CONFIDENTIAL

~~RESTRICTED~~

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON

M I L I T A R Y   C R Y P T A N A L Y S I S

PART IV

TRANSPOSITION AND FRACTIONATING SYSTEMS

by

WILLIAM F. FRIEDMAN

Principal Cryptanalyst,

SIGNAL INTELLIGENCE SERVICE

Prepared under the direction of the Chief Signal Officer.

(PRELIMINARY EDITION)

NOTE: Students are earnestly requested to make note of all errors and obscure points in this text and to advise the instructor, so that corrections may be made in the printed edition.

* * * * * *

~~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.

1939

CONFIDENTIAL

Declassified and approved for release by NSA on 05-23-2014 pursuant to E.O. 13526

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

Paul S. Willard
Colonel, AGC
Adjutant General

~~CONFIDENTIAL~~

MILITARY CRYPTANALYSIS, PART IV

TRANSPOSITION AND FRACTIONATING SYSTEMS

CONTENTS

SECTION I.

GENERAL

1. Introductory remarks concerning transposition ciphers. - a. As stated in a previous text, transposition ciphers are roughly analogous to "jig-saw puzzles" in that all the pieces of which the original is composed are present but are merely disarranged. The pieces into which the picture forming the basis of a jig-saw puzzle may be divided are usually quite irregular in size and shape, the greater the amount of irregularity, as a rule, the greater the difficulty in reassembling the pieces in proper order. In this respect, too, transposition ciphers are analogous to jig-saw puzzles, for the greater the amount of distortion to which the plain text is subjected in the transposition process, the more difficult becomes the solution.

b. In jig-saw puzzles there is usually no regularity about the size of the individual pieces into which the original picture has been cut, and this feature, of course, materially contributes to the difficulty in reconstructing the picture. There are, to be sure, limits (dictated by considerations of practicability) which serve to prevent the pieces being made too small, for then they would become unmanageable; on the other hand, there are also limits which must be observed in respect to the upper magnitude of the pieces, for if they are made too large the puzzle becomes too easy to solve. These features of jig-saw puzzles also have their analogies in transposition methods. In the latter, if the textual units to be subjected to transposition are made quite large, say entire sentences, the difficulties a cryptanalyst will have in reconstructing the text are practically nil; on the other hand, if these textual units are made quite small, even smaller than single letters[1], then the reconstruction of the transposition text by a cryptanalyst often becomes a very difficult matter. In between these two extremes there may be various degrees of fragmentation, limited only by considerations of practicability.

c. It is fortunate, however, that the cryptanalyst does not, as a rule, have to contend with problems in which the size of the textual units varies within the same message, as is the case in jig-saw puzzles. It is perhaps possible to devise a transposition system in which the text is divided up in such a manner that entire sentences, whole words, syllables, individual letters, and fractions of letters form the units for transposition; but it is not difficult to imagine how impractical such a scheme would be for regular communication, and it may be taken for granted that such irregularity in size of textual units will not be encountered in such communication.

d. The days when the simple methods of word or letter transposition were sufficient for military purposes have long since

---

[1]Reference is here made to so-called fractionating systems. See Special Text No. 166, Advanced Military Cryptography, Sect. XI.

passed by, and it is hardly to be expected that cryptograms of such ineffectual nature will be encountered in the military communications of even the smaller armies of today. However, in time of emergency, when a counter-espionage censorship is exercised over internal communications, it is possible that isolated instances of simple transposition may be encountered. The solution of such cases should present no difficulties, unless numerous code names and nulls are also used in the cryptograms. Mere experimentation with the cryptograms, trying various sizes of rectangles, will usually disclose the secret text. If code names are used and the context gives no clue to the identity of the persons or places applicable, it may be necessary to wait until additional messages become available, or, lacking such a possibility, there is usually sufficient justification, under the exigencies of war, to compel the correspondents to reveal the meaning of these code names.

e. Although transposition ciphers, as a general rule, are much less complex in their mechanics than are substitution ciphers, the cryptanalyst usually experiences a feeling of distaste and dismay when confronted with unknown ciphers of this category. There are several reasons for his dislike for them. In the first place, although transposition ciphers are admittedly less intricate than substitution ciphers, as a general rule there are not nearly so many cryptanalytic tools and "tricks" to be used in the solution of the former as there are in the latter, and therefore the mental stimulus and satisfaction which the cryptanalyst usually derives and regards as part of the reward for his hard labor in solving a cipher is often missing in the case of transposition ciphers. In the second place, despite their lack of complexity, the solution of transposition ciphers often involves a tremendous amount of time and labor most of which commonly turns out to be fruitless experimentation. Thirdly, in modern military communication transposition methods are usually not employed alone but in conjunction with substitution methods -- and then the problems may become difficult indeed, for usually before the substitution can be solved it is necessary to uncover the substitutive text by first removing the transposition. Finally, in working with transposition ciphers a much higher degree of accuracy in mere mechanical operations is required than in working with substitution ciphers, because the accidental omission or addition of a single letter will usually necessitate rewriting entire messages and starting afresh. Thus, this sort of work calls for a constant state of concentrated attention, with its resulting state of mental tension, which takes its toll in mental wear and tear.

2. Basic mechanism of transposition ciphers. - a. Basically all transposition ciphers involve at least two processes: (1) writing the plain-text units (usually single letters) within a specific regular or irregular two-dimensional design, in such a prearranged manner that the said units are distributed regularly or irregularly throughout the various cells or subsections of that design; (2) removing the plain-text units from the design in such a prearranged manner as to change the original sequence in which they followed one another in the plain text, thus producing cipher text. Since the first process consists of <u>inscribing the text</u> within the design, it is

technically referred to as the process of inscription; and since the second process consists of transcribing the text from the design, it is technically referred to as that of transcription. Either or both processes may be repetitive, by prearrangement of course, in which case the intermediate steps may be referred to as processes of rescription, or rescriptive processes.

b. It is hardly necessary at this point to give the student any indications as to how to differentiate a transposition from a substitution cipher. If a review is necessary, however, he is referred to Section IV of Military Cryptanalysis, Part I.

3. Monophase and polyphase transposition. - a. As may be inferred from the foregoing definitions, when a transposition system involves but a single process of inscription, followed by a single process of transcription, the system may be referred to as monophase transposition, commonly called single transposition. When one or more rescriptive processes intervene between the original inscription and the final transcription the system may be referred to as polyphase transposition. As a general rule, the solution of the latter type is much more difficult than the former, especially when the transpositions are theoretically correct in principle.

b. Any system which is suited for monophase transposition is also usually suited for polyphase transposition, the processes of inscription, rescription and transcription being accomplished with the same or with different keys.

SECTION II

SOLUTION OF SIMPLE TRANSPOSITION CIPHERS

4. Simple types of transposition. - a. The simple cases of reversed writing, vertical writing, or rail fence writing hardly require serious attention, since they may be solved almost by inspection. These methods are included here only because they may be encountered in censorship operations.

b. The low degree of cryptographic security afforded by these methods may be increased to a slight degree by adding nulls or by disguising the original word lengths, and regrouping into false words or into groups of regular length.

c. Some examples of these simplest types of transposition follow. Let the message be: BRIDGE DESTROYED AT ELEVEN PM.

(1) Reversing only the words and retaining original word lengths:

Cipher .. E G D I R B D E Y O R T S E D T A N E V E L E M P

(2) Reversing only the words and regrouping into false word lengths:

Cipher .. E G D I R B D E Y O R T S E D T A N E V E L E M P

(3) Reversing the whole text and regrouping into fives:

Cipher .. M P N E V E L E T A D E Y O R T S E D E G D I R B

(4) Reversing the whole text, regrouping into fives, and inserting a null in every fifth position:

Cipher .. T R I M M P N E V P E L E T A A D E Y R O R T S L

E D E G U D I R B M

(5) Writing the text vertically in two columns and taking the resulting digraphs for the cipher text, as shown at the side. The cipher message becomes:

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

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

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

These simple types can be solved merely by inspection.

5. The principles of solution of uniliteral route transposition ciphers. - a. The so-called uniliteral route transposition methods[1] are next to be examined. The solution of cryptograms enciphered by these methods is a matter of experimenting with rectangles of various dimensions suggested by the total number of letters in the message, then inspecting these rectangles, searching for whole words or the fragments of words by reading horizontally, diagonally, vertically, spirally, and so on.

b. The amount of experimentation that must be performed in the solution of ciphers of this type may be materially shortened by means of formulae and tables constructed for the purpose. But because ciphers of this type are of infrequent occurrence today, these

---

[1]See Special Text No. 165, Elementary Military Cryptography, 1935, Pars. 20, 21.

formulae and tables are only occasionally useful and hence they have been placed in an appendix to this volume.[2]

6. Keyed columnar transposition with completely-filled rectangles. - a. In practical cryptography, the dimensions of the transposition rectangle, as a general rule, cannot vary between large limits; that is, it can be assumed in practice that rectangles based upon lines of writing containing less than 5 letters or more than 25 letters will not commonly be encountered. If the width, that is, the number of columns, is determined by a key, then the number of rows becomes a function of the length of the message to be enciphered. If the latter is very long, longer than can be conveniently handled without too many errors, it is a common practice to break up a message into two or more parts and treat each part as though it were a separate communication.

b. When the last row of a transposition rectangle is completely filled, the solution of the resulting cryptogram is considerably more simple than when this is not the case.[3] Consequently, this will be the first case to be studied.

c. In solving a cryptogram of this type the first step taken by the cryptanalyst is to ascertain the dimensions of the rectangle. Clues for this are usually afforded by finding the factors of the total

---

[2]See Appendix 1.

[3]See Special Text No. 165, Elementary Military Cryptography, 1935, Sec. V.

number of letters in the cryptogram. Suppose the cryptogram contains 152 letters. The dimensions of the transposition rectangle may be 4 x 38, 8 x 19, by which is meant that four hypotheses may be made with respect to its dimensions. The rectangle may consist of:

(1) 4 columns with 38 rows, or

(2) 38 columns with 4 rows, or

(3) 8 columns with 19 rows, or

(4) 19 columns with 8 rows.

In practical work it is rather unlikely to encounter a rectangle that conforms to hypothesis (1) or (2), and for the present these may be discarded. As to choosing between hypotheses (3) and (4), a rather simple test will disclose which is the more likely to be true.

d. It is obvious that if the cryptogram is transcribed within a rectangle of the correct dimensions, the letters in each row will be the ones which actually were in those rows in the original transposition rectangle and formed good plain text therein. In fact, the rows of letters in the correctly-dimensioned rectangle would read plain text were it not for the transposition which they have undergone within the rows. Therefore, the rows of a correctly-dimensioned rectangle are more likely to manifest the expected vowel-consonant proportions of normal plain text than are the rows of an incorrectly-dimensioned rectangle, because in the latter case there are brought into some of the rows letters which belong to other rows and which are likely to disturb the normal vowel-consonant proportions of plain text. That is, in an incorrectly-dimensioned rectangle some of the rows will have too many consonants and not enough vowels, in other rows this relationship will be reversed; whereas in a correctly-dimensioned rectangle each row will have the proper number of vowels and consonants. Hence in solving an unknown cryptogram of this type, if a count is made of the vowels and consonants in the rows of rectangles of various probable dimensions, that rectangle in which the rows show the best distribution of vowels and consonants is most likely to be the correctly-dimensioned one, and the one that should be tried first.

e. Having ascertained the correct dimensions of the rectangle by the foregoing procedure, the next step is to experiment with the columns of the rectangle, trying to bring together several which will show good digraphs, trigraphs, or polygraphs in the rows thereof. This process of combining or matching columns in order to build up these fragments of plain text will herein be referred to as anagramming.[4]

---

[4] The Standard Dictionary defines the word anagram as follows: "(noun) 1. The letters of a word or phrase so transposed as to make a different word or phrase; as, 'time' and 'mite' are anagrams of 'amit'. 2. A transposition; interchange." As a verb, it is defined as "to anagrammatize; to make an anagram of; make anagrams." (The construction of anagrams was a very widespread pastime in previous centuries. See Wheatley's Of Anagrams, London, 1862.) A strict interpretation of the word would therefore confine it to cases wherein the letters to be rearranged already form bonafide words or intelligible phrases. However, this would hardly be broad enough for cryptanalytic purposes. As used in cryptanalysis the word is commonly employed as a verb to refer to the process of rearranging the disordered letters of cipher text so as to reconstruct the original plain text.

The procedure is to select a column which has a good assortment of high-frequency letters and find another column which may be added before or after the selected column to build up high-frequency digraphs; when such a pair of columns has been found, attempt is made to add another column before or after this pair to build up high-frequency trigraphs, and so on, gradually building up longer and longer polygraphs until entire words begin to appear in the various rows of the rectangle. In this process of anagramming advantage may be taken of such simple mathematical considerations as adding the normal plain-text frequency values of the digraphs in the columns to assist in discarding combinations which are on the borderline of choice. Once a set of four or five columns has been correctly assembled it is usually the case that the process may be completed very quickly, for with the placement of each column the number of remaining columns possible for selection diminishes; toward the close of the process, when only two or three columns remain, their placement is almost automatic.

f. It is desirable as a final step to try to reconstruct, if possible, the literal key from which the numerical transposition key was derived.

7. Example of solution. - a. Given the following cryptogram, the steps in solution will be set forth in detail:

CRYPTOGRAM (126 letters)

```
ILHHD  TIEOE  UDHTS  ONSOO  EEEEI  OEFTR
RHNEA  TNNVU  TLBFA  EDFOY  CAPDT  RRIIA
RIVNL  RNRWE  TUTCU  VRAUO  OOFDA  ONAJI
UPOLR  SOMTN  FRANF  MNDMA  SAFAT  YECFX
RTGET  A
```

b. The cryptogram contains 126 letters and the factors of 126 are 2, 3, 7, 9, 21, suggesting rectangles 7 x 18 or 9 x 14. If the former dimensions are taken, the rectangle may have 7 columns and 18 rows or 18 columns and 7 rows; if the latter dimensions are taken, it may have 9 columns and 14 rows or 14 columns and 9 rows. In making the vowel-consonant test described in Par. 5d, it is advisable to make the count on the columns as well as the rows of a rectangle, since it is possible that the cryptogram was prepared by inscribing the plain text in rows and transcribing the text from the columns, or vice versa. After examining a rectangle both horizontally and vertically, it is often possible to discard various arrangements without further tests. For example, Fig. 1a shows a rectangle of 7 columns and 18 rows. Now in

7 x 18

Row No.	1	2	3	4	5	6	7	No. of vowels
1	I	O	N	T	T	U	M	3
2	L	O	N	R	C	P	A	2
3	H	E	V	R	U	O	S	3
4	H	E	U	I	V	L	A	4
5	D	E	T	I	R	R	F	2
6	T	E	L	A	A	S	A	4
7	I	I	B	R	U	O	T	4
8	E	O	F	I	O	M	Y	5
9	O	E	A	V	O	T	E	5
10	E	F	E	N	O	N	C	3
11	U	T	D	L	F	F	F	1
12	D	R	F	R	D	R	X	0
13	H	R	O	N	A	A	R	3
14	T	H	Y	R	O	N	T	2
15	S	N	C	W	N	F	G	0
16	O	E	A	E	A	M	E	6
17	N	A	P	T	J	N	T	1
18	S	T	D	U	I	D	A	3
No. of vowels	7	11	6	6	10	4	7	

a

18 x 7

Row No.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	No. of vowels
1	I	E	S	E	T	T	B	Y	R	N	T	A	A	P	T	M	F	X	6
2	L	O	O	E	R	N	F	C	I	L	U	U	O	O	N	N	A	R	9
3	H	E	N	E	R	N	A	A	I	R	T	O	N	L	F	D	T	T	6
4	H	U	S	I	H	V	E	P	A	N	C	O	A	R	R	M	Y	O	7
5	D	D	O	O	N	U	D	D	R	R	U	O	J	S	A	A	E	E	9
6	T	H	O	E	E	T	F	T	I	W	V	F	I	O	N	S	C	T	6
7	I	T	E	F	A	L	O	R	V	E	R	D	U	M	F	A	F	A	8
No. of vowels	2	4	4	6	2	1	3	2	4	1	2	5	5	2	1	2	3	2	

b

9 x 14

Row No.	1	2	3	4	5	6	7	8	9	No. of vowels
1	I	S	T	B	R	T	A	T	F	2
2	L	O	R	F	I	U	O	N	A	5
3	H	N	R	A	I	T	N	F	T	2
4	H	S	H	E	A	C	A	R	Y	4
5	D	O	N	D	R	U	J	A	E	4
6	T	O	E	F	I	V	I	N	C	4
7	I	E	A	O	V	R	U	F	F	5
8	E	E	T	Y	N	A	P	M	X	4
9	O	E	N	C	L	U	O	N	R	4
10	E	E	N	A	R	O	L	D	T	4
11	U	I	V	P	N	O	R	M	G	3
12	D	O	U	D	R	O	S	A	E	5
13	H	E	T	T	W	F	O	S	T	2
14	T	F	L	R	E	D	M	A	A	3
No. of vowels	6	10	3	5	5	7	7	3	5	

c

14 x 9

Row No.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	No. of vowels
1	I	F	O	F	N	E	T	N	T	O	U	N	M	C	6
2	L	U	O	T	N	D	R	L	C	F	P	F	A	F	3
3	H	D	E	R	V	F	R	R	U	D	O	R	S	X	3
4	H	H	E	R	U	O	I	N	V	A	L	A	A	R	7
5	D	T	E	H	T	Y	I	R	R	O	R	N	F	T	4
6	T	S	E	N	L	C	A	W	A	N	S	F	A	G	4
7	I	O	I	E	B	A	R	E	U	A	O	M	T	E	10
8	E	N	O	A	F	P	I	T	O	J	M	N	Y	T	6
9	O	S	E	T	A	D	V	U	O	I	T	D	E	A	8
No. of vowels	4	3	9	2	2	4	4	2	5	5	3	1	5	2	

d

FIGURE 1.

