~~CONFIDENTIAL~~ REF ID:A64691

~~RESTRICTED~~

THE DISTRIBUTION OF THIS SPECIAL TEXT WILL BE RESTRICTED TO REGULARLY ENROLLED EXTENSION COURSE STUDENTS, TO MILITARY PERSONNEL, AND TO OTHER PERSONS COMING WITHIN THE MEANING OF THE PHRASE "FOR OFFICIAL USE ONLY."

ARMY EXTENSION COURSES

Words taken from WFF's home

SPECIAL TEXT No. 166

ADVANCED MILITARY CRYPTOGRAPHY

SECOND (1943) EDITION

PREPARED UNDER THE DIRECTION OF THE CHIEF SIGNAL OFFICER
FOR USE WITH THE ARMY EXTENSION COURSES

~~RESTRICTED~~

NOTICE.—This document contains information affecting the national defense of the United States within the meaning of the Espionage Act (U. S. C. 50: 31, 32). The transmission of this document or the revelation of its contents in any manner to any unauthorized person is prohibited.

UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON : 1943

2683

~~CONFIDENTIAL~~

30 April 1959

This document is re-graded ~~"CONFIDENTIAL"~~ UP of DOD Directive 5200.1 dated 8 July 1957, and by authority of the Director, National Security Agency.

Paul S. Willard
Colonel, AGC
Adjutant General

WAR DEPARTMENT,

WASHINGTON, *February 2, 1943.*

This revision of Special Text No. 166, Advanced Military Cryptography (1935), for use with the Army Extension Courses, is published for the information and guidance of all concerned.

BY ORDER OF THE SECRETARY OF WAR:

G. C. MARSHALL,
General,
Chief of Staff.

OFFICIAL:

JAMES A. ULIO,
Major General,
The Adjutant General.

SPECIAL TEXT NO. 166

ADVANCED MILITARY CRYPTOGRAPHY

1943 EDITION

		Paragraphs	Page
SECTION I.	Introductory remarks	1– 2	1
	A. TRANSPOSITION SYSTEMS		
II.	Monophase transposition systems	3– 9	5
III.	Polyphase transposition systems	10– 12	17
IV.	True double transposition	13– 14	20
V.	Grilles and other types of matrices	15– 24	24
VI.	Miscellaneous transposition systems	25– 28	39
	B. SUBSTITUTION SYSTEMS		
VII.	Polygraphic systems	29– 31	41
VIII.	Checkerboard digraphic substitution	32– 37	51
IX.	Complex substitution systems	38– 45	61
	C. REPETITIVE AND COMBINED SYSTEMS		
X.	Repetitive systems	46– 49	68
XI.	Combined substitution—transposition systems	50– 58	70
	D. CRYPTOGRAPHS AND CIPHER MACHINES		
XII.	Cryptographs	59– 62	81
XIII.	The obsolete U. S. Army cipher device, type M–94	63– 69	85
XIV.	Cipher machines	70– 75	95
	E. CODE SYSTEMS		
XV.	Code systems in general	76– 77	100
XVI.	Enciphered code	78– 86	102

SECTION I

INTRODUCTORY REMARKS

	Paragraph
Résumé of preceding information	1
Sequence of study	2

1. Résumé of preceding information.—*a.* In Special Text No. 165 (1935), Elementary Military Cryptography, the student was given his first introduction to the study of the more simple means and methods of secret writing. Considerable attention was devoted to certain preliminary data in the nature of definitions of basic terms employed in cryptography and of the general circumstances surrounding the use of cryptography in military communications. The factors determining the influence or effect that the analysis of military cryptograms will have on the tactical situation were discussed somewhat in detail, and it was shown that of these factors the most important is the degree of cryptographic security inherent in the cryptographic system itself. This was then discussed in detail in connection with related factors involved in the length of time required to solve military cryptograms. Attention was also directed to information bearing upon the employment of cryptography in our Army, and the functions, duties, and responsibilities of the various arms and services concerned in it were set forth. Coming then to a discussion of certain preliminary details of a practical nature, it was shown that systems suitable for the military use must conform to certain more or less rigid requirements before they can even be considered for such use because of the present-day limitations of the art of signal communication in general.

b. Having assimilated all the foregoing data of an introductory nature, the student then took up the study of the two principal classes of cryptograms: transposition and substitution. Various examples of cipher systems of the transposition class were first illustrated, these starting out with the simplest varieties of monoliteral route transposition and then progressing through more complex types of simple columnar and keyword columnar methods. Only a hint was conveyed as to the existence of far more complicated double and triple transposition systems. The principal disadvantages of transposition methods in general were discussed. Then substitution systems were taken up and after a brief discussion of the nature of alphabets in general and of the kinds of cipher alphabets in particular, a few examples of simple monoalphabetic substitution ciphers were given.

Methods of producing mixed alphabets were illustrated, and the use of sliding basic sequences to derive a set of secondary alphabets was described. Cases of monoalphabetic substitution with variants were presented and their disadvantages from the point of view of cryptographic security were discussed. It was stated that despite a multiplicity of values for cipher equivalents, such methods do not yield cryptograms of a high degree of security, and for this reason other methods of producing a multiplicity of values, based upon true polyalphabetic methods, are more satisfactory. The use of cipher disks and cipher tables of various sorts was discussed in connection with more complicated types of substitution, and their disadvantages pointed out. Mention was made of methods of increasing the degree of cryptographic security by suppressing or eliminating the manifestations of periodicity in polyalphabetic systems based upon the use of a repeating key. These led to a consideration of the development and use of cryptographs and cipher machines, a few of which were merely mentioned.

c. The category of substitution methods under the heading of code systems was then discussed and examples of the various types of code words and codebook arrangements given. The discussion included a comparison of the advantages and disadvantages of cipher and code methods from the point of view of simplicity, rapidity, practicability, secrecy, accuracy, and economy. Considerable attention was devoted to the secrecy requirements of a cryptographic system for military use.

d. There then followed a brief discussion of the errors which are almost inevitable in cryptographic communication, and of methods for their suppression and elimination. Finally, a summary of the fundamental rules for safeguarding cryptograms was presented.

e. With the foregoing as a background, a review of which is recommended, the student is in a position now to take up the study of more advanced cryptographic methods. Special emphasis is to be laid only upon such systems as are practicable for military use. It is necessary to add, however, that cryptography is by no means a static art or science and that 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 the World War, and indeed for the first two 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, says:

[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.

The necessity for exact expression of ideas practically excludes the use of codes 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 this revision (1943) the author finds it necessary to say that the forecast he made in 1935 in regard to the rebirth of cipher methods has 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 devices and mechanisms.

f. It may be added, too, that modern electrical communication methods and instrumentalities are finding an increasing need for applications of cryptographic theory and practice to their efficacious 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 plain-text characters, the latter are instantaneously and automatically enciphered in transmission and the received signals are instantaneously and automatically deciphered upon reception at the distant end. Thus the printing mechanism at the receiving station records the original 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.

g. 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 the 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 may, a few years from now, 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 the student to fall outside the realm of what is today considered practicable, it should be remembered that the purpose in describing them is to present for his consideration 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.

2. Sequence of study.—Just as in the preceding text, transposition systems will first be discussed, then substitution systems. Considerable attention will be devoted to combined substitution and transposition methods. Following this will come a description of a limited number of cryptographs, together with a discussion of their present-day limitations. Finally, a small amount of space will be devoted to code systems, with special emphasis upon enciphered code systems.

SECTION II

MONOPHASE TRANSPOSITION SYSTEMS

	Paragraph
Transposition systems employing geometric designs	3
Trapezoidal designs	4
Triangular designs	5
Diagonal methods	6
Interrupted keyword transposition	7
Permutation method	8
Transposition method using special figures	9

3. Transposition systems employing geometric designs.—In the preceding text 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.

