8	9	0	
Alphabet No. 1	4	5	6	7	8	9	0	1	2	3	"Cipher"
Alphabet No. 2	1	2	3	4	5	6	7	8	9	0	
Alphabet No. 3	9	0	1	2	3	4	5	6	7	8	
Alphabet No. 4	0	1	2	3	4	5	6	7	8	9	

Note that merely a simple cyclic displacement of values is involved in the process, the amount of displacement being governed by the particular digit in each position of the additive group. What this amounts to, in cryptographic terms, is a four-alphabet encipherment using direct standard alphabets, where the "normal alphabet" is 1 2 3 4 5 6 7 8 9 0. The process could be made more difficult by employing "mixed alphabets" of course, but then the feature of speed, which is now possible (in view of early training in addition, whereby the mental arithmetic involved becomes second nature), would be lost, since constant reference would have to be made to enciphering and deciphering tables.

b. It becomes clear that when a series of different additives or subtractors is used, as when a keybook is employed, then the number of alphabets involved corresponds to the number of digits employed. Thus, despite the fact that the encipherment process is here one that involves merely the numerical equivalents of direct standard alphabets, the system can have great cryptographic security, depending upon (1) how long the keying sequence is, that is, the number of groups comprising the additive or subtractor series; (2) the composition of this keying sequence, that is, whether it consists of random digits or is systematic in its construction; and (3) whether this sequence or parts of it are used only once or several times. The last-mentioned factor is the most

important of the three, for if the keying sequence or parts of it are used but once or a very limited number of times, say 2 or 3, its recovery by cryptanalytic processes is difficult or impossible and therefore even if the sequence is systematic in its construction this fact might not become known. However, as a rule the additives or subtractors are merely digits selected by a purely random means, such as drawing them out of a box, or equivalent means. The length of the sequence is guided only by the amount of traffic to be superenciphered; for a voluminous traffic, keybooks containing thousands of groups are necessary, even with a good indicator system, and even then the books must be changed at frequent intervals.

c. Arithmetical methods are favored above most other methods of superencipherment because of their simplicity and relatively better speed of operation than in the case of alphabetical methods. The speed factor is, of course, attributable to the fact that practically everybody can add (or subtract) rapidly and accurately when single digits are involved, and although very similar processes could be applied in cryptographic processes involving letters of the alphabet, the operations of addition or subtraction would proceed very much more slowly because early training does not devote any time to arithmetical processes involving letters. For example, every child learns that "8 plus 5 equals 13" but none learns that "H plus E equals M."

d. However, these arithmetical methods have two serious disadvantages. First, there is the disadvantage that the final encode text is composed of numbers. The latter are not only more subject to errors in telegraphic handling than are letters, but also it is more difficult to correct garbled groups when figures are involved than when letters are involved. These disadvantages are, it must be admitted, more serious in American practice, when emphasis in training is laid upon the telegraphic transmission of letters and not figures, than they are in other practices; they may not hold in regard to countries where the emphasis in training is in the other direction, figures being preferred to letters. Second, the physical procedures involved in the preparation, reproduction, distribution, and accounting of the necessary keybooks of adders or subtractors are tedious, costly, and time consuming. Where provision must be made for voluminous intercommunication among many units and for relatively long periods of time, these matters constitute a difficult if not impossible problem for the compiling agency.