a row of 7 letters there should be ($7 \times 40\% = 2.8$) either 2 or 3 vowels; but rows 12 and 15 contain no vowels at all and rows 8 and 9 contain 5 vowels, row 16, 6 vowels. It is concluded at once that this arrangement is highly improbable. If the plain text had been inscribed vertically in this same rectangle, and then the rows had been transposed in forming the cipher text, then in each column (18 letters) there should be ($18 \times 40\% = 7.2$) about 7 vowels; but column 2 contains 11 vowels and column 6 only 4. This likewise indicates that it is highly improbable that the message was inscribed vertically and the cryptogram formed by transposing the rows. But when the arrangement in Fig. 1_b_ is studied, it is not so easy to say at once that it is improbable. For in 18 letters there should be about 7 vowels and none of the rows of this arrangement shows too great a departure from this expected number. This possibility will have to be explored further and it is for the moment put aside. If it be assumed that the message was inscribed vertically in the rectangle 18 x 7 and the rows subjected to transposition, there should be ($7 \times 40\% = 2.8$) 2 or 3 vowels in each column. But since several of the columns show rather considerable departures from this expected number, it may be concluded that a vertical inscription and horizontal transposition is not probable and this assumption may be eliminated. Then the arrangements in Fig. 1_c_ and _d_ are studied in the same manner, with the result that at the end of the study the situation as regards the various assumptions is summarized as follows:

Rectangle 7 x 18

7 columns and 18 rows:
(1) Horizontal inscription, columnar transcription .... Very Improbable
(2) Vertical inscription, horizontal transcription .... Very Improbable

18 columns and 7 rows:
(3) Horizontal inscription, columnar transcription ..... Possible
(4) Vertical inscription, horizontal transcription ..... Improbable

Rectangle 9 x 14

9 columns and 14 rows:
(5) Horizontal inscription, columnar transcription ..... Possible
(6) Vertical inscription, horizontal transcription ..... Improbable

14 columns and 9 rows:
(7) Horizontal inscription, columnar transcription ..... Improbable
(8) Vertical inscription, horizontal transcription .... Very Improbable

c. Discarding all assumptions except (3) and (5), the latter are subjected to further scrutiny. Suppose the average amount of deviation from the expected number of vowels in each row is calculated by finding the difference between the actual and expected numbers in each row, adding these differences (neglecting signs), and dividing by the total number of rows. For assumptions (3) and (5) the results are as follows:

13 x 7

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	No.of Vowels	Deviation from expected No.
1	I	E	S	E	T	T	B	Y	R	N	T	A	A	P	T	M	F	X	6	1.2
2	L	O	O	E	R	N	F	C	I	L	U	U	O	O	N	N	A	R	9	1.8
3	H	E	N	E	R	N	A	A	I	R	T	O	N	L	F	D	T	T	6	1.2
4	H	U	S	I	H	V	E	P	A	N	C	O	A	R	R	M	Y	G	7	.2
5	D	D	O	O	N	U	D	D	R	R	U	O	J	S	A	A	E	E	9	1.8
6	T	H	O	E	E	T	F	T	I	W	V	F	I	O	N	S	C	T	6	1.2
7	I	T	E	F	A	L	O	R	V	E	R	D	U	M	F	A	F	A	8	.8
																			Total deviation =	8.2
																			Average deviation =	1.2

FIGURE 1b.

9 x 14

	1	2	3	4	5	6	7	8	9	No. of Vowels	Deviation from expected No.
1	I	S	T	B	R	T	A	T	F	2	1.6
2	L	O	R	F	I	U	O	N	A	5	1.4
3	H	N	R	A	I	T	N	F	T	2	1.6
4	H	S	H	E	A	C	A	R	Y	4	.4
5	D	O	N	D	R	U	J	A	E	4	.4
6	T	O	E	F	I	V	I	N	C	4	.4
7	I	E	A	O	V	R	U	F	F	5	1.4
8	E	E	T	Y	N	A	P	M	X	4	.4
9	O	E	N	C	L	U	O	N	R	4	.4
10	E	E	N	A	R	O	L	D	T	4	.4
11	U	I	V	P	N	O	R	M	G	3	.6
12	D	O	U	D	R	O	S	A	E	5	1.4
13	H	E	T	T	W	F	O	S	T	2	1.6
14	T	F	L	R	E	D	M	A	A	3	.6
										Total deviation =	12.6
										Average deviation =	.9

FIGURE 1c.

The average amount of deviation for assumption (5) is only .9 as against 1.2 for assumption (3); therefore the former assumption is considered to be somewhat better than the latter and it will be tried first.

d. The columns of the rectangle shown in Fig. 1c are now to be cut apart and the procedure of anagraming applied. (For this it is best to have the cryptogram written on cross-section paper preferably with 1/2-inch squares for ease in handling.) Consider column 7, with the letter J in row 5; this letter, if it is a part of a word, must be followed by a vowel, which eliminates columns 1, 3, 4, and 5 as possibilities for placement on the right of column 7. Here are the digraphs formed by combining column 7 with 2, 6, 8 and 9, and the totals obtained by adding the frequency values of the digraphs:[5]

(1) 7-2	Frequency Value	(2) 7-6	Frequency Value	(3) 7-8	Frequency Value	(4) 7-9	Frequency Value
A S	41	A T	47	A T	47	A F	4
O O	6	O U	37	O N	77	O A	7
N N	8	N T	82	N F	9	N T	82
A S	41	A C	14	A R	44	A Y	12
J O	2	J U	2	J A	1	J E	2
I O	41	I V	25	I N	75	I C	22
U E	11	U R	31	U F	1	U F	1
P E	23	P A	14	P M	4	P X	0
O E	3	O U	37	O N	77	O R	64
L E	37	L O	13	L D	9	L T	8
R I	30	R O	28	R M	9	R G	7
S O	15	S O	15	S A	24	S E	49
O E	3	O F	25	O S	14	O T	19
M F	1	M D	1	M A	36	M A	36
Totals	262		371		427		313

FIGURE 2.

Combination (3) gives the highest frequency value for the digraphs and an attempt is made to add a column to it. Here are some of the combinations tried:

---

[5] The frequencies shown are as given in Table 6, Appendix to Military Cryptanalysis, Part I. The totals obtained by addition of the frequency values of the digraphs should be considered only as rough approximations or guides in weighing probabilities in favor of one hypothesis against another, for theoretically the probability of the simultaneous occurrences of two or more independent events is the product, and not the sum, of their respective probabilities. However, in this case the calculation of the products would involve an amount of labor entirely unwarranted by the results to be expected, so that a simple addtion of the probabilities is considered sufficient.

7-8-1	7-8-2	7-8-3	7-6-9
A T I	A T S	A T T	A T F
O N L	O N O	O N R	O N A
N F H	N F N	N F R	N F T
A R H	A R S	A R H	A R Y
J A D	J A O	J A N	J A E
I N T	I N O	I N E	I N C
U F I	U F E	U F A	U F F
P M E	P M E	P M T	P M X
O N O	O N E	O N N	O N R
L D E	L D E	L D N	L D T
R M U	R M I	R M V	R M G
S A D	S A O	S A U	S A E
O S H	O S E	O S T	L S T
M A T	M A F	M A L	M A A

FIGURE 3

e. Each of these combinations shows at least one "impossible" trigraph and several "poor" ones.[6] After more or less work along these lines, the cryptanalyst begins to get the feeling that "something is wrong," for, as a rule, once a correct start has been made in cases of this kind, solution comes rather quickly. Hence, the cryptanalyst decides here that possibly his first choice of combination (3) was a bad one, even though it gave the greatest total when frequency values for the digraphs were summed. The second greatest total was for combination (2), in which columns 7 and 6 were put together. The infrequent digraph JU suggests a word such as JUST or JUNCTION. If it were the former there should be a column containing an S in the 5th row, and there is no such column. If the word is JUNCTION, there should be a column containing an N in the 5th row, and there is only one such

---

[6] Following the steps taken in subparagraph d, frequency weights may be given the various trigraphs in Fig. 3 and the sums obtained taken as indications of the relative probability of each of the four trials. These steps are here omitted, for they are obvious.

column, the 3d. Placing column 3 after column 7-6 gives the trigraphs shown in Fig. 4. All of these trigraphs are excellent except the last, and that one may be either an abbreviation of a signature, or possibly nulls added to complete the rectangle. If the word JUNCTION is correct then there should be a column with a C in the 5th row; but none is found. However, column 9 has a C in the 6th row, and if it happened that the last column on the right is number 3, then column 9 would be the 1st column. Thus, as shown in Fig. 5, the arrangement of columns becomes quite definite:

```
7-6-3

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

FIGURE 4.

```
9-?-?-?-?-?-7-6-3

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

FIGURE 5.

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

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

FIGURE 6.

f. It is believed that the procedure has been set forth with sufficient detail so as to make further demonstration unnecessary. The rectangle can be completed very quickly and is found to be as shown in Fig. 6.

8. The probable-word method of solution. - a. The probable-word method of attack is as important in the solution of transposition ciphers as it is in the solution of substitution ciphers, and if the

cryptanalyst is able to assume the presence of such probable words as are usually encountered in military communications, the solution, as a rule, comes very quickly.

b. As an illustration, looking at the first row of letters in the rectangle shown in Fig. 1c, the letters I S T B R T A T F almost at once suggest FIRST BATTALION as the initial words of the message. A rearrangement of the columns of the cryptogram to bring the necessary letters into juxtaposition at once discloses the key. Thus:

9	1	5	2	8	4	7	6	3
F	I	R	S	T	B	A	T	T
A	L	I	O	N				

It will be noted that this assumption requires that there be a column headed by FA, another headed by IL, another headed by RI, and so on. Had such columns not been found, then the word BATTALION would not be possible. In that case the word FIRST would still remain as a point of departure for further experimentation.

c. In the foregoing illustration, the probable word was assumed to appear in the first line of text in the rectangle. If the probable word being sought is in the interior of the message, the steps must be modified somewhat but the basic principle remains unchanged. The modifications are of course obvious.

9. General remarks on solution. - a. In solving transposition ciphers advantage should be taken of all the characteristics and idiosyncrasies which are peculiar to the language of the enemy, because they often afford clues of considerable assistance to the cryptanalyst. In all languages there are certain letters, usually of medium or low

frequency, which combine with other letters to form digraphs of high frequency. For instance, in English the letter H is of medium frequency, but it combines with T to form the digraph TH, which is of highest frequency in literary text; it also combines with C, a letter of medium frequency, to form the fairly frequent digraph CH. The letter V is almost in the low-frequency category yet it combines with E to form the digraph VE, which in military text is the 14th in frequency. The low-frequency letter K often combines with C to form the digraph CK. Consequently, in working with transposition ciphers in English, when there is an H, attempts should be made to combine it first with a T, or with a C; a V should be combined first with an E; a K should be combined first with a C; and so on.

b. There is usually in every language at least one letter which can be followed by only a certain other letter, forming what may be termed an obligatory sequence, or an invariable digraph. In all languages having the letter Q, the combination QU constitutes such an invariable digraph.[7] In genuine words of the German language the letter C is never used by itself, when present the letter C is invariably followed by an H, except on rare occasions when the digraph CK is employed. In English, the letter J can be followed only by a vowel; the letter X can only be preceded by a vowel and, except at the end of a word, can only be succeeded by a vowel, and so on. Letters

---

[7] The letter Q may, of course, be part of an abbreviation, such as SQ for "square", or it may be used as a null, or as a sign of punctuation. However, unless there are good reasons for believing that this letter is used for these purposes, QU may be considered to be an invariable digraph.

which behave in this manner, that is, letters which have what may be called a <u>limited affinity</u> in combining with other letters to form digraphs, constitute good points of departure for solution and are therefore of sufficient importance to warrant their being designated by the more or less descriptive name of <u>pilot letters</u>.

<u>c</u>. The presence of pilot letters in a transposition cipher often forms the basis for the assumption of probable words. Obviously, a special lookout should be kept for <u>words</u> of rather high frequency (in military correspondence) which contain <u>letters</u> of low or medium frequency. The frequent word CAVALRY, for example, would suggest itself if the cryptogram has the letters C, V, L, and Y, which are all of medium frequency. The important word ATTACK suggests itself if the cryptogram has a K, a letter of low frequency and a C, one of medium frequency; and so on.

<u>d</u>. The mechanics of simple columnar transposition make possible the production of rather long sequences of vowels and long sequences of consonants in the text of the cryptogram. Note, for example, in the cryptogram on p. 11, the sequence of vowels O O E E E E I O E, and the sequence of consonants V N L R N R W. If the enciphering or plain-text rectangle is consulted, it will be seen that these two sequences belong together, that is, they are in adjacent columns in that rectangle. It is a characteristic of plain text that consonant-vowel or vowel-consonant digraphs are much more frequent than consonant-consonant or vowel-vowel digraphs,[8] and therefore when long sequences of consonants

---

[8] The CV and VC digraphs constitute about 62 per cent of all digraphs.

and of vowels are found in transposition ciphers, a good start toward solution may result from assuming that such sequences come from adjacent columns.

e. It should, however, be noted in connection with tell-tale letters such as Q (entering into the composition of QU) and C (entering into the composition of CH), that astute cryptographers who realize the clues which such letters afford often replace the invariable sequences they form by a single character, usually one that is rarely used in the language in question. For example, CH in German may be replaced by Q, QU in French, by K, and so on. When this is done, solution is made more difficult; but only in those cases where it is dependent upon finding letters forming obligatory sequences in plain text does this sort of subterfuge become a factor of importance.

f. The presence of many Q's, or K's, or X's in a transposition cipher should not, however, be taken as prima facie evidence of the type of replacement noted in the preceding subparagraph. It is possible that such letters may be used as sentence separators or other punctuation, or possibly they may be nulls, although the alert cryptographer would either use nulls not at all or, if he had to, would use letters of medium or high frequency for this purpose.

g. Because it is important that the cryptanalyst take advantage of every peculiarity specifically applicable to a cryptogram to be solved, especially as regards the presence of low-frequency letters, it is advisable that a uniliteral frequency distribution be prepared, just as though he were going to deal with a substitution cipher. This is probably the quickest way of bringing to light the peculiarities which may be helpful in solution.

10. Reconstruction of literal key. - a. The reconstruction or recovery of the literal key from which the numerical transposition key was derived is naturally the last step in the solution of cryptograms of this type. It is often of more than merely academic interest, because if it is found that the enemy is employing for this purpose words or phrases of a simple nature associated with the locale of operations this fact may be of importance in subsequent work.

b. In this process there are only a few guiding principles to be noted and much must be left to the ingenuity and imaginative powers of the cryptanalyst. Taking as an example the numerical key uncovered in the solution of the cryptogram in Par. 7, the procedure will be set forth below.

c. The numerical key referred to was found to be 9-1-5-2-8-4-7-6-3. Assuming that this sequence was derived in the usual manner, by assigning numbers to the letters of a keyword in accordance with their relative positions in the normal alphabet, then it is likely that the digit 1 in the foregoing numerical key represents a letter at or at least close to the beginning of the alphabet. Since the digits 2 and 3 are to the right of 1 in the key, it is likely (1) that the letter represented by 1 occurs two more times in the keyword, or (2) that they represent another letter, also near the beginning of the alphabet, and repeated, or (3) that they represent two different letters both near the beginning of the alphabet. The digit 4 must represent a letter beyond the letter represented by the digit 3; the digit 5 must represent one beyond the letter represented by the digit 4, and so on. Assuming that the letters composing the keyword are fairly well distributed over the entire alphabet the digit 7 must represent a letter near or slightly beyond the middle of the alphabet, the digit 8 must represent one further toward the end of the alphabet than does the digit 7, and so on. Assigning several values to the digits, in accordance with the foregoing principle, the results are as follows:

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

FIGURE 7.

d. Now comes the trying process of finding a "good" word in this assemblage of letters. The beginning and end of the word are the easiest points of attack, and it is useful to keep in mind the relative frequency order of letters as initial and final letters of the language in question.