4. Trapezoidal designs.—*a.* A trapezoid or, more accurately, a truncated triangle, of prearranged 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 1. 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 1, 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:

```
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 con-

structed. 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

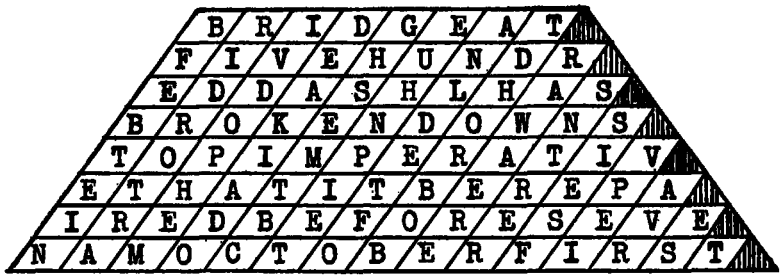


FIGURE 1

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

5. 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 2, where the length agreed upon is nine, i. e., nine cells per side.

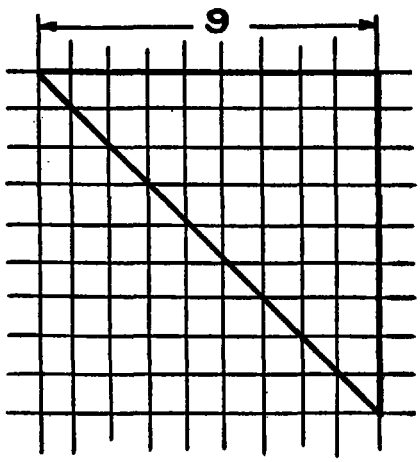


FIGURE 2.

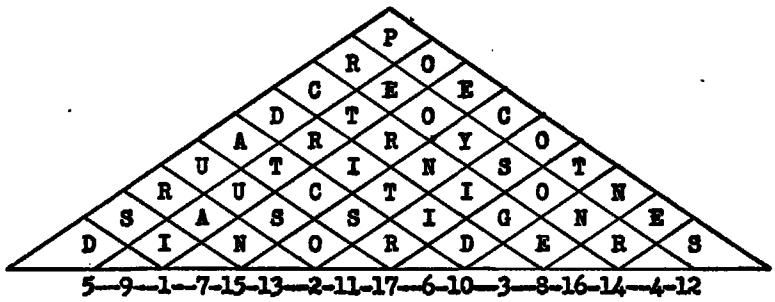
The letters of the plain text are inscribed in accordance with any prearranged route, the one illustrated in Figure 3 being a simple method wherein the letters are inscribed in horizontal lines in the normal manner. When so inscribed, the letters in the diagram will form $2n-1$ columns where n is the number of cells forming one of the sides of the square from which the triangle has been constructed. The total number of letters that can be inscribed within 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:

$n=9$; $2n-1=17$

	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 3.



Cryptogram:

RICRC OCSGE DOONI UAOOE
SEYID RTISS DTSNR AUNTN
PERTR

FIGURE 3.

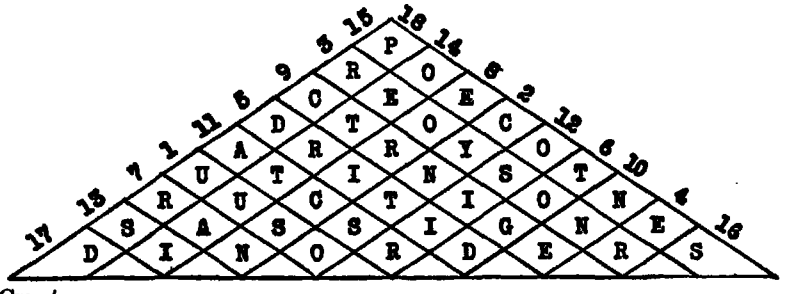
b. By a slight change in procedure it is possible to encipher a message and produce a text which, for the sake of accuracy in special cases, is double the original length, but which is self-checking. Suppose that instead of applying a single numerical key to the base of the triangle, a double-length key is applied to the legs, as shown in Figure 4. 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 5.

6. Diagonal methods.—*a.* A method involving diagonal transposition which is reported to have been employed by the French

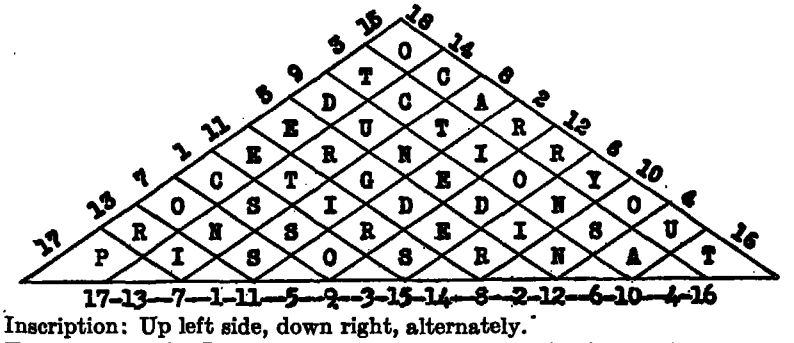


Cryptogram:

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

FIGURE 4.

Army in the World War 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 6. The text is inscribed in this rectangle in



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 5.

normal fashion, nulls being employed, if necessary, to complete the last line of the rectangle.

b. The correspondents agree beforehand upon several diagonals which run from left to right, and from right to left and which inter-

sect, thus cutting up the design quite thoroughly. In Figure 6 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, or, again, if specially agreed upon, repeating them every time they are encountered. If the latter is done, the inclusion of such letters not only serves as a check upon accuracy but also materially increases the difficulties of solution, since in this case these letters act like nulls. The cryptographing process will become clear upon the study of the example in Figure 6.

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 6.

7. 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 7.

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 7.

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 8.

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 8.

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 the following diagram, which uses the same message and key as under *a* above:

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)*	.	.	.	.	.

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

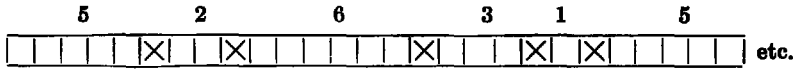
FIGURE 9.

d. This method may be combined with that shown under *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.

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.

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

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:



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 N 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.

8. Permutation method.—*a*. An old method, known in literature as the *aerial telegraphy method*,[1] forms the basis of this system.

[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.

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 10a:

Permutation

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 10a.

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 LOCATIONS 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 10b.

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:

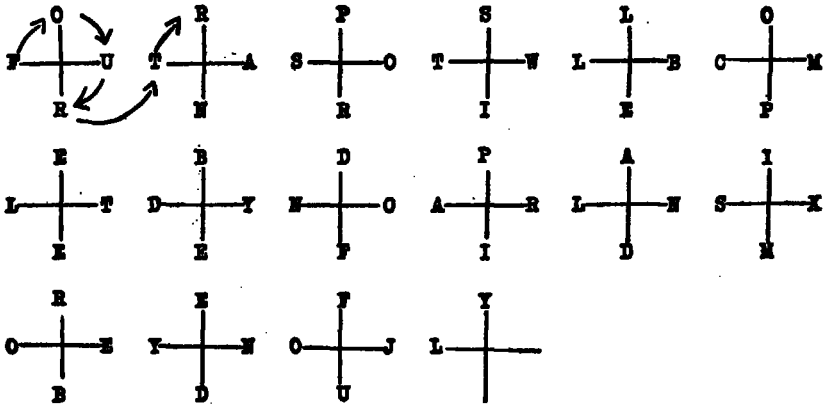
EASEO MCTID MARCO TRMMO IECDO ITBEN
NOSRP SESNO MOANU TNTMN OFOPD FMEAT
TESWY OSLST NROBB LHOIW TECMN AEFAR
LNIRC BROME SCFLU HGOOP TDODO OBAEW

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.

9. 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:



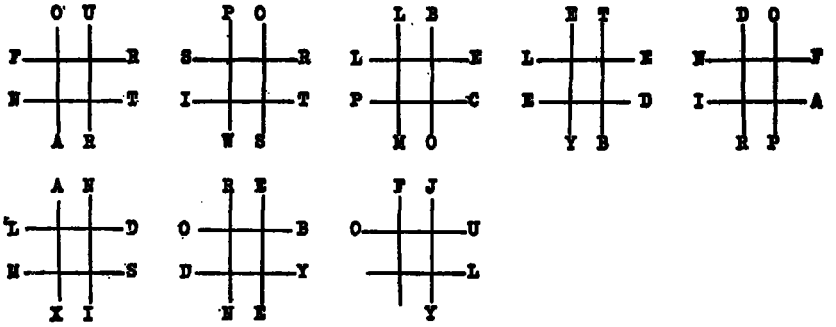
Cryptogram:

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

FIGURE 11.

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.

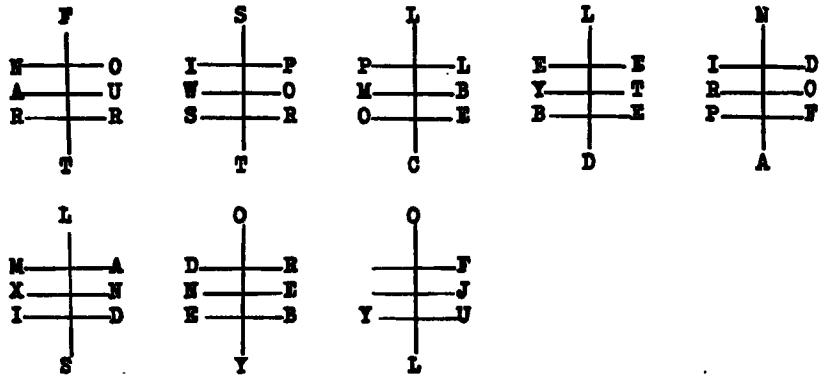


Cryptogram:

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

FIGURE 12.

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

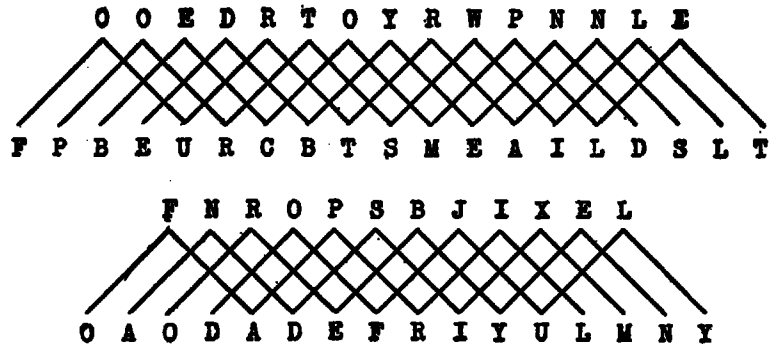


Cryptogram:

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

FIGURE 13.

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



Cryptogram:

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

FIGURE 14.

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 III

POLYPHASE TRANSPOSITION SYSTEMS

	Paragraph
Polyphase transposition methods in general	10
True and false polyphase transpositions	11
True double transposition	12

10. Polyphase transposition methods in general.—*a.* In paragraph 32 of Special Text No. 165, 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.

11. 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 has 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 most thorough

scrambling of the letters composing the original text. Examples will serve to clarify the difference between false and true polyphase transposition.

b. Note the following simple columnar transposition cipher prepared according to the method described in paragraph 26 of Special Text No. 165:

Message: DELIVER ALL AMMUNITION TO 4TH DIVISION DUMP

Keyword: SCHEDULE=$\begin{matrix}S&C&H&E&D&U&L&E\\7&1&5&3&2&8&6&4\end{matrix}$

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
U	R	T	H	D	I	V	I
S	I	O	N	D	U	M	P

D–1

Cryptogram (T–1):

ELIRI VMTDD IMNHN AIOIP LAOTO RNFVM
DLTUS EUOIU

FIGURE 15.

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 16.

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 17.

Each letter in 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 18.

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 under *b* above: 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 under *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.

12. 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 IV

TRUE DOUBLE TRANSPOSITION

	Paragraph
True double transposition of the columnar type	13
General remarks on true polyphase transposition	14

13. 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

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 the T–1 transposition* are then

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 19a.

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 19a 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 19b.

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

c. In paragraph 28 of Special Text No. 165 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 to which reference was made:

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.

14. 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 13*b* and *c* will convince the student 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 cryptoanalyzed 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 transposition 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 13*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 is it 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. Finally, one or more nulls may be inscribed at the end of either the

D–1 or the D–2 rectangle (but not both) in order that the total number of letters involved in the two transpositions be different, a factor which still further increases the degree of cryptographic security.

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 V

GRILLES AND OTHER TYPES OF MATRICES

	Paragraph
Types of cryptographic grilles	15
Simple grilles	16
Revolving grilles	17
Grilles of other geometric forms	18
Polyphase transposition by grilles	19
Increasing the security of revolving grilles	20
Construction of revolving grilles	21
Nonperforated grilles	22
Rectangular or "post card" grilles	23
Indefinite or continuous grilles	24

15. Types of cryptographic grilles.—Broadly speaking, cryptographic grilles [1] 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) nonperforated grilles, and (4) "post card" grilles.

16. 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 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 20. 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

[1] 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.

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

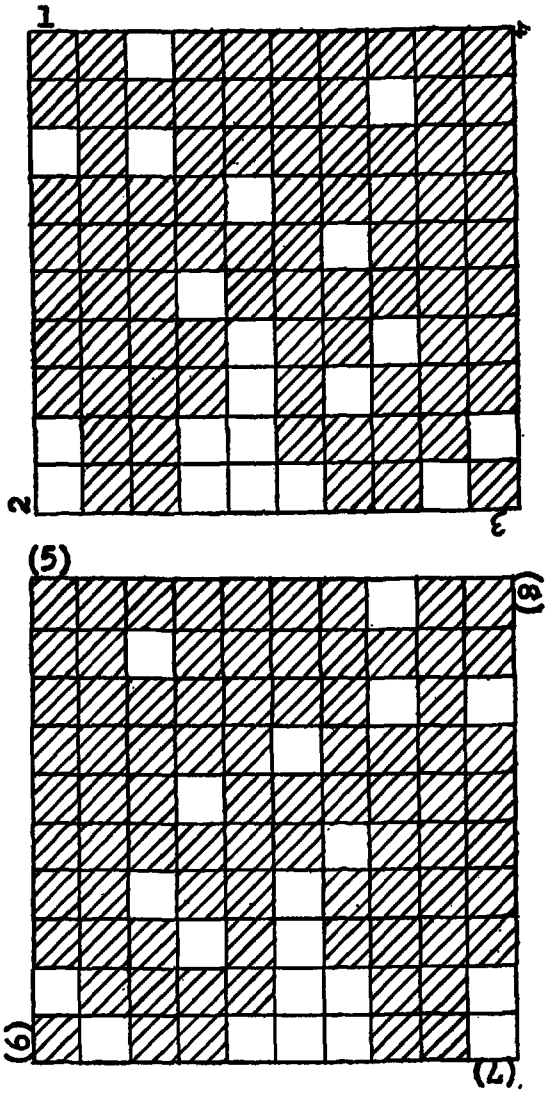


FIGURE 20.

figure 1, 2, 3, or 4 at the top left; or reverse surface up, with 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 21, 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.

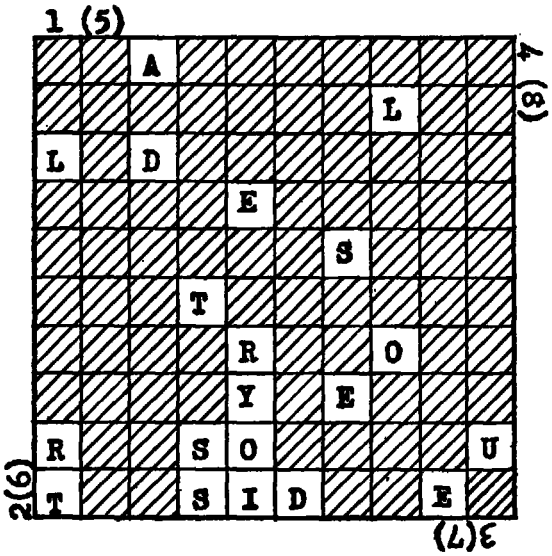


FIGURE 21.

(2) The transcription process now follows. The cipher text is written down, the letters being taken by following any prearranged 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 20 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 21. 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 22, 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	4 (8)