For English, the data are as follows:[9]

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

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

Studying the list of letters at the end of the key, it is seen that E is one of the possibilities. If that is correct, then a good ending would be one of the type V-C-V, with E as the final letter. There is

---

[9] Taken from Tables 2-D (2) and 2-E (2), p. 111, Military Cryptanalysis, Part I.

but one vowel in the column under the digit 7, the letter O. This gives OKE, OLE, OME, ONE as possible ending trigraphs, the best of which from a frequency standpoint is ONE. Seeing the letters P and H in columns 5 and 6, the ending PHONE and then the word TELEPHONE suggests itself. Checking to see if there are any inconsistencies, none is found and the solution is:

Column number	1-2-3-4-5-6-7-8-9
Numerical key	9-1-5-2-8-4-7-6-3
Literal key	T E L E P H O N E

e. In future studies cases will be encountered wherein the reconstruction of the numerical key is an essential or at least useful element after the solution of one or more cryptograms has been achieved by cryptanalysis; this is done in order that subsequent cryptograms in the same key can be read directly without cryptanalysis. The reconstruction of the numerical key is, however, a different process than the one illustrated in this paragraph, wherein the problem is solely one of building up a literal key from its numerical equivalent.

11. Column and row transposition. - It should be obvious that when the rows as well as the columns of a completely-filled rectangle undergo transposition the increase in security is hardly worth mention, since the underlying procedure in solution aims simply at assembling a few columns on the basis of "good" digraphs and trigraphs brought to light by juxtaposing columns. After three or four columns have been properly juxtaposed, the placement of additional columns becomes easier and easier, merely by continuing to build upon the fragments of words in the rows. Hence, the cryptanalyst is, during a large part of the process, not particularly interested in the intelligibility of the text

he is building up; only at the end of the process does this become a factor. When all of the columns have been assembled in proper order, then the text will read continuously in the normal manner (left to right, top to bottom). If it does not, then it is usually a very simple matter to rearrange the rows of the rectangle to bring this about, since the letters at the ends and beginnings of the rows give the necessary clues for continuity.

SECTION III.

INCOMPLETELY-FILLED RECTANGLES

12. General principles underlying solution. - a. In the system designated keyed columnar transposition the feature which differentiates an incompletely-filled rectangle from one that is completely filled is a very simple one from the cryptographic point of view: the bottom row of the rectangle in the former case merely lacks one or more letters, a feature which only very slightly complicates the system in practical operation. But the consequences of this simple difference between the two types are, from the cryptanalytic point of view, quite profound, and the cryptanalytic effect of this small change in cryptographic procedure is seemingly all out of proportion with the simplicity of the difference.

b. Cryptograms involving completely-filled rectangles are rather easy to solve because of two circumstances. In the first place, since the rectangle is completely filled, the various possible dimensions of the rectangle can be ascertained by noting the factors of the total number of letters. Usually only a few possibilities are indicated and therefore this materially reduces the amount of experimentation that would be required in the absence of this situation, since it is obvious that when working with incompletely-filled rectangles a good many rectangles of various dimensions become possibilities for trial.

In the second place, the columns in a completely-filled rectangle all contain the same number of letters, and therefore the anagramming process (matching and assembling of columns) can be performed without any mental reservations such as must be made in working with incompletely-filled rectangles because of uncertainty as to whether the letters which are juxtaposed to form digraphs and trigraphs really come from the same row in the plain-text rectangle. The latter statement calls for a bit more explanation.

c. The columns of an incompletely-filled rectangle are of two sorts which may conveniently be designated as long and short. The long columns are at the left of the rectangle and each one contains just one more letter than the short columns, which are at the right. This follows, of course, from the fact that it is only the last row in such a rectangle which lacks one or more letters to complete the rectangle. The term width, as applied to a transposition rectangle, will be convenient to designate the number of columns, which is, of course, determined by the length of the numerical key or the number of letters in the literal key. Given the width of the rectangle and the total number of letters in the cryptogram, the length and number of the long and the short columns may be found by a simple calculation: Multiply the width of the rectangle by the smallest number which will yield a product greater than the total number of letters in the cryptogram. The multiplier gives the length of the long columns; this multiplier minus 1 gives the length of the short columns; the excess over the total number of letters gives the number of short columns, the latter deducted from the width gives the number of long columns. Thus, with a cryptogram of 287 letters and a rectangle 15 columns in width: [(15 x 20) - 13 = 287]; the long columns will have 20 letters, the short ones, 19 letters; there will be 13 short columns and 2 long ones.

d. Now if the cryptanalyst were able to cut up the text of a cryptogram produced from an incompletely-filled rectangle into sections corresponding in length with the actual long and short columns, he could handle these columns in exactly the same manner that he handles the equal-length columns in the solution of a cryptogram produced from a completely-filled rectangle. In fact, the solution would be easier because he knows that all the short columns fall at the right, all the long columns at the left of the transposition rectangle, and therefore the amount of experimentation he must undertake in his attempts to juxtapose columns in the anagramming process is considerably reduced. But, unfortunately, there is usually no way in which, at the initial stage of solution, the cryptanalyst can find out, from a single cryptogram, which are the long columns and which the short. This is obviously a matter directly connected with the specific transposition key, and the latter is the sole unknown factor in the whole problem.

e. If it were practicable to transcribe a cryptogram of this type according to all the possible transposition keys for a given width of rectangle, solution would obviously merely consist in scanning the various rectangles to find the one which is correct - for there will be only one such rectangle. A rectangle 15 columns in width may have been enciphered by any one of factorial 15 transposition keys.[1] While it is

[1] Factorial 15, or 15 x 14 x 13 x ... x 1, equals 1,369,944,576,000 different transposition keys.

conceivable that machinery might be devised for this purpose, so that the production of the millions of possible rectangles could be effected in a relatively short time, in the present state of the art no such machinery has yet been devised. Furthermore, it is problematical whether a solution by such means could be achieved in a reasonable length of time even if the machinery were available, because of the immensity of the task it would have to perform.

f. However, this question may be asked: Given a cryptogram of T letters and a rectangle of n columns in width, is it possible to transcribe the text within a single rectangle so that the latter will show what letters will constitute the respective columns for all possible transposition keys of n elements? If so, then such a rectangle would be useful in trying to solve the cryptogram, because the rectangle would then limit the amount of experimentation that would have to be performed by the anagramming process, since it would show whether or not two letters which are brought together in that process to form a digraph could possibly have been in the same row in the plain-text rectangle. If not, then of course there would be no use in forming such digraphs, and thus the number of trials becomes much reduced. Another way of indicating what is meant is to say that such a rectangle would show the maximum amount that one column may be shifted up or down in trying to match it with another column in the anagramming process. This will be made clearer in a subsequent paragraph. At this point it will merely be stated that it is easy to prepare a rectangle of the nature indicated above, for any keyed columnar transposition cryptogram.

13. Construction of diagram. - a. Given the following cryptogram of 224 letters and an assumed width of 12 columns in the enciphering rectangle:

CRYPTOGRAM

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

Distribution

b. A cryptogram of 224 letters and a rectangle of 12 columns [(12 x 19) - 4 = 224] indicates 4 short columns of 18 letters and 8 long columns of 19 letters. The outlines of a rectangle of this specification are drawn on a sheet of cross-section paper and the text is transcribed within it, for the moment assuming merely that the transposition key consists merely of the straight sequence of numbers 1 to 12. Thus:

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

FIGURE 8.

c. The rectangle shown in Fig. 8 is the same as though it had been assumed that the key numbers 9, 10, 11, and 12 happened to fall at the extreme right in the numerical transposition key. Columns 1 to 8, inclusive, would then be long columns, and columns 9, 10, 11, and 12 would be short columns. But suppose that the key numbers on the extreme right happened to be 1, 2, 3, and 4, instead of 9, 10, 11, and 12. Then columns 1, 2, 3, and 4 would be the short columns, 5 to 12 the long ones. In this case, making reference to Fig. 8, the final letter of column 1 would pass to the top of column 2; the final two letters of column 2 would pass to the top of column 3; the final 3 letters of column 3 would pass to the top of column 4; the final 4 letters of columns 4, 5, 6, 7, and 8 would pass to the top of columns 5, 6, 7, 8, and 9; the final 3 letters of column 9 would pass to the top of column 10; the final 2 letters of column 10 would pass to the top of column 11; and the final letter of column 11 would pass to the top of column 12. The results of the foregoing reasoning are indicated in Fig. 9.

d. Now the capital letters in Fig. 9 represent the letters which are in the columns in case the first hypothesis (key numbers 9, 10, 11, 12 at the extreme right) is true. The capital letters above the heavy

	1	2	3	4	5	6	7	8	9	10	11	12
1					t	m	u	i	e			
2				e	e	b	m	e	f	e		
3			t	a	e	i	e	t	e	s	y	
4		l	d	a	e	e	t	e	a	r	t	r
5	O	N	M	C	M	H	Y	T	O	A	F	A
6	D	I	A	T	I	B	O	N	O	I	I	T
7	N	E	N	R	A	V	I	O	T	I	T	S
8	N	T	L	M	I	T	K	T	H	E	A	O
9	P	G	N	S	T	B	N	R	E	A	N	A
10	T	N	O	C	E	E	K	A	A	T	L	L
11	I	W	E	L	A	S	T	A	C	E	N	O
12	R	T	B	C	I	R	N	V	N	E	N	D
13	N	T	O	S	J	S	D	R	S	A	U	I
14	T	M	U	O	N	Y	A	I	H	L	A	R
15	D	E	H	E	S	L	H	R	E	A	C	O
16	T	D	E	F	O	X	I	S	E	E	L	R
17	U	S	N	C	I	R	R	T	V	N	R	Y
18	R	T	L	F	V	O	H	G	T	E	E	N
19	O	E	E	F	F	R	Q	S	R	E	N	N
20	E	O	S	T	M	U	I	E	E	M	R	R
21	X	I	E	E	B	M	E	F	S	Y	T	G
22	A	T	A	E	I	E	T	E	R	T	R	Y
23	L	D	A	E	E	T	E	A				

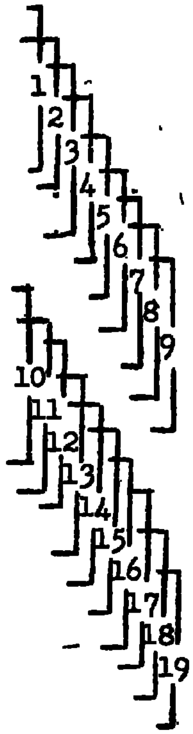


FIGURE 9.

black line together with the small letters at the top of the diagram (the latter forming what may be termed the crown) represent the letters which are in the columns in case the second hypothesis (key numbers 1, 2, 3, 4 at the extreme right) is true. Therefore, Fig. 9, since it covers the two possible extremes with reference to the positions occupied by the short columns, embraces all possible intermediate conditions and shows what letters may be in the respective columns under any possible arrangement of long and short columns, and hence this diagram is applicable to any possible numerical key for the cryptogram in question and for the assumed width of rectangle. Therefore, in the anagramming process such a diagram shows the maximum possible amount that any column may be shifted up or down in juxtaposing two columns to form digraphs of letters assumed to come from the same row in the plain-text rectangle. This is because all the letters of the 1st row of the actual enciphering rectangle will be found in rows 1 to 5, inclusive, of Fig. 9; all the letters of the 2d row of the rectangle will be found in rows 2 to 6, inclusive, and so on, as indicated by the braces at the right in Fig. 9.

e. Thus there arises the following important principle: Designating the number of short columns in a specific diagram by n, only such letters as fall within (n + 1) consecutive rows, will be letters that may have appeared in the same row in the actual transposition rectangle. Or, another way of stating the principle is this: both members of any pair of letters actually in the same row in the transposition rectangle will be found only among the letters appearing in (n + 1) consecutive rows in the reconstruction diagram. In the case under discussion, if the first letter of such a pair is located in row 8, for example, the other letter cannot be in rows 1, 2, 3, or 13 to 23 of Fig. 9.

f. The usefulness of this principle will soon become apparent. For example, again referring to Fig. 9, take the letter Q in row 19, column 7; it must be followed by a U in the plain text. There are 4 U's in the message; they are in row 13 column 11, row 14 column 3, row 17 column 1, and row 20 column 6. Now the question is, can any of these 4 U's follow the Q, or may one or more of them be eliminated from consideration at once? Since the U's in rows 13 and 14 fall outside the 4 consecutive rows above that in which the Q is located, it follows that neither one of these U's can be the one that succeeds the Q. Thus two candidates are automatically eliminated from consideration. The U in row 17 and the U in row 20 are both possible candidates.

14. Solution of example. - *a*. With the foregoing preliminaries out of the way, the solution of the cryptogram can now be carried forward with rapid progress. It has been indicated that the Q in row 19, column 7, (Fig. 9), may be combined with either the U in row 17 column 1, or the U in row 20 column 6. Suppose the columns of Fig. 9 are now cut apart for ease in anagramming. Juxtaposing the indicated columns yields what is shown in Fig. 10. Since the combination shown at Fig. 10*a* involves column 1, it obviously begins with the letter O and ends with the letter A or L; no other letters can be added to this column. Since column 7 is already the maximum length this column can be under any circumstances, no letters can be added to it at the bottom. Therefore, all the digraphs possible to form by juxtaposing these two columns are indicated in Fig. 10*a*. There are only 17 digraphs in all,

7-1		7-6	
u		u	b
m		m	i
e		e	e
t		t	H
Y		Y	B
O		O	V
I	O	I	T
K	D	K	B
N	N	N	E
K	N	K	S
T	P	T	R
N	T	N	S
D	I	D	Y
A	R	A	L
H	N	H	X
I	T	I	R
R	D	R	O
H	T	H	R
Q	U	Q	U
I	R	I	M
E	O	E	E
T	E	T	T
E	X	E	
	A		
	L		
a		b	

FIGURE 10.

whereas there should be at least 18. Hence, combination 7-1 is impossible, and combination 7-6 is the only one that needs to be considered further. There are many excellent digraphs in it, and only one which admittedly looks rather bad, the HX. Seeing the digraphs KB and KS in these columns, a good assumption to make is that the K's are preceded by the letter C. Is there a column with 2 C's in approximately the correct region? Column 4 meets this requirement. Note the excellent trigraphs it yields, as shown in Fig. 10c. It now becomes fairly easy to add columns to this nucleus. For instance, the trigraph R Y B suggests a word ending in R Y, such as INFANTRY, ARTILLERY, CAVALRY; the trigraph M O V suggests MOVING; the trigraph C K B suggests the word ATTACK; followed by a word beginning with B, and so on. Trial of only a few columns soon yields what is shown in Fig. 10d, from which it soon becomes probable that the long columns end with column 12, since the letters after L Y yield an impossible sequence (E E E Y). Since it was originally assumed that there are only 4 short columns in the transposition rectangle, and since 4 columns have already been placed at the right (4-7-6-10), the rectangle, with the columns thus far placed, must be as shown in Fig. 10e. This then at once tells what the limits of

```
4-7-6        1-12-4-7-6-D

e                  a u b
a u h              a m i e
a m i        o r c e e s
c e e        D A T t H r
T t H        N T R Y B A
R Y B        N S M O V I
M O V        P O S I T I
S I T        T A C K B E
C K B        I L L N E A
L N E        R O C K S T
C K S        N D S T R E
S T R        T I O N S E
O N S        D R E D Y A
E D Y        T O F A L L
F A L        U R C H X A
C H X        R Y F I R E
F I R        O N F R O N
F R O        E N T H R E
T H R        X R E Q U E
E Q U        A G E I M M
E I M        L Y E E E Y
E E E              T T T
  T T              E
  E
```

FIGURE 10c   FIGURE 10d

columns 2, 3, 5, 8, 9, and 11 must be, and the rectangle can now be filled in without further delay. The completed rectangle is shown in Fig. 11.

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

FIGURE 10e

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

FIGURE 11

b. The last step, recovering the literal key, is then taken. The key is to be found among the letters of the diagram in Fig. 12.

8	2	5	3	11	9	1	12	4	7	6	10
N	E	M	E	R	N	A	R	H	N	M	P
O	F	N	F	S	O	B	S	I	O	N	R
P	G	O	G	T	P	C	T	J	P	O	S
R	H	P	H		R	D		K	R	P	T

FIGURE 12

The termination ATIONS seems a likely possibility. If this is correct, assignment of letters becomes modified as shown in Fig. 13:

8	2	5	3	11	9	1	12	4	7	6	10
O	E	N	E	T	P	A	T	I	O	N	S
P					R						
R					S						

FIGURE 13.

The word PENETRATIONS will fit and it is taken to be presumably correct. There is no absolute certainty about the matter, for it is conceivable and possible that there are other words which can be made to fit the sequence of key numbers given, but inasmuch as the recovery of the literal key is not an essential part of the solution and is often merely a subject for curiosity or speculation, no further time will be spent on the matter.

15. Alternative method of solution. - a. The foregoing solution will no doubt appeal to the student as being straightforward and simple - if the original assumption as to the width of the transposition rectangle is correct. But, unfortunately, there is no way of knowing whether such an original assumption is correct until solution is well under way. In practice, of course, what might be done within a well-organized cryptanalytic unit would be to divide up the work among the

individuals constituting the unit, each being assigned one or more specific hypotheses to try out with respect to width of rectangle. Then one of these individuals would find the correct width and he would be joined by the others as soon as an entering wedge had been found in this way. Or, if the cryptanalyst is working alone, he must try out successive hypotheses as to width of rectangle until he hits upon the correct one. In making these hypotheses he must be guided by previous experience with enemy correspondence, which may afford clues as to minimum and maximum widths of rectangles.

b. However, there is another method of attack which does not necessitate making any definite initial assumptions with respect to the width of the transposition rectangle. This method is a modification of the method set forth in the preceding paragraph. The text of the cryptogram is written out columnwise on cross-section paper, every 5th letter being numbered for purposes of reference. Plenty of space is left between the columns, and about 10 or 15 letters at the bottom of each column are repeated at the top of the next column so that at any point in the transcription there will be in a single unbroken string at least one complete column of letters from the transposition rectangle. Then a section of consecutive letters of text is written on a separate strip of cross-section paper, columnwise of course, and by juxtaposing this strip against the whole text, sliding it to various points of coincidence against the text, an attempt is made to find that position in which the best digraphs are formed of the letters on the movable strip and the fixed sequence. Of course, if there is a Q in the cryptogram, the sliding strip section is made to contain this letter, and the strip is then placed against the text where a U is found, so as to form the digraph QU. The digraphs formed above and below the QU are then studied; possibly a written record is made of the digraphs found. Then the same thing is done with the Q and all other U's in the text, to insure that a correct start is made. It is this initial step which is likely to give the most difficulty (if there is anything difficult at all in the procedure) and it is important that it be correct. If this first step is easy, then solution follows quite rapidly; if the cryptanalyst is unlucky and makes several false starts, the process is likely to be a slow one. In choosing from among several possible juxtapositions it may be advisable to calculate the probability value of each possibility by adding the frequency values of the digraphs, as explained in Par. 7d. In the absence of any Q's in the text, recourse must be had to the formation of other probable digraphs, based upon the presence of certain other tell-tale low-frequency letters, such as C, H, J, K, V, and X. The cryptanalyst is fortunate if there are two or three of these low-frequency letters close to one another in a series of letters, for in this case he can search for a place where there are high-frequency letters (in a corresponding sequence) that might be combined with them. For example, suppose that a text shows a sequence ... V E H H K ...; a sequence such as ... A R T C C ... would be excellent to try, for it will yield the digraphs AV, RE, TH, CH, CK. Or if there is a long sequence of consonants, the cryptanalyst should look for a correspondingly long sequence of vowels, since these make the best combinations and are therefore most probable. For these reasons it pays to study the text quite carefully before choosing a starting point, to find all such peculiar sequences as might be useful in affording a good point of departure. It should also be noted that there are at least two correct positions at which the sliding strip can be juxtaposed against the text, since in the enciphering rectangle the letters in one column form digraphs with the letters in the column not only on the right but also on the left. In the absence of any Q's, or other low-frequency letters suitable for a point of departure, the very first 20 or 25 letters of the cryptogram may be used as the starting point, since these letters come from column 1 of the transposition rectangle and therefore there is no uncertainty at least as to the letter which is at the top of that column; or, the last 20 or 25 letters of the cryptogram may be used as the starting point, since these letters come from the last-numbered column of the rectangle and therefore there is no uncertainty at least as to the letter which is at the bottom of that column.

c. Suppose that a good initial juxtaposition has been found for the portion of the text that has been written on the sliding strip, and that a series of excellent digraphs has been brought to light. The next step is, of course, to add to these digraphs on either side by finding sections of text that will yield "good" trigraphs and tetragraphs. For example, suppose that the initial juxtaposition has yielded what is shown in Fig. 14. The digraph PR suggests that it must be followed by a vowel, preferably E, A, or O; the digraph AV might be part of the word CAVALRY, in which case it will be followed by A; the digraph CR suggests that it might be followed by the vowel A or E. A place is therefore sought, in the rest of the text, where there is a sequence of the letters here desired, and, of course, at the proper intervals. Suppose such a sequence is found and yields what is shown in Fig. 15. The skeletons of words are now beginning to appear.

FIGURE 14.	FIGURE 15.
. .	. . .
. .	. . .
. .	. . .
R R	R R S
N A	N A T
P R	P R E
T O	T O R
A V	A V A
R E	R E D
T H	T H R
C H	C H U
C K	C K A
I L	I L L
T I	T I N
C R	C R A
B E	B E S
Z E	Z E R
E A	E A O
. .	. . .
. .	. . .
. .	. . .

Assuming that A V A is indeed part of the word CAVALRY, there should be an L to follow it; the trigraph T I N suggests the termination G; the trigraph Z E R suggests the word ZERO. A section of text is therefore sought, which will have the letters L, G, and O in the order L 1 2 3 4 5 6 G 1 2 O. Enough has been shown to demonstrate the procedure. In the course of the work it soon becomes evident where the ends of columns are, because the digraphs above and below the nuclear or "good" portion become "bad" quite suddenly, just as soon as letters belonging to non-adjacent columns in the original rectangle are brought together. For example, in Fig. 15 it is observed that the topmost trigraph R R S is highly improbable, and likewise the bottom-most trigraph E A O. This suggests that these letters have been brought together erroneously, that is, that they do not belong in adjacent columns in the enciphering rectangle. If this is true then the "good" portion is composed of the 13 letters between these two extremities and therefore the columns are about 13 letters long. Additional work will soon show exactly how long each column really is, and when this has been ascertained the problem has been practically completed, since at the same time that this becomes evident the sequence of columns has also become evident.

16. Example of solution by alternative method. - a. Using the cryptogram of Par. 14 as an example, Fig. 16 shows how the text might be transcribed on a sheet of cross-section paper. Noting that the message contains a Q as the 129th letter, a section of text to include the Q is transcribed on a strip of cross-section paper and this strip is then juxtaposed against the whole text so as to bring the Q in front of a U. How many letters should be included in this strip? The message contains 224 letters; if a width of say 10 to 20 columns is assumed, the columns of the rectangle will be about 12 to 22 letters in length. It will be safer to assume a convenient length closer to the maximum than to the minimum; consequently a length of 20 letters will be tentatively assumed. Now the Q may be at the top of a column, at the middle, or at the bottom--there is no way of telling at this point. Hence, to make sure that nothing is overlooked, suppose a section of 41 letters is taken, with the Q at the center. There are 4 U's in the message, and four trials are to be made. The results are as indicated in Fig. 17. Examining combination 1 in Fig. 17, the digraphs formed both above and below the QU are not at all bad. In fact, not one of those above the QU is impossible and the same is true of those below the QU until the digraph V N is reached. Hence, combination 1 is possible. As for combination 2, this at once appears to be bad. Trigraphs such as I I, and I H are highly improbable, and this combination may be discarded with safety. Combination 3 is possible from

	O	31	D	61	M	91	F	121	T	151	E	181	A	211	A
	D		S		S		M		N		A		E		L
	N		T		C		B		D		O		N		O
	N		E		L		I		A		O		E		D
5	P	35	O	65	C	95	E	125	H	155	T	185	E	215	I
	T		I		S		H		I		H		M		R
	I		T		O		B		R		E		Y		O
	R		D		E		V		H		A		T		R
	N		M		F		T		Q		C		F		Y
10	T	40	A	70	C	100	B	130	I	160	N	190	I	220	N
	D		N		F		E		E		S		T		N
	T		L		F		S		T		H		A		R
	U		N		T		R		E		E		N		G
	R		O		E		S		T		E		L		Y
15	O	45	E	75	E	105	Y	135	N	165	V	195	N		
	E		B		E		L		O		T		N		
	X		O		M		X		T		R		U		
	A		U		I		R		R		E		A		
	L		H		A		O		A		S		C		
20	N	50	E	80	I	110	R	140	A	170	R	200	L		
	I		N		T		U		V		A		R		
	E		L		E		M		R		I		E		
	T		E		A		E		I		I		N		
	G		S		I		T		R		E		R		
25	N	55	E	85	J	115	Y	145	S	175	A	205	T		
	W		A		N		O		T		T		R		
	T		A		S		I		G		E		A		
	T		C		O		K		S		E		T		
	M		T		I		N		E		A		S		
30	E	60	R	90	V	120	K	150	F	180	L	210	O		
	D		M		F		T		E		A		A		
	S		S		M		N		A		E		L		
	T		C		B		D		O		N		O		
	E		L		I		A		O		E		D		
35	O	65	C	95	E	125	H	155	T	185	E	215	I		
	I		S		H		I		H		M		R		
	T		O		B		R		E		Y		O		
	D		E		V		H		A		T		R		
	M		F		T		Q		C		F		Y		
40	A	70	C	100	B	130	I	160	N	190	I	220	N		

FIGURE 16.

1	2	3	4
O	OT-28	OF-91	OE-177
R	RM	RM	RE
U	UE-30	UB	UA
M	MD	MI	ML-180
E	ES	EE-95	EA
T	TT	TH	TE
Y	YE	YB	YN
O	OO-35	OV	OE
IC	II	IT	IE-185
KD	KT	KB-100	KM
NN	ND	NE	NY
KN	KM	KS	KT
TP-5	TA-40	TR	TF
NT	NN	NS	NI-190
DI	DL	DY-105	DT
AR	AN	AL	AA
HN	HO	HX	HN
IT-10	IE-45	IR	IL
RD	RB	RO	RN-195
HT	HO	HR-110	HN
QU	QU	QU	QU
IR	IH	IM	IA
EO-15	EE-50	EE	EC
TE	TN	TT	TL-200
EX	EL	EY-115	ER
TA	TE	TO	TE
NL	NS	NI	NN
ON-20	OE-55	OK	OR
TI	TA	TN	TT-205
RE	RA	RK-120	RR
AT	AC	AT	AA
AG	AT	AN	AT
VN-25	VR-60	VD	VS
RW	RM	RA	RO-210
IT	IS	IH-125	IA
RT	RC	RI	RL
SM	SL	SR	SO
TE-30	TC-65	TH	TD
GD	GS	GQ	GI-215
SS	SO	SI-130	SR
ET	EE	ET	EO
1	2	3	4

FIGURE 17.

the top digraph, O F, to the 12th digraph below the Q U, although the digraph H X looks very bad. However, the X might be a sentence separator, so that this combination cannot be discarded. Combination 4 looks very improbable, with the digraph H N occurring twice, and other equally bad digraphs showing. Of the four possibilities then, combinations 2 and 4 are discarded, leaving 1 and 3 for further study. It is very difficult to choose between these two possibilities. All the digraphs in combination 1 down to digraph V N are possible; many of them are excellent. As for combination 3, all the digraphs down to V D are also possible and many of them are excellent. There does not seem to be much use to add the frequency values of the digraphs in each combination because it is hard to know with what digraphs to begin or end. However, perhaps it is not essential that a choice be made at once; possibly further work along the lines now to be demonstrated will show which combination is correct. Noting the two K's (in the digraphs K B and K S) among the combinations before the Q, assume that these K's are parts of the digraph CK. Is there a sequence C-C in the text? There is but one such place, at the 63rd letter. Suppose the corresponding section is placed in front of the combinations 1 and 3 of Fig. 17, as shown in Fig. 18. It immediately becomes evident that combination 3 is the correct one, for note the excellent trigraphs it gives, as compared with those in combination 1. Also note that the second trigraph below the E Q U in combination 3 consists of three E's, indicating that the end of the columns has been reached just before this trigraph. As for the top trigraphs of Fig. 18, they are good all the way up. But now the skeletons of words are beginning to appear. The T H R immediately above the E Q U suggests either THREE or THROUGH; the F R O above the T H R suggests FROM or FRONT. Suppose the word REQUEST is assumed for the E Q U, and the word THREE is assumed for the T H R above it. This requires a section with two E's in succession.

	SOF
	ERM
	AUB
	AMI
	CEE
	TTH
	RYB
	MOV
SIO	SIT
CKD	CKB
LNN	LNE
CKN	CKS
STP	STR
ONT	ONS
EDI	EDY
FAR	FAL
CHN	CHX
FIT	FIR
FRD	FRO
THT	THR
EQU	EQU
EIR	EIM
EEO	EEE
MTE	MTT
IEX	IEY
ATA	ATO
INL	INI
TON	TOK
ETI	ETN
ARE	ARK
IAT	IAT
JAG	JAN
1	3

FIGURE 18.

SOFV
ERMT
AUBR
AMIE
CEES
TTHR
RYBA
MOVI
SITI
CKBE
LNEA
CKST
STRE
ONSE
EDYA
FALL
CHXA
FIRE
FRON
THRE
EQUE
EIMM
EEEY

FIGURE 19.

There are several such places in the text, and further limitation is advisable. The 8th trigraph from the top is certainly suggestive of the word MOVING, which requires an I to follow the V. Is there a place in the text where an I occurs 12 letters before a double E? There is one such place, and the corresponding section is juxtaposed at the proper place, yielding what is shown in Fig. 19. The upper and lower limits of the columns are now fairly definite and are marked by the horizontal bars; tetragraphs E E E Y at the bottom and A M I E at the top are very improbable. The tetragraph C E E S below the top bar is possible, because it may represent the end of a word like FORCE followed by the beginning of the word ESTIMATED; the tetragraph below the bottom bar suggests a word ending in E followed by the word IMMEDIATE. It seems hardly necessary to continue with the demonstration; in a few moments the entire diagram is reconstructed and yields the solution. During this process, as soon as a section of text in Fig. 16 has been used it is crossed off, so as to prevent its letters from being considered as further possibilities for addition to the reconstruction diagram. Thus, as the work progresses the number of available sections becomes progressively less, and the choice for successive sections for addition to the diagram becomes a quite easy matter.

b. When two or three operators are assigned to work upon a cryptogram by this method, solution can be reached in a very short space of time, especially if each one of the operators takes a different point of attack. After a few minutes the fragments of texts obtained may be assimilated into one message which is then completed very speedily.

SECTION IV.

OPPORTUNITIES AFFORDED BY STUDYING ERRORS AND BLUNDERS MADE BY ENEMY CRYPTOGRAPHERS.

17. Importance of the study of errors and blunders in early work upon an unknown system. - a. Blunders and mistakes made by cryptographic clerks in the execution of cryptographic instructions should be rare in a well-trained and well-disciplined cryptographic service. Nevertheless, blunders and mistakes are committed despite all that can be done to prevent their occurrence. Especially in the excitement prior to or during an important action or movement do such instances take place and these afford golden opportunities for the enemy cryptanalytic service. This situation exists in respect to all types of cryptographic systems and no cryptanalytic instruction would be complete if cognizance were not taken of the advantages which may be reaped from the blunders, the mistakes, and, occasionally, the downright ineptitude of the adversary's cryptographers.

b. Practically every cryptographic system affords opportunities for the commission of errors in its application, and each system more or less presents a separate case. That is, the errors which may be made in one type of cryptographic system may be peculiar to that type alone and to no other type; hence, the astute cryptanalyst is constantly on the lookout for instances of cryptograms containing the specific type of error by which that system is handicapped. Furthermore, the general types of blunders or errors that may be committed are nearly as numerous as are the general types of cryptographic systems, so that no complete list of such as may be encountered in practice can be drawn up.

c. After the cryptanalyst has by painstaking and more or less arduous labors solved a system and has become thoroughly familiar with its mechanics, he should carefully review the details of the mechanics to learn what things can go wrong, what sorts of mistakes the enemy cryptographic personnel are likely to make, and then study the external manifestations of these aberrations so that he may be able to recognize instances of their occurrence in subsequent cryptograms. This sort of study has no value in itself particularly; its importance lies in the fact that the effects of erroneous treatment may lead to very rapid solution or to quick recovery of keys of subsequent messages.

d. When an unknown system is under investigation and the cryptanalyst is striving to ascertain just how it operates (which is often the most difficult step in solution), a study of the cryptograms representing corrections to previous messages containing errors is a most fruitful source of data. Indeed, at times this sort of intensive study will yield clues for solving a system which might otherwise resist all efforts to break it down for a very long time.

18. Significance of terms special solution and general solution. - a. Now the importance of the comments made in the foregoing paragraph will be clear if it is noted that a study of the blunders and errors often leads to the elaboration of methods for the rapid breaking down of cryptographic systems. But it must also be realized that in some

cases no blunders or errors are essential to a rapid solution of the type alluded to above: sometimes the mechanics of the system are such that unavoidable or unpredictable circumstances arise, so that special solutions become possible. The latter term calls for a bit of explanation.

b. When the circumstances surrounding a specific cryptogram or set of cryptograms are such as to present peculiar or unusual conditions that make a solution possible when in the absence of these conditions solution is either impossible or improbable, the methods employed in reaching a solution in such cases constitute what is commonly termed a special solution. Some examples will be demonstrated very soon. Systems of which this may be true are, of course, cryptographically weak but it may be observed that it is perhaps impossible to devise a system which may be considered to be absolutely free from this source of weakness.

c. The advantages of a special solution for any type of cryptographic system are, as a rule, two in number. First, it often makes a solution possible when otherwise this might not be the case. Secondly, it often affords a method of achieving a very rapid solution in the case of a problem which otherwise might require a long time. But a special solution presents one basic disadvantage: it is by its very nature dependent upon the existence of unusual circumstances, in other words, upon chance or good fortune bringing about a set of circumstances favorable for a solution. When these unusual conditions or circumstances do not obtain, then solution may be impossible. Therefore, it is desirable to have, if possible, for every type of system a more or less general solution which may be applied in the absence of the unusual conditions necessary for the application of a special solution. In other words, a general solution in cryptanalysis implies a method or procedure which if applied in ordinary cases and under normal conditions will yield the solution. However, the term general solution in cryptanalysis must not be taken too literally. The situation in cryptanalysis is not exactly analogous to that which obtains in the field of pure mathematics, for the circumstances are often quite different in the two sciences. A general solution in mathematics is expected to and will solve every case that falls within its province; a general solution in cryptanalysis is intended to solve every case that falls within its province but this is more of a hope than an expectation. Much depends upon the amount of traffic available for study, the length of individual cryptograms, and the indefinable element called "luck", that is, a set of fortuitous circumstances which happen to make a solution easy or difficult, such as the presence of many or exceptionally long repetitions, etc. Furthermore, whereas in mathematics a general solution prescribes the exact steps to be followed in arriving at the solution; the latter can be applied in all instances without variation or deviation from a fixed procedure, in cryptanalysis a general solution merely outlines a broad path that may be followed in order to arrive at a solution; application of the latter in specific instances may involve minor detours to circumvent unexpected obstacles, or it may involve quite large changes or modifications in the general procedure.