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	

2 (6) 3 (7)

FIGURE 22.

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 23, 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

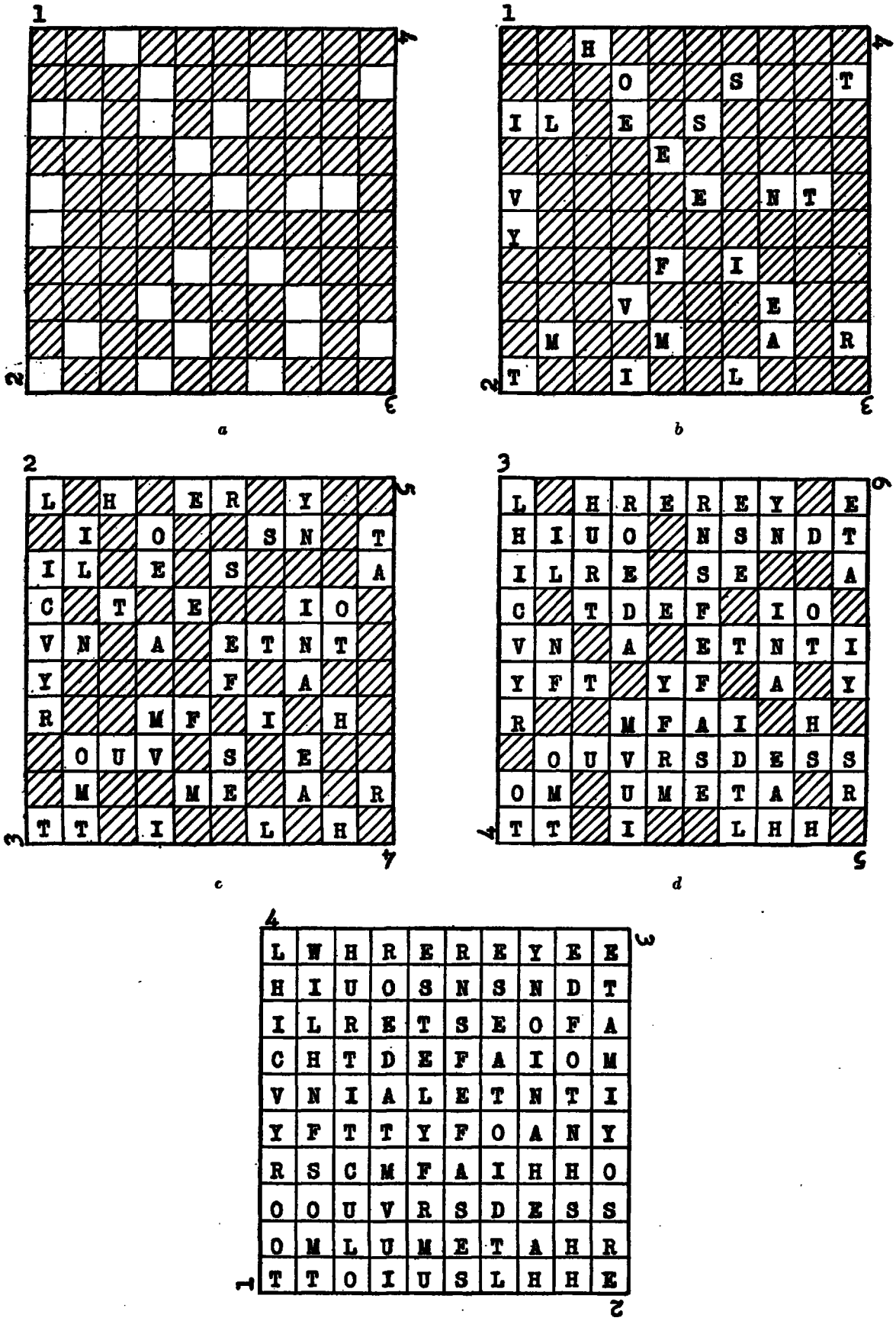
FIGURE 23.

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.[1]

17. Revolving grilles.—*a.* In this type of grille (see fig. 24a) 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 will be discussed in par. 21.) 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 (i. e., 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

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



Cryptogram:

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

FIGURE 24.

of letters 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 Figure 24b. 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 Figure 24c. In Figure 24d and e, 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 (i. e., 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.

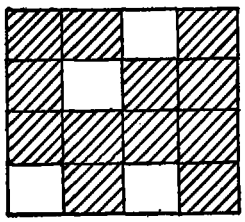
18. Grilles of other geometric forms.—Grilles are not limited to square-shaped figures. They may be equilateral triangles, pentagons, hexagons, and so on. Any figure which can be pivoted upon a central point and which when revolved upon this pivot can be placed in a succession of homologous positions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

19. 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.

20. 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.



a

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					

b

FIGURE 25.

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 Figure 25b. 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 Figure 25a, 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 Figure 25b, together with the number indicating the positions occupied by the letters of the text.

21. 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 Figure 26a. 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 Figure 26b 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.

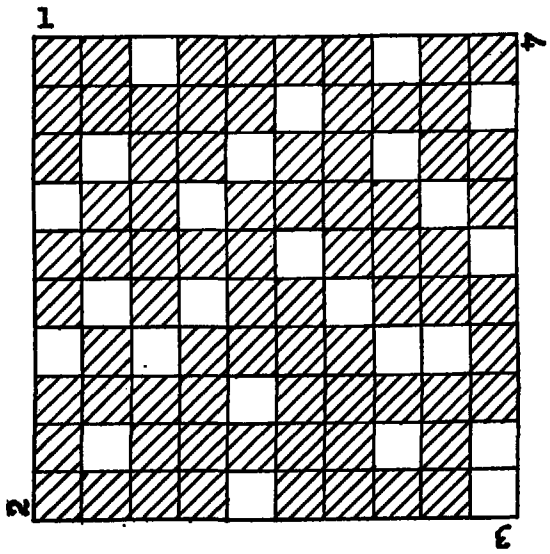
f. A system for designating the positions of the perforated cells of a grille may be established between correspondents, so that the necessity for physical transmission of grilles for intercommunication is eliminated. An example of a possible system is that which is based upon the coordinate method of 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 Figure 26b would have the following formula:

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

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 Figure 26b. Then the initial position of the grille can be indicated by the number which appears at the

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 26.

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 counterclockwise, 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, etc., correspond in this obverse-reverse relationship, as shown in Figure 20.

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

22. 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 27.

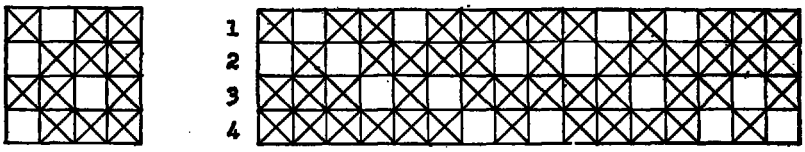
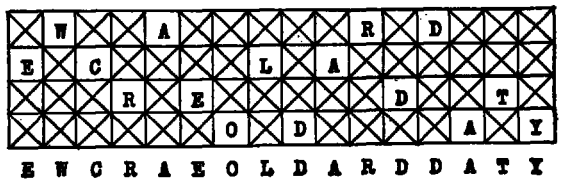


FIGURE 27a. FIGURE 27b.

b. Note should be made of the fact that in Figure 27b 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 27c.

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 27c 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

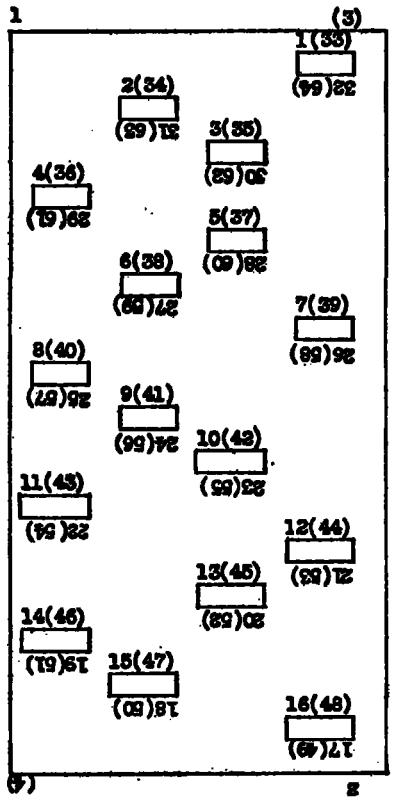


FIGURE 28.

messages may be enciphered by the superposition of several diagrams of the same dimensions as Figure 27c.

23. Rectangular or "post card" grilles.—*a.* The grille shown in Figure 28 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 28 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.

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 21, 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 Figure 29a are assigned numbers; homologous cells in each band receive the same number. In Figure 29a there are three bands, 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 Figure 29c is shown a grille as finally prepared, the nonshaded cells representing apertures.

h. The grille, Figure 29c, 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

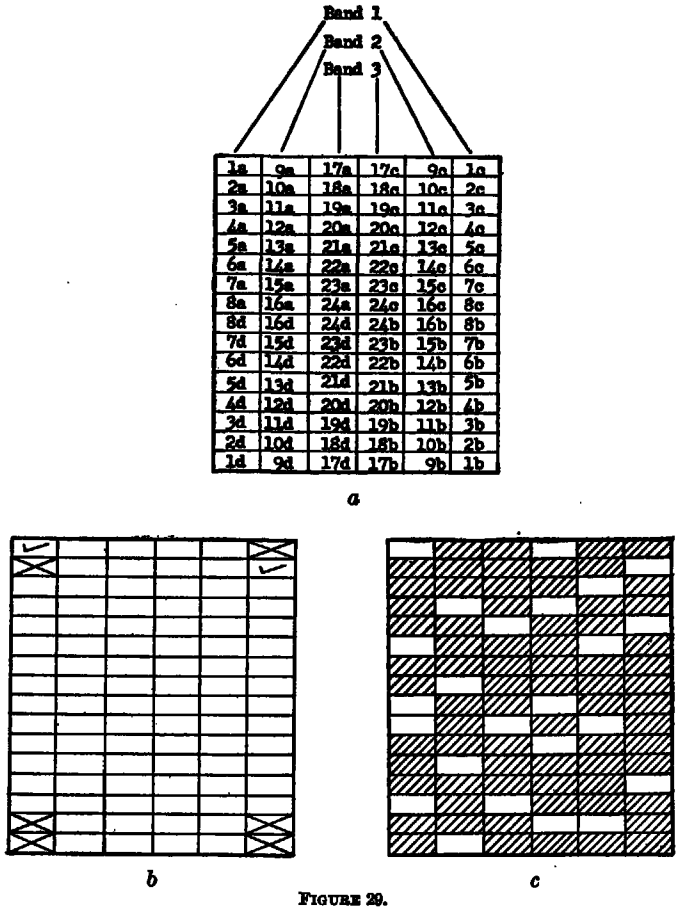


FIGURE 29.

the one shown in Figure 29c 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 number of columns, $16 \times 6 = 96$. 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.

24. 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 29*a*. 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.)

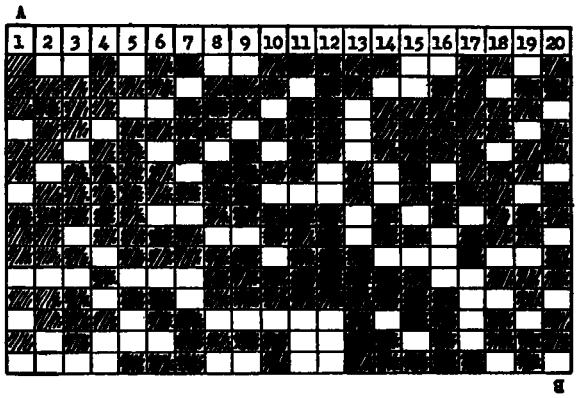


FIGURE 29*a*.

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 29*a* 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. In Figure 29*b* is shown how a message is enciphered.

Message:

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

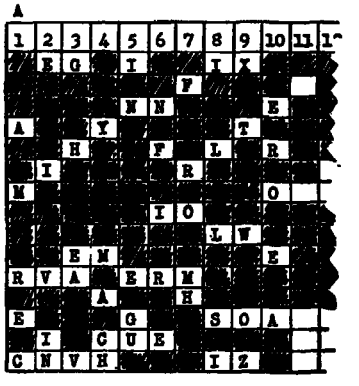


FIGURE 29*b*.

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 VI

MISCELLANEOUS TRANSPOSITION SYSTEMS

	Paragraph
Complex route transposition	25
Transposition of groups of letters, syllables, and words	26
Disguised transposition methods	27
Cipher machines for effecting transposition	28

25. Complex route transposition.—*a.* In Figure 30 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.

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 30.

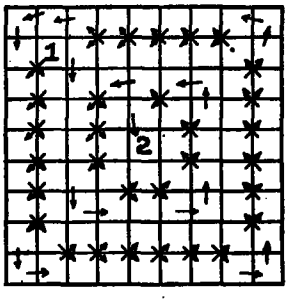


FIGURE 31.

b. A variation of the foregoing is that illustrated in Figure 31, 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 [1] on a chessboard of the usual 64 cells.

26. 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

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

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. X).

27. 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 16.

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.

28. 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 under paragraph 71

B. SUBSTITUTION SYSTEMS

SECTION VII

POLYGRAPHIC SYSTEMS

	Paragraph
Preliminary remarks	29
Monographic and polygraphic substitution	30
Polygraphic substitution by means of tables	31

29. Preliminary remarks.—*a.* It is assumed that the student has absorbed the information contained in Sections VII to XIII, inclusive, Special Text No. 165, Elementary Military Cryptography. The sections deal 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 present study of 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. Before entering upon the study referred to, 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 under Section X, Special Text No. 165, 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 Section X, Special Text No. 165, will be discussed. Attention now will be directed more particularly to a different type of substitution designated as *monographic* and *polygraphic* substitution.

30. Monographic and polygraphic substitution.—*a.* All the methods of substitution heretofore described are monographic 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 poly-

graphic 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 combina-

tions 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 digraph." 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.

31. 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 1. 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.

TABLE 1

(Showing only a partially filled table)

Final Letter (θ^2_p)

Initial letter (θ^1_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	

b. The foregoing table 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., cryptograms 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 52*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 $\theta^1{}_p$ in a first case of $\overline{\theta^1\theta^2}_p=\overline{\theta^1\theta^2}_c$ is identical with $\theta^1{}_p$ 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 1 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 the following Table 2, 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.

TABLE 2

l_p \ m_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	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	CH	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

g. A cursory examination of Table 2 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 following rearrangement of Table 2.

TABLE 3

θ^1_p \ 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

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 4.

TABLE 4

θ^1_p θ^1_c	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	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

i. The results given by Table 3 or Table 4 may be duplicated by using sliding alphabets, as shown in Figures 32 and 33. In the former, which corresponds to Table 3, 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 32.

j. To correspond with Table 4 the alphabet strips are arranged as shown in Figure 33. 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 } ---------- Movable alphabet
IV—IJKLMNOPQRSTUVWXYZABCDEFGH }

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

I—ABCDEFGHIJKLMNOPQRSTUVWXYZ ---------- Fixed alphabet
II—WESTINGHOUARBKCDFJLMPQVXYZ ---------- Fixed alphabet
III—ALCTIOMPYBDFHJKQSUVWXZGENR } ---------- Movable alphabet
IV—EFGHIJKLMNOPQRSTUVWXYZABCD }

FIGURE 33.