19. Examples to be studied. - a. As stated above in Paragraph 17, a complete list of the specific blunders that cryptographic clerks are prone to perpetrate cannot be drawn up. Certain of them may be described in general terms and examples given of some which have already been encountered in this and in preceding texts. Commonly it is the case that these blunders do not become evident until two or more cryptograms are available for comparison. One of the most frequent sources of circumstances leading to the transmission of cryptograms affording rich material for cryptanalytic comparison is the following: A cryptographic clerk prepares a cryptogram, in the course of which he makes a mistake of such a nature as to render the cryptogram difficult or impossible to decipher by the cryptographic clerk serving the addressee. A request for repetition ensues, whereupon the enciphering clerk reexamines his original work and finds that he has made a mistake. He then commits the grave blunder of reenciphering the identical message (without paraphrasing) and transmitting what to the enemy cryptanalysts is obviously a second version of the original message. The consequences are often fatal to cryptographic security. The least that can happen is that the key for this particular message may be disclosed very quickly; more serious, the basic or primary elements for the entire day's traffic may be wrested from the blunder; but most serious are the consequences if it happens that the blunder has been committed immediately or soon after a new cryptographic system has been instituted and the enemy cryptanalysts are exerting strenuous efforts to learn its mechanics, for then is when the information to be gained is most valuable.

b. In the next few paragraphs some specific examples of the consequences of cryptographic blunders and ineptitude in the case of transposition systems will be studied. These are intended to give the student some idea of the far-reaching effects such studies may have. It is important that he grasp the fundamental principles for they will enable him to develop for himself the methods that he may find necessary in practical work. Incidentally, it may be added that the student should not get the idea that these instances are purely theoretical. It is sometimes almost unbelievable that cryptographic clerks with any common sense would perpetrate the stupid blunders that they do occasionally commit.

SECTION V

SPECIAL SOLUTIONS FOR TRANSPOSITION CIPHERS

20. Solution when the beginning or end of the plain text is known. - a. It often happens, when correspondents have fallen into the bad habit of sending stereotyped communications, that the beginnings or the ends of messages become so fixed in their form and content that the enemy can with a fair degree of certainty guess what these will be in specific cases. If so, a quick solution can be reached and the key reconstructed for one message, and this will of course enable him to read all other messages in the same key. This is particularly true of simple keyed columnar transposition ciphers. It is only necessary that the cryptanalyst cut the text up in such a manner as to bring the letters composing the assumed text all within the same row or rows of the transposition rectangle.

b. Suppose that the enemy is addicted to the introductory expression REFERRING TO YOUR NUMBER. Here is a cryptogram assumed to begin with this phrase:

CRYPTOGRAM

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

c. Assuming that previous experience has indicated that the enemy uses keys varying from 10 to 20 letters in length, the arrangement of the letters in the tops of columns under a key length of 10 would be as shown in Fig. 20.

1	2	3	4	5	6	7	8	9	10
R	E	F	E	R	R	I	N	G	T
O	Y	O	U	R	N	U	M	B	E
R									

FIGURE 20.

The 1st group of the cryptogram begins with I M. The arrangement shown above gives I U as the top of a column: hence a key length of 10 is not correct. A key length of 11 is then tried.

1	2	3	4	5	6	7	8	9	10	11
R	E	F	E	R	R	I	N	G	T	O
Y	O	U	R	N	U	M	B	E	R	

FIGURE 21.

Here a column is headed by I M, so that this is a possible arrangement. If the width of the rectangle is 11, its outlines are as shown in Fig. 22. There are 5 columns of 11 letters and 6 columns of 10 letters. The

R	E	F	E	R	R	I	N	G	T	O
Y	O	U	R	N	U	M	B	E	R	

FIGURE 22.

text can now be marked off into sections of proper lengths and, moreover, guided by the letters which must be at the heads of columns, the text can be inscribed in the rectangle in key order. For example, column 1 must end with the 2d group, R M G R N; column 2 therefore begins with E R. There is only one possibility, viz, the 4th column. This is a long column, and must therefore have 11 letters, making column 3 begin with R Y. This definitely fixes the position of the number 3 in the key, and so on. The solution is reached after only a very few moments and is as shown in Fig. 23.

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

FIGURE 23.

d. The same general principles, modified to suit the circumstances, may be followed in the case involving known or suspected endings of messages. The probable words are written out according to various assumed key lengths and the superimposed letters falling at the bottoms of columns are sought in the cryptogram.

21. The case of an omitted column. - a. Sometimes a very careless clerk omits a column in transcribing the text from the enciphering rectangle and fails to check the number of letters in the final cryptogram. Obviously such a cryptogram will be difficult if not impossible to decipher at the other end, and a repetition is requested and sent. If now the identical plain text is enciphered correctly, two cryptograms are at hand for comparison. This will disclose the length of one column, which can be assumed to be either a long one or a short one.

The position, in the correct cryptogram, of the column omitted from the incorrect one will often afford direct clues as to the exact dimensions of the enciphering rectangle. For example, suppose the cryptogram in Par. 20b had first been transmitted as follows:

CRYPTOGRAM

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

b. The column which was omitted is E R N I N T U S F S D, and falls between columns 1 and 3. Since the omitted column contains 11 letters and column 1 contains 10, the dimensions of the rectangle immediately become known. Thus, uncertainties as to the dimensions of the rectangle are dissolved and a large step in the solution taken. Also, the general positions of columns 1 and 2 are now known, since the former is a short one, the latter a long one.

22. The case of an interchanged pair of columns. - a. The keying element in the case of columnar transposition is simply a practical means of controlling the order in which the columns of the enciphering rectangle are transcribed in forming the cipher text. Commonly this numerical key is derived from a literal key. Suppose that a cryptographic clerk makes a mistake in the latter step. For example, suppose that the literal key is ADMIRATION and that as a result of a slight relaxation in attention he assigns the number 5 to the letter N and the number 6 to the letter M. A pair of columns will become interchanged as regards their order of selection in the transcription process, and likely as not a repetition will be requested by the addressee. If a

second version is sent, enciphered by the correct key, a comparison of the two versions will disclose the width of the enciphering rectangle and possibly the general position (left or right) of the columns that were interchanged.

b. An example will serve to make the matter clear. Assume the two cryptograms to be as follows:

FIRST VERSION

```
ODNIL  NTTHD  GSOHA  OOQSG  TERPS
INENE  NFUEH  RWRRI  RATPE  DETAN
OOCOO  ROGIO  S
```

SECOND VERSION

```
ODNIL  NTTHD  GSOHA  OOQSG  TERNF
UEHRW  RPSIN  ENERI  RATPE  DETAN
OOCOO  ROGIO  S
```

c. The two cryptograms are superimposed as shown in Fig. 24 and their points of similarity and difference noted.

```
1st version .. O D N I L N T T H D G S O H A O O Q S G T E R[P S I N E N E]
2nd version .. O D N I L N T T H D G S O H A O O Q S G T E R[N F U E H R W.

1st version ..[N F U E H R W R]R I R A T P E D E T A N O O C O O R O G I O S
2nd version .. R]P S I N E N E]R I R A T P E D E T A N O O C O O R O G I O S
```

FIGURE 24.

d. The two versions are alike except for a pair of interchanged sequences; the bracketed sequence P S I N E N E in the 1st version is matched by the same sequence in the 2d version, but at a different position in the message; likewise the bracketed sequence N F U E H R W R in the 1st version is matched by a similar sequence in the 2d version, but at a different position in the message. The various deductions which can be made from the situation will now be set forth.

e. One of these sequences contains 7 letters, the other contains 8. It follows that the columns of the enciphering rectangle are probably 7 and 8 letters in length; hence, with 61 letters, the width of rectangle is 8. Since there are 23 letters from the beginning of the messages to the first point of their difference, it follows that there are 2 columns of 8 letters and 1 column of 7 letters involved in this section [(2 x 8) + (1 x 7) = 23], and that the error made in encipherment does not involve columns 1, 2, or 3, which are therefore properly placed in the 1st version. Since the sequences which are interchanged are consecutive in the text it means that the numbers 4 and 5 were interchanged in the key for the 1st version. Since one of these sequences is of 7 letters, the other of 8 letters, one of the numbers, 4 or 5, applies to a long column, the other, to a short column. Since the 2d version is presumably the correct version, and since in the 2d version the 8-letter sequence comes first, the key number 4 applies to a long column, the key number 5, to a short column in the correct version. With the foregoing deductions in mind, the solution and the reconstruction of the numerical key becomes a simple matter.

f. The text of the correct version is written out as seen in Fig. 25a. Seeing a Q in column 3 and a U in column 4, these two columns are made adjacent by sliding column 3 one interval downward, as shown in Fig. 25b. In the latter, column 7 has also been placed to the right of column 5, because it yields good trigraphs with columns 3-4. Seeing the trigraph T R O near the bottom of columns 3-4-5 and the letters O and P in the same row, suggests the word TROOP. The columns are to be rearranged to make this word TROOP. There are two columns which have

```
1 2 3 4 5 6 7 8    1 2 3 4 5 6 7 8    3 4 5 2 6    3 4 7 2 6 8 1 5
    a         c                  c    O N E T R    O N E T R O O P
  t o       d o              d   o    O F T H I    O F T H I R D S
O H O N P R E O    O T A N E R P O    Q U A D R    Q U A D R O N I
D D Q F S I T R    D H O F T I S R    S E N G A    S E N G A G I N
N G S U I R A O    N D Q U A R I O    G H O S T    G H O S T I L E
I S G E N A N G    I G S E N A N G    T R O O P    T R O O P O N N
L O T H E T O I    L S G H O T E I    E W C H E    E W C H E S T E
N H E R N P O O    N O T R O P N O    R R O   D    R R O A D
T A R W E E C S    T H E W C E E S
T O   R   D O      T   R R O D

       a                  b                c              d
```

FIGURE 25.

an O in the proper row, columns 2 and 8. The trial of combination 3-4-5-8-6, while producing TROOP in the proper row, gives bad pentagraphs in the other rows; but the combination 3-4-5-2-6 shows excellent pentagraphs, as will be seen in Fig. 25c. The words SQUADRON and HOSTILE are clearly evident; the completion of the rectangle is now a very simple matter. The result is shown in Fig. 25d. The recovery of the numerical key now will enable other cryptograms to be read directly.

23. Messages with similar beginnings. - a. In military correspondence it is often the case that somewhat similar instructions or information must be conveyed by a superior commander to several subordinate commanders simultaneously. Such a situation frequently results in the circumstance that two or more cryptograms addressed to different stations will begin with exactly the same words. When simple columnar transposition is the system used for encipherment, then it will result, in such cases as the foregoing, that the first two or more rows of the transposition rectangle will be identical in the messages which begin alike. Therefore, the cryptograms will show identical sequences of two or more letters, distributed throughout the texts and

by studying these identities the cryptanalyst is able at once not only to ascertain the width of the rectangle but also to divide up the cipher text into sections corresponding with the exact columns of the rectangle, thus eliminating the only real difficulty in solution, viz, the determination of which are the long columns, which the short. An example will demonstrate the short cut to solution which such a situation provides.

b. Here are two cryptograms which are assumed to have been intercepted within a few minutes of each other, the messages being addressed to two battalion commanders by the regimental commander.

CRYPTOGRAM 1

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

CRYPTOGRAM 2

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

c. The cryptanalyst now carefully compares the two texts, looking for identical sequences of letters between the cryptograms. For example, No. 1 begins with B N T S E and so does No. 2; after an interval of 4 letters in No. 1 and 5 letters in No. 2 he notes the identical sequences L C E T; after an interval of 5 letters in No. 1 and 5 letters in No. 2 he notes the identical sequences E R R O, and so on. The identities are underlined or marked in some distinctive manner throughout the texts, as shown in Fig. 26.

CRYPTOGRAM 1

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

CRYPTOGRAM 2

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

FIGURE 26.

d. Now it is obvious that these identities exist because the two messages begin alike, and by taking advantage of the identical portions in the cryptograms it will be possible to transcribe the texts of the latter into transposition rectangles which shall not only have the identical portions in homologous positions, but also shall show which are long columns, which are short. All that is necessary is to begin transcribing the texts on cross-section paper, in columns, arranging matters so that the identical sequences will fall at the tops of the columns. Thus, the 1st column of No. 1 will contain the letters B N T S E A R K C and the 1st column of No. 2 will contain the letters B N T S E I N D O T; the 2d column of No. 1 will contain the letters L C E T T N B I T and the 2d column of No. 2 will contain the letters L C E T S A F P L, and so on. It appears that the identical portion embraces the first four rows of the rectangle and runs over a number of letters on the 5th row. This is because the identical sequences consist of 4 and 5 letters. Fig. 27a shows the identities between the 1st 5 columns of the two transposition rectangles. Only once in the case of this particular example does any uncertainty arise as to exactly where an identical sequence begins or ends, and that is in connection with the 7th pair of identities, involving the series of letters A E F T F S N P G N P in No. 1, and A E F T F S T O N T N in No. 2. These sequences contain 6 identical letters, but even here the uncertainty is of only a moment's duration: the initial letter A does not belong to the identical portions at the top of the transposition rectangle because the A's are needed to complete columns 6 in both rectangles. (If the A were placed at the head of column 7 in No. 1, then column 6 would lack a letter at the bottom.) Cases of "accidental identities" of course complicate the process of cutting up the text into the respective columns, but they only serve to add a small degree of interest to what would otherwise be a purely cut and dried process. The final results of the transcription into columns are shown in Fig. 27b.

1

B	L	E	N	T
N	C	R	N	O
T	E	R	O	K
S	T	O	N	M
E	T	T	N	S
A	N	A	E	Z
R	B	E	N	T
K	I	L	O	G
C	T	T	O	N

2

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

FIGURE 27a.

e. It is clear from a comparison of these two transposition rectangles, and a consideration of the fact that the long columns must of necessity go to the left side, that the numbers 7 and 10 occupy the first two positions in the key, and that the numbers 2, 4, 11, and 13 occupy the last four positions in the key. By segregating and anagramming

1

1	2	3	4	5	6	7	8	9	10	11	12	13	14
B	L	E	N	T	Y	E	A	T	N	I	M	O	A
N	C	R	N	O	I	F	R	F	O	O	M	U	G
T	E	R	O	K	T	T	W	C	E	S	A	T	A
S	T	O	N	M	D	F	O	T	W	T	O	I	A
E	T	T	N	S	K	S	I	O	X	I	A	O	P
A	N	A	E	Z	L	N	A	T	E	D	R	B	N
R	B	E	N	T	A	P	O	D	R	R	P	I	E
K	I	L	O	G	N	G	F	N	F	R	A	E	I
C	T	T	O	N	A	N	G	I	A	R	T	O	K
						P			S				

2

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

FIGURE 27b.

1.

7-10		2-11-13-4
E N	....	L I O N
F O	....	C O U N
T E	....	E S T O
F W	....	T T I N
S X	....	T I O N
N E	....	N D B E
P R	....	B R I N
G F	....	I R E O
N A	....	T R O O
P S	....	

2.

7-10		2-11-13-4
E N	....	L I O N
F O	....	C O U N
T E	....	E S T O
F W	....	T T I N
S X	....	S T E S
T P	....	A T E T
O V	....	F F L I
N T	....	P O S I
T I	....	L C O U
N T		

FIGURE 27c.

columns 7 and 10 as one group, and columns 2, 4, 11, and 13 as another group, the exact positions occupied by these 6 columns are easily ascertained, as shown in Fig. 27c.

f. The remaining columns 1, 3, 5, 6, 8, 9, 10, 12, and 14 form a third group of columns to be anagrammed, but this is rather easy now that the columns on either side are fixed. The completed rectangles are shown in Fig. 27d.

24. Messages with similar endings. - a. What has been said at the beginning at the preceding paragraph with respect to the nature of military correspondence and the presence of identical phraseology in

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

FIGURE 27d.

the messages sent by a superior commander to his subordinates also operates to produce messages in which the endings are identical. It has been noted that when two messages with similar beginnings are available for comparison, the reconstruction of the transposition rectangles and the recovery of the transposition key is an easy matter. It will now be shown that solution is an even easier matter when two messages having identical endings are available for study.

b. Given the following two cryptograms:

No. 1.

```
ETRTE EESOA AEUNI VAFLN IAMND RYHRV MENRI
EETRO UDCCC OHTCY MRREA RHITN DEYEN RNERV
SRBEN IGSKA ILNRA NFNAD ALOLT XOMAH HRREI
```

No. 2.

```
TLVSX OPNRE MEFDS KYENR UEERB TSREH TIANT
IVYMR VESIR EENEI NOLTM NNEDE TROOP UNARA
CIAAI NSCWN A
```

The cryptanalyst now carefully compares the two texts, searching for identical sequences of letters, but in this case instead of trying to locate identities in what may be termed a parallel progression (as in the preceding case) he searches for identical sequences of two or more letters appearing in both messages. For example, in the present case, he notes the sequence T R O forming the final trigraph of the 8th group of No. 1 and finds a similar sequence forming the initial trigraph of the 13th group of No. 2. Going through both cryptograms in this way, all the identities are marked off in some fashion, by colored crayon or by brackets, as shown below. In this search for identities the cryptanalyst bears in mind that when all have been found they should be distributed at quite regular intervals throughout the text. For example, note in the following that the identities in No. 1 fall at intervals of 6 letters, with one exception; in No. 2 they fall at intervals of 4 letters, with one exception. The intervals between identities serve as a guide in finding them. After they have all been located, the identities in the cryptograms are numbered serially.

No. 1

```
             1                2             3                    4
E T R T E  E[E S]O A  A E U N[I  V]A F L N  I A[M N]D  R Y H R V [M E]N R I

    5              6                 7              8
E E[T R O] U D C C C  O[H T]C Y  M R R E[A  R]H I T N  D E[Y E N] R N E R V

  9              10             11             12            13
S[R B]E N  I G S K[A  I]L N R A  N F[N A]D  A L O L T [X O]M A H  H R R[E I]
```

No. 2

```
         1               2             3             4              5
T L V S[X  O]P N R E [M E]F D S  K[Y E N]R  U E E[R B] T S R E[H  T]I A N T

 6          7            8             9          10            11
[I V]Y M R  V[E S]I R  E E N[E I] N O L T[M  N]N E D E [T R O]O P  U N[A R]A

      12           13
C I A[A I]  N S C W[N  A]
```

c. The numbers above the identities may now be used to draw up a table of equivalencies of identities. For instance, identity 1 in cryptogram 1 matches identity 7 in cryptogram 2; identity 2 in cryptogram 1 matches identity 6 in cryptogram 2, and so on. Thus:

Cryptogram 1 ... 1-2-3-4--5-6--7-8-9-10-11-12-13
Cryptogram 2 ... 7-6-9-2-10-5-11-3-4-12-13--1--8

d. Now cryptogram 1 has 105 letters, since the key consists of 13 numbers (indicated by the 13 identities), the rectangle for cryptogram 1 contains 12 columns of 8 letters and 1 column of 9 letters. Cryptogram 2 has 81 letters, and its rectangle contains 10 columns of 6 letters and 3 columns of 7 letters. The rectangle of cryptogram 1 has but 1 long column, whereas that of cryptogram 2 has 3 long columns. Relative to the position the last letter in each rectangle occupies in the last row of the rectangle, it is obvious that the last letter of the rectangle for cryptogram 2 is 2 letters in advance of the last letter of the rectangle for cryptogram 1. Using this difference, viz, 2, a cyclic sequence is generated from the series of equivalencies given above. Thus, the equivalent of identity 1 of cryptogram 1 is identity 7 of cryptogram 2, and the number 7 is placed two intervals to the right of the number 1; the equivalent of identity 7 of cryptogram 1 is identity 11 of cryptogram 2, and the number 11 is placed two intervals to the right of number 7, and so on until the following sequence is obtained:

1-2-3-4-5-6-7-8-9-10-11-12-13
1- 7- 11- 13- 8- 3- 9

e. The equivalent of identity 9 of cryptogram 1 is identity 4 of cryptogram 2, and the number 4 is placed between the numbers 1 and 7 in this sequence, for the sequence may be regarded as partaking of the nature of a cycle or a continuous series. From this point on, the process is the same as before, and finally the following is obtained:

1--2--3--4---5--6---7--8--9--10--11--12--13
1--4--7--2--11--6--13--5--8--10---3--12---9

f. After little experiment it becomes obvious that column 8 belongs on the extreme left and that the key is 8-10-3-12-9-1-4-7-2-11-6-13-5. The completely deciphered messages are shown in Fig. 28.

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

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

FIGURE 28.

g. The possibility of the rapid solution of columnar transposition ciphers by means of the method of similar beginnings and endings, constitutes one of the most serious drawbacks to the use of transposition ciphers in military cryptography, because it is almost impossible to avoid such cases where many messages must be sent in the same key each day.

25. Solution of a single message containing a long repetition. - a. Sometimes a lengthy phrase or a series of numbers (spelled out in letters) is repeated within a message and if the message is enciphered by a transposition rectangle of such narrow width (in comparison with the length of the repetition) that the repeated portion forms identical

sequences within the text of the cryptogram, a solution somewhat similar in principle to that explained in Par. 24 may be achieved within a few minutes.

b. Note the following cryptogram, in which identical portions have been underlined.

CRYPTOGRAM (169 letters)

```
O E A E L  T R S E D  H N U F F  R N R Y F  N T A E D  I L S M Y
                  1a              1b                        2a

N C E T S  L S T O C  A W I A O  T S L S S  L E D H N  O R I I S
       2b                          3a          3b

F E B N N  U U P W E  S S M Y E  R C N N O  R V T T A  O G N U G  G T I F E
            4a          4b                        5a              5b

R S E O M  S W E R N  R A S T B  O S A A A  O S N O O  I B O S D
                 6a          6b                          7a

C A Y H L  H O N E M  S E T F Y  H L A U X  T A O G G  P R S V L
     7b                         8a          8b

Y E E G G  T I S S O  U U P V
       9a               9b
```

c. There are 18 segments of underlined letters, which means in this case that the rectangle is 9 columns wide, because the repeated portion in the text will give rise to two repeated sequences in each column. This means that the rectangle has 7 columns of 19 letters and 2 columns of 18 letters. The first two segments may therefore be assigned the numbers 1a and 1b, since they come from column 1; the next two segments may be assigned the numbers 2a and 2b, since they come from column 2, and so on, as shown above. A table of equivalencies may now be drawn up, showing the segments which are identical. Thus:

1a-2a-3a-4a-5a-6a-7a-8a-9a
3b-4b-2b-9b-8b-1b-6b-7b-5b

This gives rise to the cycle 1-3-2-4-9-5-8-7-6, which is a cyclic permutation of the actual transposition key.

d. By transcribing the text into a rectangle of proper width, "cutting" the columns so as to bring the identical portions within the same rows, the result shown in Fig. 29 is obtained.

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

FIGURE 29.

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

FIGURE 30.

e. Study of Fig. 29 shows that columns 2 and 7 are the short columns and belong on the right, either in the sequence 2-7 or 7-2. The cyclic permutation of the transposition key obtained in subparagraph c is

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

In order to bring the 2 and 7 adjacent in a sequence 2-7 or 7-2 one must take intervals of 5 and 4, respectively, and "decimate" the cycle, giving the following:

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

Since columns 2 and 7 belong on the right, the key must be:

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

Only a few moments are necessary to establish the correctness of the former alternative and the solution is at hand. It is as shown in Fig. 30.

26. Solution when several cryptograms of identical length and in the same key are available. - a. Although the method to be described in

this paragraph is included within the category of special solutions, it is of such general applicability that it might well be treated as a general solution for all transposition systems. It is based upon the very mechanics of transposition as a cryptographic scheme, viz, that the essential feature of the transposition method consists merely in the alterations in the positions of the elements (letters, groups of letters, or words) composing the plain text according to a specific key. It follows, therefore, that the respective elements of two or more messages of identical lengths, when transposed according to the same key, will undergo identical alterations in position in the course of encipherment, and therefore all plain-text elements occupying homologous positions in the original messages will emerge in homologous positions in the cryptograms. The situation is very much like that which may be observed in the movements executed by two symmetrical groups of dancers in a chorus. Suppose each group consists of 8 dancers starting originally in definite positions relative to one another. When a movement is executed each dancer in each group performs certain evolutions; at the conclusion of the movement the 8 dancers in each group may be in quite different positions relative to one another than they were at the beginning of the movement, but the correspondingly numbered dancers in both groups find themselves in identical positions relative to their neighbors. Of course, the fact that in this analogy the groups are based upon 8's is of no significance; if the groups consisted of many more the principle would still apply. Another way of looking at the matter is to call attention to the fact that in any type of transposition the position which a specified letter or element of the plain text will occupy in the final cryptogram is quite definitely a function of the number of letters or elements in the plain text itself. For example, suppose that a plain-text message contains exactly 100 letters, and suppose that the transposition system and specific key is such that the 1st plain-text letter appears as the 17th cipher-text letter, the 2d plain-text letter, as the 68th, and so on; in another message of exactly 100 letters, enciphered by the same general system and specific key, it is obvious that the 1st plain-text letter must also appear as the 17th cipher-text letter, the 2d plain-text letter, as the 68th, and so on. In short, all correspondingly numbered plain-text letters in both messages will appear in identical positions in the cryptograms.

b. Granting the obvious truth of the foregoing, to what use can it be put in the solution of transposition ciphers? Simply this: it enables the cryptanalyst to reconstruct the plain texts of cryptograms of identical length without even knowing what the transposition key or system was that produced them. The process is not at all complicated and if there are several messages the process is very easy. It consists in superimposing the several cryptograms and anagramming the columns formed by the superimposition, for it is obvious that any circumstances which can be used as a guide for rearranging the letters in one of the lines of superimposed text in order to form plain text will require and can be checked by the results of an identical rearrangement of the corresponding letters of the other lines of superimposed text.

c. An example of the method involving the application of the principles of solution will now be given, using as a basis five messages assumed to have been enciphered by an unknown but complex type of transposition. It will now be shown how the security of such a system is demolished when it is used by a large number of intercommunicating commands.

d. Let the following be five cryptograms isolated from among many messages intercepted on the same day and therefore suspected of being in the same key. These five cryptograms have been isolated because they all contain exactly the same number of letters. They are here shown superimposed (Fig. 31) and therefore all the letters in one column have undergone exactly the same evolutions or changes in position in the course of encipherment.

FIGURE 31.

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

26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
E	I	H	I	S	A	T	F	T	D	N	R	L	V	O	R	O	D	S	W	E	E	R	O	R	Q
A	I	E	U	T	T	A	R	D	T	E	D	N	S	O	E	I	P	E	C	M	F	E	A	R	N
E	I	S	I	G	A	O	R	W	L	L	D	L	V	V	O	R	D	E	L	O	C	H	O	T	H
W	I	A	A	R	N	O	I	H	N	L	L	N	R	F	V	W	L	R	E	M	R	A	I	E	A
N	N	A	I	B	T	N	H	I	T	N	I	A	S	D	R	M	S	E	C	U	I	O	V	S	A

e. Noting a Q in Message 1 column 51, the obligatory sequence Q U is assumed to be present in that message. There is in Message 1 but one U, which is fortunate. Combining columns 51 and 23, the results are found to be fair. (Fig. 32a). The H T in the 3d row suggests a word ending in G H T, such as FIGHT, MIGHT, EIGHT, etc. Searching in Message 3 for a G, two candidates are found: columns 10 and 30. The trigraphs yielded by each combination are shown in Fig. 32b. The second of the two possibilities looks much the better. The trigraph in the first row

51-23	10-51-23	30-51-23
Q U	G Q U	S Q U
N O	N N O	T N O
H T	G H T	G H T
A I	F A I	R A I
A T	O A T	B A T

FIGURE 32a. FIGURE 32b.

suggests the word SQUARE or SQUADRON; that in the last row suggests BATTLE or BATTALION. This means that a column with an A at the top and a T at the bottom should be sought. There is only one such column, 31. Adding it to the 30-51-23 combination gives what is shown in Fig. 32c. Looking for a column with a D at the top (for SQUAD) and either an A (for BATTALION) or an L (for BATTLE), there is only one candidate, column 22, yielding the sequences shown in Fig. 32d. Enough has been shown of the procedure to make further demonstration unnecessary.

30-51-23-31			
S	Q	U	A
T	N	O	T
G	H	T	A
R	A	I	N
B	A	T	T

FIGURE 32c.

30-51-23-31-22				
S	Q	U	A	D
T	N	O	T	C
G	H	T	A	X
R	A	I	N	F
B	A	T	T	A

FIGURE 32d.

Once a good start has been made, progress is quite rapid, unless the cryptanalyst is unfortunate and arrives at a point where all the messages simultaneously terminate in complete words, without a clue as to what follows or precedes in any one of the messages. In such a contingency the only thing he can do is to try all sorts of possible continuations, either "fore" or "aft", that is, in front of the original starting point or after it, until he picks up another word which will enable him to continue. Or he may have to search for a new point of entry and build upon that, later joining this structure with the other. In the case under examination no particular difficulties are experienced and the entire five messages are reconstructed. In the course of this reconstruction the numbers applicable to the columns become assembled in proper order. This sequence of numbers is shown in Fig. 33, as the second row of numbers. In the first row are shown the numbers 1, 2, 3, ..., corresponding to the order of the letters in the plain text.

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
28	3	14	46	19	37	25	47	48	26	35	41	2	34	27	12	36	45	17	13	40	18	9	24	33
H	A	V	E	O	R	D	E	R	E	D	R	A	T	I	O	N	W	A	G	O	N	S	O	F
E	N	E	M	Y	D	E	F	E	A	T	E	D	D	I	R	E	C	T	I	O	N	O	F	R
S	E	C	O	N	D	E	C	H	E	L	O	N	W	I	L	L	E	A	V	E	H	E	R	
A	N	I	M	A	L	D	R	A	W	N	V	E	H	I	C	L	E	S	O	F	E	N	G	I
A	M	M	U	N	I	T	I	O	N	T	R	A	I	N	I	N	C	L	U	D	I	N	G	H

26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
8	1	50	44	11	30	51	23	31	22	16	7	21	32	42	10	49	4	43	15	5	39	29	20	38	6
F	I	R	S	T	S	Q	U	A	D	R	O	N	T	O	G	O	L	D	E	N	V	I	L	L	E
E	T	R	E	A	T	N	O	T	C	E	R	T	A	I	N	A	M	P	U	R	S	U	I	N	G
E	A	T	E	I	G	H	T	A	X	M	X	F	O	R	G	O	L	D	E	N	V	I	L	L	E
N	E	E	R	T	R	A	I	N	F	O	L	L	O	W	F	I	E	L	D	T	R	A	I	N	S
O	R	S	E	D	B	A	T	T	A	L	I	O	N	M	O	V	E	S	A	T	S	I	X	A	M

FIGURE 33.

27. Recovery of the transposition key. - a. Having reconstructed the plain text of the messages in the foregoing case, can the transposition key be found? First, it is necessary to ascertain whether a single columnar transposition had been used and if not, then the assumption will be that a double transposition[1] had been used.

b. If a single transposition were the case, then there would be a rather simple relationship between the letters which are in adjacent columns in the rectangle. Note what happens in a simple transposition

---

[1] See Special Text No. 166, Advanced Military Cryptography, Sect. IV.

rectangle such as that shown in Fig. 34, where the successive cells are numbered and these numbers, taken out of columns just as though letters were present in the cells, then are set down as though they constituted the cryptogram. The numbers then give the order in which the plain-text letters, if present, would appear in the cryptogram. Order in which the plain-text letters would appear in cryptogram: 04-12-20-28-36-44-02-10-18-26-34-42-06-14-22-etc. Note the constant difference between sequent numbers: 04-12 = 8; 20 - 12 = 8; 28 - 20 = 8; etc. The only exceptions to this constant difference of 8 occur when there is a break occasioned by passing from the bottom of one column to the top of the next one, as, for example, the skip from 44 to 02. This constant difference (with occasional exceptions) is an obvious consequence of the fact that the width of the transposition rectangle is 8 and simple columnar transposition has been employed.

6	2	7	1	5	3	8	4
01	02	03	04	05	06	07	08
09	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44				

FIGURE 34.

c. In order to ascertain, in the case of the 5 messages, solved in Par. 26, whether single columnar transposition was employed, it is necessary first to obtain the series of numbers which give the order in which the plain-text letters appear in the cryptogram. This is now easy in the case of the 5 messages solved in Par. 26, for the disarranged numerical sequence at the top of Fig. 33 gives the inverse of the sequence desired. There the numbers in mixed sequence merely give the order of the cipher letters in the cryptogram. Hence, by developing the inverse of this sequence, the order in which the plain-text letters appear in the cryptogram may be obtained. The disarranged numerical sequence in Fig. 33 is 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
28	3	14	46	19	37	25	47	48	26	35	41	2	34	27	12	36	45	17	13	40	18	9	24	33

26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
8	1	50	44	11	30	51	23	31	22	16	7	21	32	42	10	49	4	43	15	5	39	29	20	38	6

FIGURE 35.