k. Neither Table 3 nor Table 4 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 5, which is based upon the same primary alphabets as Table 3 and Table 4, 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 5 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 be also accomplished by means of such tables, as illustrated in the accompanying Table 6, which is the same as Table 5 with the addition of one more alphabet at the top of the table.

TABLE 5

σ^2_p

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

TABLE 6

	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

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 cryptographic 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.

SECTION VIII

CHECKERBOARD DIGRAPHIC SUBSTITUTION

	Paragraph
Disadvantages of large tables	32
Four-alphabet checkerboards	33
Two-alphabet checkerboards	34
One-alphabet checkerboards; Playfair Cipher	35
Rectangular designs	36
Combined alphabetical and numerical checkerboard	37

32. Disadvantages of large tables.—Digraphic substitution by means of tables such as those illustrated in Tables 1, 2, and 5 is impractical for military use on account 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 XII, Special Text No. 165, Elementary Military Cryptography, that simple sliding alphabet strips can replace large quadricular tables, so it will be found that small designs similar to a checkerboard can replace the large quadricular tables in digraphic substitution. Although the usual chess or checkerboard is based on a square 8 by 8, with 64 cells, the term *checkerboard* will here be used to designate any square design with n^2 cells.

33. Four-alphabet checkerboards.—*a.* The simple or single-alphabet checkerboard consists of a square 5 by 5, containing 25 cells in which the letters of a 25-element alphabet (I and J being interchangeable) are inserted in any prearranged order. When four such checkerboard alphabets are arranged in a large square as shown in Figure 34, the latter may be employed for digraphic substitution to yield the same cipher results as does the much larger Table 1 (par. 31). 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	
Sec. 1 (θ^1_p)	H	V	Z	P	I	K	Y	Z	S	N	Sec. 3 (θ^1_c)
	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	
Sec. 4 (θ^2_c)	M	Y	Z	U	A	O	Y	Z	T	C	Sec. 2 (θ^2_p)
	L	X	W	V	B	N	X	W	U	D	
	K	G	F	D	C	M	L	K	H	G	

FIGURE 34.

b. It is possible to construct a digraphic substitution checkerboard 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 35a. The alphabet in section 3 is now to be constructed. Any horizontal row

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

FIGURE 35a.

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 3, in any transposed order, which is immediately written at the top of section 3, as shown in Figure 35b.

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

FIGURE 35b.

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 35c. Then row 2 of section 1 is transferred to another row

	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						
Sec. 1 (θ^1_p) 3	S	I	C	T	K						Sec. 3 (θ^1_c)
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
Sec. 4 (θ^2_c)						S	A	E	W	L	3 Sec. 2 (θ^2_p)
						G	Z	Q	N	R	4
						T	H	I	F	U	5
						1	2	3	4	5	

FIGURE 35c.

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 35d, where section 3 is completely constructed. The

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

FIGURE 35d.

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, viz, 3–5–1–4–2.

The completed square is then as shown in Figure 35e, 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 35e.

d. The total number of reciprocal permutations of five elements is 26, as follows:

		(1) 12345		
(2) 12354	(7) 14325	(12) 21354	(17) 34125	(22) 45312
(3) 12435	(8) 14523	(13) 21435	(18) 35142	(23) 52341
(4) 12543	(9) 15342	(14) 21543	(19) 42315	(24) 52431
(5) 13245	(10) 15432	(15) 32145	(20) 43215	(25) 53241
(6) 13254	(11) 21345	(16) 32154	(21) 42513	(26) 54321

Since the row permutations of sections 2 and 4 are independent, the total number of different four-alphabet squares as regards row permutations is $26^2=676$. Taking into account the column permutations, $5\times4\times3\times2\times1$ in number, it is therefore possible to have 676×120 or 81,120 different, four-alphabet checkerboards 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.

34. Two-alphabet checkerboards.—*a.* It is possible to effect digraphic substitution with a checkerboard consisting of but two sections by a modification in the method of finding equivalents. In the checkerboard shown in Figure 36, θ^1_p of $\overline{\theta^1\theta^2}_p$ is located in the square at the left, θ^2_p, in the square at the right.

When $\overline{\theta^1\theta^2}_p$ 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 2-section checkerboard by reciprocal permutation of the rows of the checkerboard, no attempt

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

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 36.

being made to effect any reciprocal permutation of columns. Figure 37 shows such a checkerboard.

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 37.

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 2-alphabet checkerboards in which one section is directly above the other, reciprocity already exists without special preparations for its production. In Figure 38, $MO_p=UA_c$ and $UA_p=MO_c$;

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
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 38.

$MA_p=MA_c$ and $MA_c=MA_p$. When both $\theta^1{}_p$ and $\theta^2{}_p$ happen to be in the same column, there is really no encipherment, 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 $\overline{\theta^2\theta^1}_c$.

35. One-alphabet checkerboards; Playfair Cipher.—*a.* By reducing the checkerboard to one alphabet, there results the square of the well-known Playfair Cipher, 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. A 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 checkerboard methods. Figure 39

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 39.

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: $\overline{MO}_p=\overline{AL}_c$; $\overline{MI}_p=\overline{UC}_c$; $\overline{LU}_p=\overline{QM}_c$; $\overline{VI}_p=\overline{YC}_c$.

(2) $\theta^1{}_p$ and $\theta^2{}_p$ are in the same row; the letter immediately to the *right* of $\theta^1{}_p$ forms $\theta^1{}_c$, the letter immediately to the right of $\theta^2{}_p$ forms $\theta^2{}_c$. When either $\theta^1{}_p$ or $\theta^2{}_p$ 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) $\theta^1{}_p$ and $\theta^2{}_p$ are in the same column; the letter immediately *below* $\theta^1{}_p$ forms $\theta^1{}_c$, the letter immediately below $\theta^2{}_p$ forms $\theta^2{}_c$. When either $\theta^1{}_p$ or $\theta^2{}_p$ 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).

36. Rectangular designs.—*a.* It is not essential that checkerboards 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 33.

b. In Figures 40 and 41 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
Sec. 1 (θ^1_p)	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
Sec. 4 (θ^2_c)	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. 3 (θ^1_c) — Sec. 2 (θ^2_p)

FIGURE 40.

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

Sec. 2 (θ^2_p)

FIGURE 41.

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

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 42 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

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 42.

the cipher text 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 checkerboard or a rectangle 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 checkerboard or rectangle.*

37. Combined alphabetical and numerical checkerboard.—*a.* In Figure 43 is shown a 4-section checkerboard which presents a rather interesting feature in that it makes possible the substitution of 3-figure combinations 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

	A	B	C	D	E	000	025	050	075	100	
	F	G	H	I	K	125	150	175	200	225	
Sec. 1 (θ^1_p)	L	M	N	O	P	250	275	300	325	350	Sec. 3 (θ^1_c)
	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	
Sec. 4 (θ^2_c)	10	11	12	13	14	X	S	N	H	C	Sec. 2 (θ^2_p)
	15	16	17	18	19	Y	T	O	I	D	
	20	21	22	23	24	Z	U	P	K	E	

FIGURE 43.

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 IX

COMPLEX SUBSTITUTION SYSTEMS

	Paragraph
Preliminary remarks	38
Continuous or nonrepeating-key systems	39
Auto-key systems	40
Progressive-alphabet systems	41
Interrupted or variable-key systems	42
Suppressing periodicity by encipherment of variable-length groupings of the plain text	43
Suppressing periodicity by encipherment by variable-length groupings of the key	44
Mechanical cryptographs in which periodicity is avoided	45

38. Preliminary remarks.—In paragraph 63, Special Text No. 165, 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 of the present text are devoted to 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.

39. 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.

503207°—43——5

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 . . .

40. 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:

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 prearranged 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, though 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 subparagraph *d*, 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	0	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	0	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	0	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	0	A	J
V	Z	Z	U	H	X	Y	0	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	0	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	0	A	J	B	K	E	D	S	L	N	M	G	W	P
N	H	H	X	Y	0	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	0	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q
E	Z	Z	U	H	X	Y	0	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	0	A	J	B	K	E	D	S	L	N	M
D	F	F	V	T	I	Z	U	H	X	Y	0	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	0	A	J	B	K	E	D	S	L	N	M
C	Y	Y	0	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	0	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	0	A	J	B	K	E	D	S	L	N	M	G
0	W	W	P	C	Q	R	F	V	T	I	Z	U	H	X	Y	0	A	J	B	K	E	D	S	L	N	M	G
N	Z	Z	U	H	X	Y	0	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	0	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	0	A	J	B	K	E
R	U	U	H	X	Y	0	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	0
F	V	V	T	I	Z	U	H	X	Y	0	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	0	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	0
L	N	N	M	G	W	P	C	Q	R	F	V	T	I	Z	U	H	X	Y	0	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	0	A	J
N	W	W	P	C	Q	R	F	V	T	I	Z	U	H	X	Y	0	A	J	B	K	E	D	S	L	N	M	G
G	H	H	X	Y	0	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	0	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	0	A	J	B	K	E	D	S	L	N	M	G	W	P	C	Q	R

i. One serious objection to such auto-key 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.

41. 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 set so that A=A (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 counterclockwise) 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.

42. 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 will be explained below.

43. 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 keyword 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 determination of the length of the key.

44. Suppressing periodicity by encipherment by variable-length groupings of the key.—*a.* In paragraph 43*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 / UNPREPARE / 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 EXTINGUISHER: 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 X T I N G U I S H E R
1–12–10—5—7—3–11—6—9—4—2—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 ⅐ yields the sequence 142857142857 . . . This fraction may be represented by the indicator letter H given as the initial letter of the cryptogram.

45. Mechanical cryptographs in which periodicity is avoided.—There are certain cryptographs which operate in such a manner that periodicity is avoided or suppressed. Some of them will be discussed in Section XII. Among them one of the most interesting is that invented by Sir Charles Wheatstone in 1867. As a rule, however, mechanical cryptographs, by their very nature, can hardly avoid being cyclic in operation, thus causing periodicity to be exhibited in the cryptograms.

C. REPETITIVE AND COMBINED SYSTEMS

SECTION X

REPETITIVE SYSTEMS

	Paragraph
Superencipherment	46
Repetitive transposition systems	47
Repetitive monoalphabetic substitution systems	48
Repetitive polyalphabetic substitution systems	49

46. 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.

47. Repetitive transposition systems.—These have been dealt with in Sections III and IV and need no further discussion at this point. It was there shown that properly selected transposition methods, when repetitive in character, can produce cryptograms of very great security.

48. 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.

49. 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 under *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 XI

COMBINED SYSTEMS

	Paragraph
Combined monoalphabetic and polyalphabetic substitution systems	50
Combined substitution-transposition in general	51
Monoalphabetic and polyalphabetic substitution combined with transposition	52
Polyliteral substitution combined with transposition	53
Fractionating systems	54
Comparison of foregoing fractionating system with certain digraphic systems	55
Fractionating systems as forms of combined substitution and transposition	56
Fractionation and recombination within regular or variable groupings of fractional elements	57
Fractionation combined with columnar transposition	58

50. 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.

51. 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.

52. 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

e. A simple variation of the foregoing method which is frequently effective with true digraphic methods of substitution is to write θ^2_p under θ^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:[1]

WLRTRAOC
ILEUNTNE

Then the following pairs would be enciphered: $\overline{WL}_p$, $\overline{RT}_p$, $\overline{RA}_p$, $\overline{OC}_p$, $\overline{IL}_p$, etc. The foregoing message enciphered in this manner by means of the Playfair Square shown in Figure 39, 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

[1] In preparing the text for encipherment, the clerk must bear in mind that if a Playfair Square is to be used no doublets can be enciphered. The message WE WILL LEAVE . . . would be arranged thus:

WXILXEV
EWLXLAE

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.

53. Polyliteral substitution combined with transposition.—In paragraph 29*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.

54. 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:

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 $\begin{cases} \theta^1_c: \\ \theta^2_c: \end{cases}$ 101 11001 01110011 1120
833 97233 83988732 7817

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 11 10 01 01 11 00 11 11 20
83 39 72 33 83 98 87 32 78 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 necessitat-

ing 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* [1] 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.

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 XYLOPHONIC 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

[1] 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.

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 $\theta^1_c\,\theta^2_c$ 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, 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 55*d*.

55. Comparison of foregoing fractionating system with certain digraphic systems.—*a.* The method described under paragraph 54*e* can be identified with some of the digraphic substitution systems discussed in Section VII.

b. Take the message of paragraph 54*e* 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 54*e*:

Message: ONE PLANE REPORTED LOST

ON	EP	LA	NE	RE	PO	RT	ED	LO	ST
41=L	34=H	41=L	13=N	23=R	44=Q	22=T	33=E	44=Q	42=O
23=R	33=E	12=A	33=E	33=E	32=D	32=D	32=D	12=A	52=W

Cryptogram: LRHEL ANERE QDTDE DQAOW

If the cryptogram given in paragraph 54*e* 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 now to be demonstrated in *c* below.

c. Note the 2-alphabet checkerboard shown in Figure 44. If the same message is now enciphered by its means, a cryptogram identical with that obtained in paragraph 55*b* 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

FIGURE 44.

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.

d. In the example in paragraph 54*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. 54*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	LO	ST
41=K	34=G	41=K	13=T	23=L	44=Q	22=I	33=F	44=Q	42=N
23=L	33=F	12=U	33=F	33=F	32=D	32=D	32=D	12=U	52=W

Cryptogram: KLGFK UTFLF QDIDF DQUNW

e. Now encipher the same plain-text message by means of the 4-alphabet checkerboard shown in Figure 45. The results are as follows:

Message: ONE PLANE REPORTED LOST.

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 45.

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 under *d* above.

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 under *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

56. Fractionating systems as forms of combined substitution and transposition.—In studying the various types of checkerboard substitution discussed in Section VIII, 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 55 shows clearly that there is a kind of transposition involved in checkerboard methods of cryptographing.

503207°—43——6

57. Fractionation and recombination within regular or variable groupings of fractional elements.—*a.* This method is an extension or modification of that illustrated in paragraph 54*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. 54*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:

LHOEB MDDEE QTERR HQTAW

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=$\overline{\text{ZB}}$
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=$\overline{\text{ZA}}$	232=R	332=G
I=111	R=232	?=313	133=D	233=P	333=O

Message: HAS AIRPLANE RETURNED YET?

HASAI	RPLAN	ERETU	RNEDY	ET?
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:[1] XURZ̄AC AYGFT MTBKC YFFAD Z̄BXF
Final cryptogram: XURZA CAYGF TMTBK CYFFA DZBXF

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.

58. 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	0	U	M
N	B	2	P	Y	N	D
T	4	E	5	F	6	G
E	7	J	Ø	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 PRISONERS 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	Ø	Ø	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								

[1] 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 Z̄A and Z̄B 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.

The C_1 text is now inscribed in a rectangle of predetermined dimensions. Transposition rectangle: (Columnar, based on key HAIL COLUMBIA HAPPY LAND.)

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 46.

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 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 German 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.

D. CRYPTOGRAPHS AND CIPHER MACHINES

SECTION XII

CRYPTOGRAPHS

	Paragraph
Preliminary remarks	59
Wheatstone Cipher	60
Jefferson Cipher	61