The inverse derived from this sequence is as follows:

27	13	2	43	46	51	37	26	23	41	30	16	20	3	45	36	19	22	5	49	38	35	33	24	7
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

10	15	1	48	31	34	39	25	14	11	17	6	50	47	21	12	40	44	29	18	4	8	9	42	28	32
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51

FIGURE 36.

Such a sequence will hereinafter be termed the basic transposition sequence, or simply the basic sequence. It merely is a sequence of numbers giving the order in which the plain-text letters appear in the final cryptogram.

d. Since there is seen to be no constant difference between successive numbers in the basic sequence in Fig. 36, single columnar transposition is ruled out. Double transposition is now assumed to have been used.

e. Referring back to Fig. 34, suppose true double transposition has been effected. Now note the order in which the plain-text letters would appear in the cryptogram.

6	2	7	1	5	3	8	4
01	02	03	04	05	06	07	08
09	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44				

Rectangle D-1

A

6	2	7	1	5	3	8	4
04	12	20	28	36	44	02	10
18	26	34	42	06	14	22	30
38	08	16	24	32	40	05	13
21	29	37	01	09	17	25	33
41	03	11	19	27	35	43	07
15	23	31	39				

Rectangle D-2

B

Basic sequence: 28-42-24-01-19-39-12-26-08-29-03-23-44-14-40-17-35-10-30-13-33-07-36-06-32-09-27-04-18-38-21-41-15-20-34-16-37-11-31-02-22-05-25-43

FIGURE 37.

Nothing in the nature of a series of constant differences between successive numbers is now discernible in the basic sequence. But there is, as can readily be seen, a fairly constant relationship between sections of this sequence. For example, take the series of numbers 04-18-38-21-41-15 appearing in the latter half of the sequence and set them under the series of numbers 12-26-08-29-03-23 appearing in the first half of the sequence and find the difference between superimposed numbers only when the number in the upper line is greater than that in the lower line. Thus:

12-26-08-29-03-23
04-18-38-21-41-15

Differences: 8 8   8   8

There is a constant difference between superimposed numbers. The reason for the constant difference is not hard to see if one studies the rectangle at B in Fig. 37. It is caused by the mechanics of the method. The 04 and the 12 come from the same column in A of Fig. 37; the 18 and the 26 also come from one column, the 21 and the 29, the 15 and the 23. But the 08 and the 38 are in different columns in A of

Fig. 37, and so are the 03 and the 41. These two cases therefore represent instances where there is a passage from one column to another in the transposition process. Now the constant difference is in this case 8 because the superimposed numbers happen to be sequent in the columns in which they occur in A, Fig. 37. If two other sections of numbers are compared the constant difference may not be 8 but will be a multiple of that number. For example:

```
               28-42-24-01-19-39
               04-18-38-21-41-15
Differences:   24 24          24
```

Here the difference is a multiple of 24 because the superimposed numbers are at 3 intervals from each other in the respective columns of A, Fig. 37.

f. The foregoing affords a method of ascertaining the width of the transposition rectangle, which is the first step in recovering the key. For if a study is made of the numbers appearing in the basic sequence shown in Fig. 36, based upon finding sections which show a constant difference, the latter will correspond to either the width of the rectangle or a multiple of the width. An easy way of making this study is to take a section of the mixed sequence in Fig. 36 and add 5, 6, 7, ... to the numbers of the sequence for the totals thus obtained from the various additions. A beginning will be made with an assumption of a rectangle of 5 columns. Since the cryptograms contain only 51 letters, all totals beyond 51 will be of no significance. Hence it is best to take a section which has a long series of low numbers so that when the additive is applied the majority of the totals will not exceed 51. Such a series is the following (only one number in it is close to the maximum):

Section of)
basic sequence)... 38-35-33-24--7-10-15-1-48-31-34-39-25-14-11-17--6

Totals after)
adding 5) ... 43-40-38-29-12-15-20-6----36-39-44-30-19-16-22-11

Searching through the basic sequence for a section which has a part of the sequence of numbers in the totals after the additive of 5 has been applied, the results are negative. Trial is then made of additives of 6 to 11, inclusive, with similar negative results. When an additive of 12 is applied the results are as follows:

Section of)
basic sequence) ... 38-25-33-24--7-10-15--1-48-31-34-39-25-14-11-17--6

Totals after)
adding 12) ... 50-47-45-36-19-22-27-13----43-46-51-37-26-23-29-18

It will be seen, on referring to Fig. 36, that the following sections are duplicated in the basic sequence:

50-47; 45-36-19-22; 27-13-2-43-46-51-37-26-23; 29-18

The width of the transposition rectangle is certainly 12 columns. There are therefore 3 long columns of 5 letters and 9 short columns of 4 letters in the transposition rectangles D_1 and D_2.

g. Having ascertained the width, the next step is to ascertain the transposition key. Let the additive 12 be applied to the entire basic sequence, as shown in Fig. 38a:

A. Basic sequence	27 13 02 43 46 51 37 26 23 41 30 16 20
B. Plus additive	39 25 14 55 58 63 49 38 35 53 42 28 32
A. Basic sequence	03 45 36 19 22 05 49 38 35 33 24 07 10
B. Plus additive	15 57 48 31 34 17 61 50 47 45 36 19 22
A. Basic sequence	15 01 48 31 34 39 25 14 11 17 06 50 47
B. Plus additive	27 13 60 43 46 51 37 26 23 29 18 62 59
A. Basic sequence	21 12 40 44 29 18 04 08 09 42 28 32
B. Plus additive	33 24 52 56 41 30 16 20 21 54 40 44

FIGURE 38a.

A study is now made to isolate and identify duplicate sections in lines A and B. For example, in line A the sequence 27-13-02-43-46-51-37-26-23 is, except for one number, identical with a sequence in line B. The number 02 in line A is replaced by the number 60 in line B. Since the number 60 in line B is greater than 51, the total number of letters in the cryptogram, it is clear that it represents the 02 in line A. Now these duplicate sections consist of 9 numbers, and it is clear that two columns of the transposition rectangle are involved, one long column of 5 and one short column of 4 numbers. The dividing point may be between the numbers 43 and 46, or between 46 and 51. No decision will be made at the moment as to which of these possibilities will be selected. But the whole section will be marked off by brackets and the small numbers 1 and 2 will/written along the brackets, as shown in Fig. 38b:

			1				2						
A. Basic sequence	27	13	02	43	46	51	37	26	23	41	30	16	20
B. Plus additive	39	25	14	55	58	63	49	38	35	53	42	28	32
A. Basic sequence	03	45	36	19	22	05	49	38	35	33	24	07	10
B. Plus additive	15	57	48	31	34	17	61	50	47	45	36	19	22
A. Basic sequence	15	01	48	31	34	39	25	14	11	17	06	50	47
B. Plus additive	27	13	60	43	46	51	37	26	23	29	18	62	59
A. Basic sequence	21	12	40	44	29	18	04	08	09	42	28	32	
B. Plus additive	33	24	52	56	41	30	16	20	21	54	40	44	

FIGURE 38b.

The next section in line A which has a duplicate in line B is 41-30-16-20. The two duplicate sections are bracketed and the process is continued in this manner and the successive sections are numbered successively in both lines until what is shown in Fig. 38c is obtained:

	1	2	3
A. Basic sequence	27 13 02 43 46	51 37 26 23	41 30 16 20
B. Plus additive	39 25 14 55 58	63 49 38 35	53 42 28 32

	4	5	6
A. Basic sequence	03 45 36 19 22	05 49 38 35	33 24 07 10
B. Plus additive	15 57 48 31 34	17 61 50 47	45 36 19 22

	7	8	9
A. Basic sequence	15 01 48 31 34	39 25 14 11	17 06 50 47
B. Plus additive	27 13 60 43 46	51 37 26 23	29 18 62 59

	10	11	12
A. Basic sequence	21 12 40 44	29 18 04 08	09 42 28 32
B. Plus additive	33 24 52 56	41 30 16 20	21 54 40 44

FIGURE 38c.

Now a table of equivalencies between the duplicate sections in lines A and B is drawn up, as follows:

A	1	2	3	4	5	6	7	8	9	10	11	12
B	8	5	12	7	9	4	1	2	11	6	3	10

Deriving a chain of equivalents (as in Par. 24), the following is obtained:

1-8-2-5-9-11-3-12-10-6-4-7

This is a cyclic permutation of the transposition key. Since Sections 1, 4, and 7 of line A have 5 numbers, the other sections only 4, it follows that these correspond to long columns, which, of course, go to the left of the rectangle. Hence the transposition key is 4-7-1-8-2-5-9-11-3-12-10-6. This key may be proved by applying it to one of the cryptograms and deciphering it.

28. Special cases of solution of double transposition ciphers. - a. When the double transposition system is employed in the field and is used for a voluminous traffic it is almost inevitable that certain situations will arise which make possible a rather easy solution. Aside from the case in which several cryptograms of identical length and in the same key are intercepted, other cases of a special nature may arise. Some of these will be discussed in this paragraph.

b. First, there is the case in which an inexperienced cryptographic clerk fails to execute the double transposition properly and causes the transmission of a cryptogram which is only a single transposition. The solution of this message will be a simple matter and will, of course, yield the key which will permit the reading of all other messages even though the latter have been correctly cryptographed. The only difficult part of the matter is to find among a large number of intercepted cryptograms one which involves a blunder of this sort. When the cryptanalyst has, as a result of considerable experience, become adept in the solution of transposition ciphers the work of testing cryptograms to ascertain whether or not they involve single columnar transposition is not difficult and goes quite rapidly. For only a few minutes are sufficient to give him the "feeling" that the cryptogram is or is not solvable by single transposition. He might not be able to point out any specific indications which give him this feeling if asked to do so; nevertheless it must be recognized that his intuition is alone sufficient to tell him when there is hope of solution along this line and when further work upon the hypothesis of single transposition is useless.

c. (1) Next comes the case in which the enciphering rectangle of a double transposition cryptogram happens to be a perfect square (that is, both D_1 and D_2 rectangles are perfect squares). In this case, not only is such a cryptogram detectable at once, since the total number of letters is the square of the number of elements in the key, but also the cryptogram can be solved in a very simple manner. For the cryptogram now represents a case in which a completely filled rectangle has been employed, and moreover there is no need even to assume various widths.

(2) Given the following cryptogram of 49 letters (7 x 7) as an example, the text is transcribed as shown in Fig. 39a and retranscribed as in Fig. 39b.

CRYPTOGRAM

UCTRN OESHI ETOLR GASOE DUWDD
NOEOE RDNDI RFENC OEEEM NNVE

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

FIGURE 39a.

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

FIGURE 39b.

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

FIGURE 39c.

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

FIGURE 39d.

(3) The columns of Fig. 39b are now anagrammed, as in Fig. 39c, and the rows rearranged, as in Fig. 39d.

d. When the enciphering rectangle is not a perfect square but nevertheless a complete rectangle, solution of a single cryptogram becomes somewhat more difficult. Here the columns are all equal in length, since the last row of the rectangle is completely filled. Two cases will be considered; first, when the width of the rectangle is a multiple of the depth, or number of letters in the columns, and second, when the depth is a multiple of the width.

e. (1) Taking up the first case, note the encipherment in Fig. 40.

6	2	10	1	7	4	9	8	3	5
W	H	E	N	W	I	L	L	F	I
1	2	3	4	5	6	7	8	9	10
R	S	T	S	Q	U	A	D	R	O
11	12	13	14	15	16	17	18	19	20
N	R	E	A	C	H	G	O	L	D
21	22	23	24	25	26	27	28	29	30
E	N	V	I	L	L	E	T	O	N
31	32	33	34	35	36	37	38	39	40
I	G	H	T	A	D	V	I	S	E
41	42	43	44	45	46	47	48	47	50

D-1

6	2	10	1	7	4	9	8	3	5
N	S	A	I	T	H	S	R	N	G
4	14	24	34	44	2	12	22	32	42
F	R	L	O	S	I	U	H	L	D
9	19	29	39	49	6	16	26	36	46
I	O	D	N	E	W	R	N	E	I
10	20	30	40	50	1	11	21	31	41
W	Q	C	L	A	L	D	O	T	I
5	15	25	35	45	8	18	28	38	48
L	A	G	E	V	E	T	E	V	H
7	17	27	37	47	3	13	23	33	43

D-2

Basic sequence 34 39 40 35 37 14 19 20 15 17 32 36 31 38 33 2 6 1 8 3 42 46 41 48 43

Cryptogram I O N L E S R O Q A N L E T V H I W L E G D I I H

4 9 10 5 7 44 49 50 45 47 22 26 21 28 23 12 16 11 18 13 24 29 30 25 27

N F I W L T S E A V R H N O E S U R D T A L D C G

FIGURE 40.

If the numbers above the letters in the cryptogram are examined it will be found that the cipher groups fall into two categories, as follows:

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

(2) There is obviously a definite regularity in the composition of the cipher groups whereby if the letters in any one group can be assembled properly, all the letters in the other groups belonging to the same category (A or B) will be assembled correctly too. For example, in category B the 3d, 1st, and 5th letters in each group are sequent; in the plain-text rectangle in category A the 1st and 4th letters in each group are sequent.

Moreover, all the letters in each group come from the same row in the D_1 rectangle. Consequently, if two groups coming from the same row can be identified, there will be 10 letters which may be rearranged by experiment to form plain text, and the key for this rearrangement will apply to all other pairs of groups. For example, the message in this case has a Q and only one U. The Q is in the 2d group, the U is in the 9th group. These two groups come from the same row and the letters may be anagrammed:

```
1 2 3 4 5   and   6 7 8 9 10
S R O Q A   and   S U R D T

2 1   6         8
8 6 10 1 4 7 5 9 2 3
R S T  S Q U A D R O
```

Experiment may now be made with two other groups, applying the same transposition. Thus:

```
1 2 3 4 5   and   6 7 8 9 10
I O N L E   and   N L E T V

2 1   6         8
8 6 10 1 4 7 5 9 2 3
O I    N        E
E N V  I L L E T O N
```

Obviously the proper key for rearrangement is 8-6-10-1-4-7-5-9-2-3. By continuing this procedure the following additional rows of the D_1 rectangle are reconstructed.

1 2 3 4 5		6 7 8 9 10
N F I W L	and	H I W L E
8-6-10-1-4		7-5-9-2-3
W H E N W		I L L F I

1 2 3 4 5		6 7 8 9 10
T S E A V	and	G D I I H
8-6-10-1-4		7-5-9-2-3
I G H T A		D V I S E

1 2 3 4 5		6 7 8 9 10
A L D C G	and	R H N O E
8-6-10-1-4		7-5-9-2-3
N R E A C		H G O L D

The various rows are now assembled in sequence, giving the following:

```
W H E N W I L L F I
R S T S Q U A D R O
N R E A C H G O L D
E N V I L L E T C N
I G H T A D V I S E
```

The key can now be reconstructed with ease.

(3) The cryptanalyst in this case must, of course, make an assumption as to the width of the enciphering rectangle before he can apply the method. With a number such as 50, the dimensions 10 x 5 or 5 x 10 suggest themselves. The process of finding cipher groups which form pairs on the same row is one of "cut and try." If there is a single Q and a single U in the message, the initial pair of groups is obvious.

f. When the depth of the rectangle is a multiple of the width, solution follows the lines of the preceding case. Taking the same message as before, note what happens in encipherment with a rectangle of 5 columns containing 10 letters each:

2	5	1	4	3
1 W	2 H	3 E	4 N	5 W
6 I	7 L	8 L	9 F	10 I
11 R	12 S	13 T	14 S	15 Q
16 U	17 A	18 D	19 R	20 O
21 N	22 R	23 E	24 A	25 C
26 H	27 G	28 O	29 L	30 D
31 E	32 N	33 V	34 T	35 L
36 L	37 E	38 T	39 O	40 N
41 I	42 G	43 H	44 T	45 A
46 D	47 V	48 I	49 S	50 E

2	5	1	4	3
3 E	8 L	13 T	18 D	23 E
28 O	33 V	38 T	43 H	48 I
1 W	6 I	11 R	16 U	21 N
26 H	31 E	36 L	41 I	46 D
5 W	10 I	15 Q	20 O	25 C
30 D	35 L	40 N	45 A	50 E
4 N	9 F	14 S	19 R	24 A
29 L	34 I	39 O	44 T	49 S
2 H	7 L	12 S	17 A	22 R
27 G	32 N	37 E	42 G	47 V

13 38 11 36 15   40 14 39 12 37   3 28 1 26 5   30 4 29 2 27   23 48 21 46 25   50 24 49 22 47

T T R L Q   N S O S E   E O W H W   D N L H G   E I N D C   E A S R V

18 43 16 41 20   45 19 44 17 42   8 33 6 31 10   35 9 34 7 32

D H U I O   A R T A G   L V I E I   L F I L N

FIGURE 41.

Taking the numbers above the letters and arranging them in sections of 10, the results are as follows:

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

It is obvious that if the 3d, 9th, 1st, 7th, and 5th columns are made sequent, good text will be produced within the 5 rows. Thus:

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

$\longrightarrow$

3	9	1	7	5
R	S	T	S	Q
W	H	E	N	W
N	R	E	A	C
U	A	D	R	O
I	L	L	F	I

FIGURE 42.