The obsolete U. S. Army cipher device, type M–94	62

59. Preliminary remarks.—The cipher systems described in the preceding sections 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 mechanical cryptographs have been based will be described.

60. Wheatstone Cipher.—*a.* The device is a little more than four inches in diameter, and consists of a dial with two hands, as shown in Figure 47. 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 47 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

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.

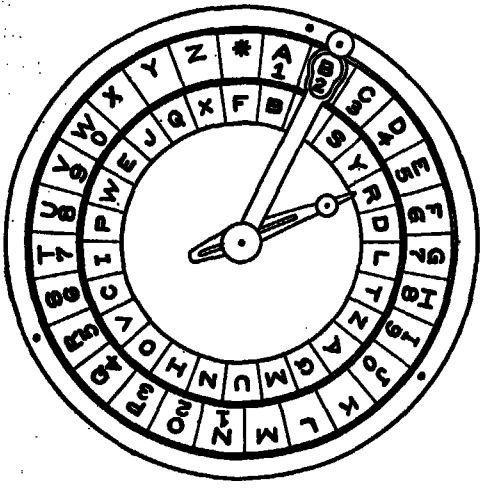


FIGURE 47.

Suppose the message to be enciphered is SEND AMMUNITION FORWARD. The long hand is moved clockwise until it is directly 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 positions, 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 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.

61. Jefferson Cipher.—*a.* Credit for the invention of the cipher system and device now to be described belongs to Thomas Jefferson,[1] the original inventor, 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 Jefferson 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.

[1] 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.

62. The obsolete U. S. Army cipher device, type M–94.—*a.* This cryptograph is based upon the Jefferson principle, using 25 mixed alphabets on small aluminum disks. It was widely employed in our military service and to a more limited extent in other U. S. services until very recently, when it was superseded by better devices.

b. Because the basic principles involved in such a cryptograph are extremely important and have a direct bearing upon modern cryptography, a detailed description of this device and its method of employment will be presented in the next section.

SECTION XIII

THE OBSOLETE U. S. ARMY CIPHER DEVICE, TYPE M–94

	Paragraph
Issue to students	63
General description	64
Necessity for key and providing for changes therein	65
Detailed instructions for setting the device to a predetermined key	66
Cryptographing a message	67
Cryptographing abbreviations, punctuation signs, and numbers	68
Decryptographing a message	69

63. Issue to Students.—When a student who has been regularly enrolled in the Army Extension subcourse to which this text applies reaches this point in his studies, one of these devices will be temporarily issued to him for use in connection with the lesson assignment dealing with it. The following description of the device and instructions for its use will be clear when he has the device in hand. They coincide with the description and instructions employed in training literature applicable when the device was in effect.

64. General description.—*a.* The device is made of aluminum alloy and consists of the following parts:

(1) A central *shaft*, the left end of which terminates with a projecting shoulder, the right end of which is threaded;

(2) A set of 25 *alphabet disks*, on the rim of each of which there is stamped a different, completely disarranged alphabet;

(3) A *guide-rule disk*, consisting of a blank or unlettered-disk from which there projects a guide rule;

(4) A *retaining plate*, consisting of a thin disk upon one surface of which are stamped the name and type number of the device;

(5) A *knurled thumb nut*.

b. Each disk has a hole at the center suitable for mounting it upon the central shaft, upon which the disk can be revolved forward or backward. The left face of each alphabet disk is provided with a circle of 26 equidistant slots; the right face is cupped, and carries at one point on the inside rim of this cup a small projecting lug. The guide-rule disk also carries such a lug. When the disks are assembled upon the shaft, the lug on each disk engages with one of the slots on the adjacent disk on the right and thus the disks can be held in engagement in any desired relative positions by screwing down the knurled thumb nut against the retaining plate, which is inserted between the last alphabet disk and the nut.

c. When the thumb nut and the retaining plate are removed and the alphabet disks are taken off the shaft, it will be noted that each alphabet is stamped on its inside or cup surface with an indentifying symbol consisting of a number that is above the central hole and a letter that is below it. The numbers run from 1 to 25, inclusive, the

letters from B to Z, inclusive. These symbols are employed to designate the sequence in which the alphabet disks are to be assembled upon the shaft in cryptographing or decryptographing messages, as described in paragraph 66. Either symbol may be used for this purpose (as prearranged) but for the present only the numerical identifying symbols will be so used.

65. Necessity for key and providing for changes therein.—*a.* Messages cryptographed by the same sequence of alphabet disks can remain secure against solution by a well-organized and efficient enemy cryptanalytic section for only a relatively short time. It is impossible to state exactly how long, because solution depends upon a number of variable factors; a conservative estimate would place the minimum at six hours, the maximum at two or three days. For this reason it is necessary to change the sequence from time to time, and the method for determining or indicating the new sequence must be agreed upon in advance and thoroughly understood by all who are to use the instrument.

b. The sequence in which the alphabet disks are assembled upon the shaft constitutes the *key* in this cipher system. When a change in key is to take place, exactly what the new key will be and the exact moment that it is to supersede the old key will be determined by the proper commander and will be communicated in signal operation instructions.

66. Detailed instructions for setting the device to a predetermined key.—*a.* The method prescribed herein is based upon a *keyword* or *keyphrase* from which the sequence of numbers constituting the key for assembling the alphabet disks can be obtained by following a simple, standardized procedure. The reason for employing such a procedure is that it makes it possible to derive, at will, a relatively long sequence of numbers (which would be difficult to remember) from a word or phrase (which is easy to remember) and thus eliminates the necessity of carrying the key in written form upon the person. It is this basic keyword or keyphrase which is communicated throughout the command in signal operation instructions. The exact method of deriving the numerical key sequence from the keyword or keyphrase is given step by step in *b* below.

b. Assume that the key phrase so communicated is CHINESE LAUNDRY. The following are the detailed steps to be followed in deriving the numerical key sequence:

(1) A set of rows of cross-section squares, 25 squares in each row, is prepared. (Prepared sheets of ¼-inch squares are suitable.)

(2) In the top row the series of numbers 1, 2, 3, . . . 25 are inserted. Thus:

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

(3) Beginning under the number 1, the successive letters of the key phrase are written in the second row of squares, under the successive numbers. Thus:

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
C	H	I	N	E	S	E	L	A	U	N	D	R	Y											

(4) The keyphrase is extended by repetition until there is a letter under the number 25, making a *key sequence* of 25 letters.[1] Thus:

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
C	H	I	N	E	S	E	L	A	U	N	D	R	Y	C	H	I	N	E	S	E	L	A	U	N

(5) The letters of the key sequence are now to be numbered serially from left to right in accordance with the relative position that each letter occupies in the ordinary alphabet. Since the letter A comes first in the ordinary alphabet, and since this letter occurs twice in the illustrative key sequence, the number 1 is written under the first appearance of A in this sequence, and the number 2 is written under its second appearance. Thus:

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
C	H	I	N	E	S	E	L	A	U	N	D	R	Y	C	H	I	N	E	S	E	L	A	U	N
								1														2		

(6) The next letter in the ordinary alphabet is B. The key sequence is carefully examined to see if it contains the letter B. Since this letter does not appear in the illustrative key sequence, the latter is examined to see if it contains the letter C. This letter occurs twice in the

[1] If the key consists of a word or phrase containing more than 25 letters, those after the 25th letter are merely omitted.

illustrative key sequence and the first C, therefore, is assigned the number 3, the second C the number 4. Thus:

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
C	H	I	N	E	S	E	L	A	U	N	D	R	Y	C	H	I	N	E	S	E	L	A	U	N
3								1						4								2		

(7) The next letter in the ordinary alphabet is D, which, being present in the key sequence, is assigned the next number, and so on. Thus, the process is continued until each letter has been assigned a number. The work must be done carefully so as not to overlook a single letter. If an error is made in the early stages of the work, it necessitates starting afresh. The operator should be especially careful with the letters which immediately follow one another in the ordinary alphabet but are present in the key sequence in reversed order, such as ED, FE, ON, and so on. It is easy to make a mistake in such cases and to assign these letters numbers in a sequence that is the reverse of what it should be.

(8) When the numbering process has been completed and if the work has been correctly performed, it will be found that every letter of the key sequence has a number under it, and that the greatest number that appears is 25. If this is not the case, it is an immediate signal that an error has been made. It cannot, however, be assumed that so long as every letter has a number under it, with the greatest number 25, this is immediate and conclusive proof of accuracy in the work. The operator should *invariably* check his work; better yet, if two clerks are available each one should derive the numerical key independently and the final results should be checked by comparison.

(9) The keyphrase selected as an example in the foregoing description yields the following numerical key:

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
C	H	I	N	E	S	E	L	A	U	N	D	R	Y	C	H	I	N	E	S	E	L	A	U	N
3	10	12	16	6	21	7	14	1	23	17	5	20	25	4	11	13	18	8	22	9	15	2	24	19

(10) It is this sequence of numbers which indicates the order in which the successive alphabet disks are to be assembled upon the shaft from left to right. Thus, according to the foregoing key sequence, alphabet disk No. 3 comes first, that is immediately to the right of the guide-rule disk; alphabet disk No. 10 comes next, and so on. Alphabet disk No. 19 is the last in this particular key, and after it has been placed on the shaft, the retaining plate and thumb nut are added and the latter screwed down a distance sufficient to keep the assembly together and yet permit of revolving individual disks freely

upon the shaft. The instrument is now ready for use in either cryptographing or decryptographing messages.

67. Cryptographing a message.—Suppose the following message is to be enciphered with the key derived in paragraph 66:

CO 3D INF

HAVE JUST REACHED EASTERN EDGE OF WOODS ALONG 552–592 ROAD. WILL REMAIN IN OBSERVATION.

CO 2D BN

a. The message is written down on the work sheet underneath the key in lines of 25 letters each. Space is left under each line for the insertion of cipher letters. (For procedure in connection with abbreviations and numbers appearing in the text of messages, see par. 68.) Thus:

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

b. By revolving the disks upon the shaft, one by one, the first 25 letters of the message are aligned to form a continuous horizontal row of letters reading from left to right along the outside of the cylinder. The guide-rule will be found very convenient in marking the row upon which the letters are being aligned, thus relieving the eyes of unnecessary strain and reducing the chance of making errors. After all 25

letters have been aligned, the assembly is locked in position so that no disk can become displaced accidentally in further manipulation of the cylinder. *The row of letters is immediately checked to make sure that no displacement has occurred among the first few disks while manipulating the last few.*

c. The outside of the cylinder now presents a series of 26 rows of letters, of which 24 rows are fully visible, the other two being hidden or partially obscured by the guide-rule. One of the 24 visible rows is the plain-text row that has just been set up, and the other 23 rows are cipher-text rows *any one of which may be selected to represent the plain-text row.* One of these cipher-text rows is selected at random and the letters composing this row are written underneath the row of plain-text letters on the work sheet. Thus, supposing the row beginning LYEUJ . . . , has been selected, the first cipher line will read as follows:

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

It is not necessary to make any record on the work sheet as to which cipher-text row (above or below the plain-text row) was selected, nor is it necessary to indicate it in any manner whatever in the cipher message.

d. The thumb nut is loosened, but not removed from the shaft. The next 25 letters of the message are aligned, the thumb nut screwed down against the retaining plate, the letters in the alignment are checked, and again any one of the 23 visible cipher-text rows, except the one used to encipher the first line, is selected at *random* for the cipher text. The letters in the row selected are written down under the second line of plain-text letters on the work sheet. Thus, supposing the row beginning KZBYJ . . . , was selected, the work sheet now appears as follows:

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

e. This process is continued in similar manner with the third and fourth lines of the plain-text message. *It should never be made a practice to "favor", that is, frequently to select a particular cipher-text row above or below the plain-text row.* As irregular a selection as possible should be made, and the selection of the cipher-text row immediately above the plain-text row or immediately below the lower edge of the guide rule should be avoided. Supposing these instructions to have been followed and that there has been selected for the the cipher-text row representing the third plain-text line of the message the row beginning RAMTF . . . , and for that representing the fourth line, the one beginning PJNSY . . . , the message now stands as follows:

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

f. There are left only 11 letters to be enciphered, not enough to make a complete row of 25 letters. This, however, makes no differ-

ence in procedure; these 11 letters are merely aligned and a cipher-text row is selected to represent them. Supposing the row beginning URZGH . . . , is selected, the message now stands as follows:

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

g. The cipher text is now to be copied on the message form in 5-letter groups. It is as follows:

LYEUJ DJNYP QBFYN ECNHP FAGPG
KZBYJ IAHNS RANDJ MEFSY RITSN
RAMTF OMOKE NCSHC SPMXH TEXGM
PJNSY VAWUC HYFHE YTBGP YKGMG
URZGH EJQSM D

h. The last group of the cipher message is, however, not a complete group of 5 letters. It is made so by adding four X's. *These are not to be cryptographed;* they are added merely to complete the last cipher group. The final message becomes as shown below:

LYEUJ DJNYP QBFYN ECNHP FAGPG
KZBYJ IAHNS RANDJ MEFSY RITSN
RAMTF OMOKE NCSHC SPMXH TEXGM
PJNSY VAWUC HYFHE YTBGP YKGMG
URZGH EJQSM DXXXX

The message as it now reads is but *one* of many different forms in which this same message could appear externally, depending on exactly which of the available cipher-text rows is selected for each line of the encipherment.

68. Cryptographing abbreviations, punctuation signs, and numbers.—*a.* Authorized abbreviations appearing in the original plain-text message may be enciphered as abbreviations without periods. Examples: Am Tn=AMTN; E. V. Brown Sch=EVBROWNSCH.

b. Normally, the writer of a message spells out the punctuation signs he wishes transmitted, as, for example, STOP, COMMA, COLON, etc. If a message contains punctuation signs not so spelled out, the message-center chief must indicate whether they are to be omitted or spelled out and transmitted.

c. Cardinal and ordinal numbers when spelled out in letters in the original plain-text message are always enciphered exactly as spelled.

d. Cardinal numbers when expressed in figures in the original plain-text message must always be spelled out, digit by digit, in cryptographing. Examples:

4=FOUR
40=FOURZERO (and *not* FORTY)
400=FOUR ZERO ZERO (and *not* FOUR HUNDRED)
455=FOURFIVEFIVE
450.7-758.8=FOURFIVEZEROPOINTSEVENDASHSEVEN-FIVEEIGHTPOINTEIGHT
2005=TWOZEROZEROFIVE
12:01 a. m.=ONETWOZEROONEAM
5:15 p. m.=FIVEONEFIVEPM

e. Ordinal numbers above the ordinal number 10th, when expressed in figures followed by "d" or "th", are cryptographed merely as digits spelled out, without adding the "d" or "th." The omission of the "d" or the "th" will cause no confusion or ambiguity. Examples: 3d Bn=THIRDBN; 7th Pack Tn=SEVENTHPACKTN; 11th Regt=ONEONEREGT; 403d Am Tn=FOURZEROTHREEAMTN.

69. Decryptographing a message.—*a.* Knowing the keyword or keyphrase, the numerical key is developed as described under paragraph 66, and the set of alphabet disks is assembled accordingly. The message to be decryptographed is written down in lines of 25 letters, on cross-section paper, if available, space being left under each line for the insertion of plain-text letters. Using the cipher

message given under paragraph 67*h*, it appears under the key in the following form:

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

b. The first 25 letters of the cryptogram are set up on the device, the letters being aligned in a row from left to right, just above the guide-rule. Fixing the disks in this position by screwing down the thumb nut, the whole cylinder is turned slowly, forward or backward, and each row of letters is carefully examined. One of these rows *and only one* will read intelligibly all the way across from left to right. That is the row which gives the plain text for the first 25 cipher letters. These letters are inserted in their proper place on the work sheet, giving the following:

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

c. The thumb nut is then loosened, the next 25 cipher letters are set up, the assembly is locked into position, again the whole cylinder is slowly revolved, and the plain-text row of letters found. These are written down in their proper place and the process is continued with the rest of the cipher letters until the message has been completely decryptographed.

d. In the case of a cryptogram the last few letters of which do not form a complete set of 25, if any difficulty is experienced in picking out the plain-text row, the context of the preceding part of the message should give a good clue. In the case of the illustrative message above, it should be realized that the last four letters of the cryptogram are not to to be decryptographed, since they were merely added *after* cryptographing to make the last group of the cryptogram a complete group of five letters. They are omitted from the work sheet.

e. The plain-text message is then copied on a message form. The code clerk may, if authorized to do so by the message-center chief, convert numbers, which had to be spelled out in letters to permit of their cryptographing, into their equivalent Arabic figures. Abbreviations and punctuation signs are, however, copied exactly as they stand in the decryptographed message.

Section XIV

CIPHER MACHINES

	Paragraph
Importance of cipher machines in modern cryptographic communication	70
Transposition-cipher machines	71
Substitution-cipher machines	72
Machine affording only monoalphabetic substitution	73
Machines affording polyalphabetic substitution	74
The advantages and disadvantages of cipher machines	75

70. Importance of cipher machines in modern cryptographic communication.—The remarks made in paragraph 1 *e–f* of this text, regarding the present trends in the art, are believed to be sufficient to give the student 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 examples. More and more attention is today being devoted to this phase of cryptography and it is highly probable that within the near future cipher machines will replace code books to a large extent, even in lower headquarters.

71. Transposition-cipher machines.—These are rarely encountered; the files of United States patents disclose but one example and so far as is known no actual machine has 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.

72. Substitution-cipher machines.—*a.* The substitution principle lends itself very readily to the construction of cipher machines for effecting it. The cryptographs described in the preceding two sections, 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.

73. 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 substitu-

tion 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.

74. 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 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.

c. 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, in the next paragraph a few remarks of a general character, dealing with the advantages and disadvantages of cipher machines in military communications today, are deemed pertinent.

75. The advantages and disadvantages of cipher machines.—*a.* Until very recently, 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 cryptographs and cipher machines in general to note the advantages and disadvantages of each category of methods.

b. (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 cryptographs. Comparative speed tests gave the following data recently:

Number of groups or words per minute

Method[1]	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

[1] 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—A small mechanical cryptographic machine producing a printed record but not provided with a keyboard.
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 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 cryptograph 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 all future cryptograms in the same machine; 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. For all these reasons, and because code books or hand-operated cipher systems are usually much more easily transportable and require less storage and operating space, cipher machines cannot, as a rule, be carried forward of the larger headquarters, such as Division. Hence, code methods may predominate in the lower echelons and troop formations.

(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 large 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.

E. CODE SYSTEMS

SECTION XV

CODE SYSTEMS IN GENERAL

	Paragraph
Preliminary remarks	76
Intermixtures of code text and other kinds of text	77

76. Preliminary remarks.—*a.* Sections XIV to XVII, Special Text No. 165, were 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 figures.

77. 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 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 XVI

ENCIPHERED CODE

	Paragraph
Preliminary remarks on enciphered code	78
The general types of methods of superencipherment	79
Transposition methods	80
Substitution methods	81
Arithmetical methods	82
Single or fixed additives	83
Repeating or recurring-key additives and subtractors	84
Nonrepeating additives and subtractors	85
Concluding remarks on arithmetical methods	86

78. Preliminary remarks on enciphered code.—*a.* The purposes of enciphering code have already been explained in the previous text, together with brief indications of methods. The superimposition of a good cipher system upon the code text of a message is today one of the safest and most practical of all methods of cryptography for governmental use.

b. In the subsequent paragraphs, for brevity and ease in reference, the term *placode*[1] 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*[1] will be employed to designate the final product of the superencipherment; it is likewise derived by telescoping the words *enciphered* and *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.

79. The 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.

80. 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

[1] Pronounced "play-code" and "n-sigh'-code."

applied strictly within the code groups, by rearranging 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, i. e., 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 76*b*. However, the restrictions in this respect were lifted on the date indicated and it is therefore probable 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.

81. Substitution methods.—*a*. 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 necessary here to indicate. Even when the actual code book is not known, but it is known that it is one of a set of commercial 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 substitution, 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 substitutive 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 message 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 being given their letter-code equivalents. Some of these methods are explained below.

82. Arithmetical methods.—*a.* These are today 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.

b. In discussing these arithmetical methods many references to the terms *additives* and *subtractives,* or *subtractors* will be encountered. They will be defined in due course.

83. 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 limita-

tions in construction. For example, should it be employed in connection with a code having only 3,000 groups numbered consecutively from 0001 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 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.* Herewith follows 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.

g. (1) 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

(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) A word or two in explanation of this phenomenon may not be amiss. 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 symbol 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 85 more will be said about this method.

84. 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 subparagraph *g* (3) above. 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 the remarks under paragraph 49*c* of this text.

85. 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 Fig. 48.

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) of paragraph 83*e*, or in the subtractor manner illustrated in Example C (a), of paragraph 83*g*. In this example 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, 8850 is the indicator for the group 6126. It is usual to take the successive groups in the normal order of reading, i. e., 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 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 of paragraph 83*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

503207°—43——8

		Ø	1	2	3	4	5	6	7	8	9
	Ø	5Ø87	5344	Ø1Ø8	396Ø	3477	2Ø75	Ø157	56Ø7	3681	1948
	1	4136	5532	3884	5286	Ø727	4Ø18	4327	84Ø1	6151	9323
	2	787Ø	5Ø86	7Ø21	7165	828Ø	63Ø3	5325	5241	Ø376	4739
	3	5465	6382	75Ø9	8938	8461	Ø624	4878	6883	1539	584Ø
	4	1685	3147	7116	7654	3766	511Ø	2646	Ø353	6Ø38	9316
88	5	6126	9524	5178	3818	1458	2915	8753	Ø134	2848	3217
	6	6667	24Ø9	6932	729Ø	1357	7176	7658	8334	4335	5991
	7	5297	2Ø99	2626	397Ø	4642	9251	5Ø54	587Ø	98Ø1	4863
	8	Ø367	3693	8875	Ø822	7694	5742	6178	8259	9987	4765
	9	65Ø2	8685	4829	3466	272Ø	Ø934	6124	9647	4Ø47	8127
	Ø	6673	6979	4382	4347	3812	928Ø	3464	3789	9498	9581
	1	8625	8347	9189	3619	473Ø	533Ø	7359	2183	7743	Ø419
	2	3829	8413	Ø541	Ø92Ø	3663	5733	26Ø2	5464	274Ø	9811
	3	5923	7427	1118	7849	2558	3324	6369	6663	3Ø51	Ø947
	4	2153	4254	Ø167	4467	3Ø53	1532	7762	4125	Ø877	3334
89	5	8727	8613	3244	2312	Ø268	8549	8843	5282	7259	1552
	6	6348	181Ø	4756	8611	259Ø	2556	9345	9112	4753	6169
	7	5378	6976	8833	Ø935	2621	9213	7674	3427	Ø83Ø	3896
	8	Ø244	1751	5242	88Ø1	1546	768Ø	4662	7727	1866	267Ø
	9	6989	1418	9552	93Ø9	8664	Ø187	3873	7253	326Ø	93Ø9

FIGURE 48.

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.

86. Concluding remarks on arithmetical methods.—*a.* The student has no doubt 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"
	2	1	2	3	4	5	6	7	8	9	0	
	3	9	0	1	2	3	4	5	6	7	8	
	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 4-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 our 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 today very frequently employed and 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 our 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 encicode 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.

○