The subsequent steps are obvious. Here again in solving an unknown example it would be necessary to test out various assumptions with respect to the dimensions of the rectangle before attempting to apply the method outlined.

g. Whenever this simple relationship between the width and depth of the rectangle obtains, that is, when one dimension is a multiple of the other, solution of a single cryptogram is relatively easy. The reason for this is not hard to see. When the enciphering rectangle is a perfect square, every column of the D_2 rectangle is composed of letters which all come from the same row of the D_1 rectangle. Hence solution is in this case the same as though a false double transposition were in effect, with merely the columns and the rows of a single rectangle shifted about. When the width of the transposition rectangle is twice the depth, a column of the D_2 rectangle contains half the letters appearing on one row of the D_1 rectangle; two columns therefore contain all the letters belonging in the same row of the D_1 rectangle. If the width were three times the depth, then three columns of the D_2 rectangle would contain all the letters belonging in the same row of the D_1 rectangle, and so on. When the width is half the depth, a column of the D_2 rectangle contains all the letters appearing in two rows of the D_1 rectangle; when the width is one-third the depth, a column of the D_2 rectangle contains all the letters appearing in three rows of the D_1 rectangle, and so on. But when this multiple relationship no longer obtains, solution becomes more difficult because each column of the D_2 rectangle is composed of letters coming from several columns of the D_1 rectangle, in an irregular distribution. Solution is, of course, most difficult when incompletely-filled rectangles are used. However, although solvable, even in the case of a single message, the solution will not be dealt with in this text.

29. Concluding remarks on transposition systems. - a. Pure transposition, that is, transposition by itself, without an accompanying substitution or other means of disguise for the letters of the plain text, hardly affords sufficient guarantees for cryptographic security in the case of a voluminous correspondence which must be kept really secret for any length of time. For no matter how complex the method, or how many transpositions may be applied to the letters of a single message, sight must never be lost of the fact that when there are many messages in the same key there are bound to be two or more of identical length; and when this is the case the type of solution described in Par. 26 may be applied to these cryptograms, the transposition keys recovered, and then all other messages in the same key translated.

b. Transposition methods are, from the cryptographic point of view, rather highly regarded because they are, as "hand methods" go, rather rapid in operation and usually quite simple. However, from their very nature they entail the disadvantage that a single-letter omission or addition may render their decryptographing difficult if not impossible for the average cryptographic clerk. But from the standpoint of modern cryptography the principal disadvantage of transposition methods is that they can be mechanized only with great difficulty--certainly with greater difficulty than is the case of substitution methods. Only one or two attempts have been made to produce machinery for effecting transposition, and these have not been successful.

SECTION VI

MISCELLANEOUS TRANSPOSITION CIPHERS

Paragraph

30. Special designs or geometric figures. - It is impossible here to elucidate and demonstrate by example all the methods which may be used for the solution of cryptograms produced by the many various types of transposition designs or geometric figures other than the rectangular ones thus far treated. Reference may be made to such designs as triangles, trapezoids, and polygons of various symmetrical shapes. Most of these designs, however, are impractical for military correspondence in any case, so that no attention need be given them in this text. If such designs were used, although it might be difficult to solve a single or even a few messages in the same key, the general solution later to be described is applicable whenever two or more messages of identical lengths but in the same key are available for study. Since most of these designs are of a fixed or inflexible character with regard to the number of letters that can be accommodated with one application of the design to the plain text to be enciphered, the production of several cryptograms of identical length in the same key is by no means an unusual circumstance. There are, however, one or two methods which do warrant discussion in this text, the most important being those which use grilles of the revolving,[1] or continuous types.

[1] See Special Text No. 166, Advanced Military Cryptography, Sec. V.

31. Revolving grilles. - a. In this type of grille apertures are distributed among the cells of a square sheet of cross-section paper in such a manner that when the grille is placed upon a grid (a sheet of cross-section paper of the same size as the grille) and turned three times successively through angles of 90° from an initial position upon the grid, all the grid cells (or all but the central grid cell) are disclosed in turn. Correspondents must, of course, possess identical grilles and they must have an understanding as to its initial position and direction of rotation, clockwise or counterclockwise. There are two procedures possible in using such a grille. (1) The letters of the plain text may be inscribed successively in the grid cells through the apertures disclosed by the grille; when the grid has been completely filled the grille is removed and the letters transcribed from the grid according to a prearranged route. (2) All the letters of the plain text may first be inscribed in the grid cells according to a prearranged route and then the grille applied to the completely-filled grid to give the sequence of letters forming the cryptogram. The two methods of using the grille are reciprocal; if the first described method is used to encipher a message, the second method is used to decipher the cryptogram, and vice versa. The first of the two above-described methods, the one in which the plain text is inscribed through the apertures, will here be referred to as the alpha method; the second method will be referred to as the beta method.

b. The number of letters in a cryptogram enciphered by such a device is either a perfect square, when the grille has an even number of cells per side, or is 1 less than a perfect square, when the grille has an odd number of cells per side, in which case the central cell of the grid is not disclosed and hence remains unfilled.[2]

c. The manner of construction and the method of use of a grille entails certain consequences which can be employed to solve the cryptograms and to reconstruct the grille itself. The student who wishes to get a thorough grasp of the underlying principles to be explained will do well to prepare a grille[3] and study the properties which characterize cryptograms produced by its use. Three principles will be brought to bear in the solution of grille ciphers of this type and they will be demonstrated by reference to the grille and message shown in Fig. 43.

d. The first principle may be termed that of symmetry. When a revolving grille is in position 1 a certain number of cells of the underlying grid are disclosed (uncovered). For each such disclosed cell of the grid there is a symmetrically corresponding cell on the same grid which is disclosed when the grille is turned to positions 2, 3, and 4, because the apertures of the grille remain fixed--only their positions change as the grille is turned in the process of encipherment. Now two successive apertures in position 1 will of course be occupied by a

---

[2]Of course, the cryptogram may consist of the letters produced by several applications of the same grille. For example, if a message of

REF ID:A56913

YOUR LINES TO THIS COMMAND POST CUT BY SHELL FIRE REQUEST YOU CHANGE THE ROUTE

GRILLE: 8 x 8

A

		1	2	3	4	5	6	7	8	
	a									b
1		1	2	3		5	6	7		
2		7		2	3	4		1	2	
3		6	5	1	2	3		2	3	
4		5		3		1	2	3	4	
5		4	3	2	1	1	3	4		
6			2	1			1	5		
7			1	5	4			1	7	
8		1		6	5	4	3	2	1	
	d									c

B

Position 1 (a, b, c, d)

1	2	3	Y 4	5	6	7	O 8
9	U 10	11	12	13	R 14	15	16
17	18	19	20	21	L 22	23	24
25	I 26	27	N 28	29	30	31	32
33	34	35	36	37	38	39	E 40
S 41	42	43	T 44	O 45	46	47	T 48
H 49	50	51	52	I 53	S 54	55	56
57	C 58	59	60	61	62	63	64

C

Position 2

1	O 2	M 3	4	5	6	7	8
M 9	10	11	12	A 13	14	N 15	16
17	18	19	20	21	22	23	24
25	26	D 27	28	P 29	30	31	O 32
33	S 34	T 35	36	37	38	39	40
41	C 42	43	44	45	U 46	T 47	48
49	50	51	52	53	54	55	56
57	58	B 59	Y 60	61	62	63	S 64

D

Position 3

1	2	3	4	5	6	H 7	8
9	10	E 11	L 12	13	14	15	L 16
F 17	18	19	I 20	R 21	22	23	E 24
R 25	26	27	28	29	30	31	32
33	34	35	36	E 37	38	Q 39	40
41	42	U 43	44	45	46	47	48
49	50	E 51	52	53	54	S 55	56
T 57	58	59	60	Y 61	62	63	64

E

Position 4

O 1	2	3	4	U 5	C 6	7	8
9	10	11	12	13	14	15	16
17	H 18	A 19	20	21	22	N 23	24
25	26	27	28	29	G 30	E 31	32
T 33	34	35	H 36	37	E 38	39	40
41	42	43	44	45	46	47	48
49	R 50	51	O 52	53	54	55	U 56
57	58	59	60	61	T 62	E 63	64

F

Final Grid

O 1	O 2	M 3	Y 4	U 5	C 6	H 7	O 8
M 9	U 10	E 11	L 12	A 13	R 14	N 15	L 16
F 17	H 18	A 19	I 20	R 21	L 22	N 23	E 24
R 25	I 26	D 27	N 28	P 29	G 30	E 31	O 32
T 33	S 34	T 35	H 36	E 37	E 38	Q 39	E 40
S 41	C 42	U 43	T 44	O 45	U 46	T 47	T 48
H 49	R 50	E 51	O 52	I 53	S 54	S 55	U 56
T 57	C 58	B 59	Y 60	Y 61	T 62	E 63	S 64

CRYPTOGRAM

plain-text digraph (alpha method of encipherment). When the grille reaches position 3, after a turn of 180°, the two apertures concerned will disclose two cells which will also be occupied by a plain-text digraph, but the letters composing the digraph will be in reverse order in the plain text. This property is true also of two successive apertures in position 2 when they turn up in position 4. Let the student verify this by means of the grille which he has constructed. Thus, referring to Fig. 43, at A is shown the grille in position 1. In the first row are shown 2 apertures, at coordinates 1-4 and 1-8. At B are shown the results of the first application of the grille to the grid. Note the letters YO (first 2 letters of message) in cells 4 and 8. Now note that the symmetrically corresponding cells disclosed when the grille is in position 3 are cells 57 and 61 and these correspond to cells 4 and 8 in the reverse order. The letter T in cell 57 therefore symmetrically corresponds with letter O in cell 8; the letter Y in cell 61 corresponds with letter Y in cell 4. The same is true of all other letters in positions 1 and 3. As a consequence of this property of grilles, a single cryptogram can be handled as though it were really two cryptograms of identical length, having certain characteristics by means of which an assumption made in one text may be verified by what it yields in the other text. That is, when the cryptogram is transcribed as a series of letters in one line and the same text is written in another line under these letters but in reversed order, then the superimposed letters will bear the symmetrical relationship pointed out in this paragraph. If two letters in the upper line of such a transcription are taken to form a digraph, the two corresponding letters in the lower line must form a digraph but in reversed order in the plain text. For example, if the cryptogram of Fig. 43 is written out as explained above, the result is as shown at Fig. 44. Now the presence of the Q in position

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
O	O	M	Y	U	C	H	O	M	U	E	L	A	R	N	L	F	H	A	I	R	L	N	E	R	I	D	N	P	G	E	O
S	E	T	Y	Y	B	C	T	U	S	S	I	O	E	R	H	T	T	U	O	T	U	C	S	E	Q	E	E	H	T	S	T
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
T	S	T	H	E	E	Q	E	S	C	U	T	O	U	T	T	H	R	E	O	I	S	S	U	T	C	B	Y	Y	T	E	S
O	E	G	P	N	D	I	R	E	N	L	R	I	A	H	F	L	N	R	A	L	E	U	M	O	H	C	U	Y	M	O	O

FIGURE 44.

39 suggests that it be combined with a U. If the U in position 43 is taken then the symmetrical digraph corresponding to QU would be LI; if the U in position 56 is taken, the symmetrically corresponding digraph would be MI. Furthermore, two apertures which are in the same column and which do not have an intervening aperture between them, will yield a good digraph in all 4 positions of the grille. For example, note apertures 2-6 and 3-6 in Fig. 43-A. When the grille is turned to positions 2, 3, and 4 they will disclose two sequent letters in each case. An analysis of the symmetries produced by an 8 x 8 grille yields the following table, which shows what cells are disclosed in the other 3 positions when an aperture is cut in any one cell in one of the four positions of the grille. For example, an aperture cut in cell 11 (position 1) will disclose grid cell 23 when the grille takes position 2, grid cell 54 when the grille takes position 3, and grid cell 42 when the grille takes position 4.

Positions:	1 3	2 4	1 3	2 4	1 3	2 4	1 3	2 4
	1	8	5	25	11	23	19	22
	64	57	60	40	54	42	46	43
	2	16	6	17	12	31	20	30
	63	49	59	48	53	34	45	35
	3	24	7	9	13	26	21	27
	62	41	58	56	52	39	44	38
	4	32	10	15	14	18	28	29
	61	33	55	50	51	47	37	36

FIGURE 45.

e. The second principle may be termed that of exclusion. On account of the system upon which the construction of a revolving grille is based, a knowledge of the location of an aperture in one of the bands brings with it a knowledge of 3 other locations in which there can be no apertures. For example, referring to Fig. 43-A, the presence of the aperture at coordinates 1-4 precludes the presence of apertures at coordinates 4-8, 8-5, and 5-1. By virtue of this principle of exclusion, the number of possibilities for choice of letters in solving a cryptogram prepared by means of a revolving grille becomes much reduced and the problem is correspondingly simplified; as will be seen presently.

f. The third principle may be termed that of sequence. When trying to build up text, the letters which follow a given sequence of plain-text letters will usually be found to the right and below, that is, if the normal method of writing was used (left to right and from the top downward). For example, referring to Fig. 44, if the trigraph Q U E is to be built up, neither the U in position 5 nor that in position 10 is very likely to be the one that follows the Q; the U in position 43 is the most likely candidate because it is the first one beyond the Q. Suppose the U in position 43 is selected. Then the E for Q U E cannot be the one in position 40, or in any position in front of 40, since the E must be beyond the U in the diagram.

g. In solving a grille, it will be found advisable to prepare a piece of cross-section paper of proper size for the grille and to cut each aperture as soon as its position becomes quite definite. In this way not only will the problem be simplified but also when completed the proper grille is at hand.

32. Solution of example. - a. Suppose the cryptogram at Fig. 43-G is to be solved. It has 64 letters, suggesting a grille 8 x 8. The cryptogram is first transcribed into a square 8 x 8, yielding what has already been obtained as Fig. 43-F. The Q in position 39 suggests that it is part of a word inscribed when the grille was in position 3, since there will be 16 plain-text letters inscribed at each position of the grille. Then a piece of cross-section paper is prepared for making the grille as shown in Fig. 45-A, and an aperture is cut in the proper position to disclose, in position 3, cell 39. It will be found that this is the aperture located at coordinates 4-2 of the grille shown in Fig. 45-A. At the same time the other 3 cells numbered 4 in the 2d band of the grille are marked so that they cannot become apertures. The result is shown in Fig. 45-B. Conforming to the principle of sequence, the U to be combined with the Q is sought to the right of the Q in Fig. 43-F. There are three candidates, in positions 43, 46 and 56. They yield:

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

FIGURE 45-A.

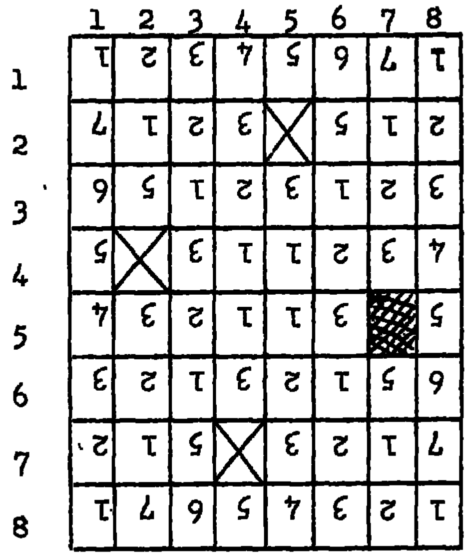


FIGURE 45-B.

(Grille in position 3)

39	43	39	46	39	56
Q	U	Q	U	Q	U
I	L	I	A	I	M

$(= L\ I_p)$ $(= A\ I_p)$ $(= M\ I_p)$

All of the symmetrical correspondents of these 3 QU's are good digraphs and it is impossible to eliminate any of the three alternatives. The U in position 43 would place an aperture at coordinates 6-3 in Fig. 45-B; the U in position 46 would place an aperture at coordinates 6-6; and the U in position 56 would place an aperture at coordinates 7-8. All of these are possible, none being excluded by principle 2. Suppose the Q U is followed by E. There are only two possibilities: an E in cell 51 and an E in cell 63. The following possibilities are presented:

39	43	51	39	43	63	39	46	51	39	46	63	39	56	63
Q	U	E	Q	U	E	Q	U	E	Q	U	E	Q	U	E
I	L	R	I	L	O	I	A	R	I	A	O	I	M	O

(= R L I) (= O L I) (= R A I) (= O A I) (= O M I)

None of the symmetrical correspondents of the Q U E's are impossible sequences in plain text, although O A I is not as probable as the others. (The O could be the end of a word, the AI the beginning of the word AID, AIM, AIR, etc.) Each of these possibilities would be tested by principle 2 to see if any conflicts would arise as to the positions of apertures. As in all cases of transposition ciphers, the most difficult part of the solution is that of forcing an entering wedge into the structure and getting a good start; when this has been done the rest is easy. Note what the results are when the proper apertures are assumed for QUEST in this case, as shown in Fig. 45-C. In position 1 this yields OUR LI ...; in position 2 it yields two digraphs AN and UT; in position 4 it yields two digraphs HA and RO. The student should note that the

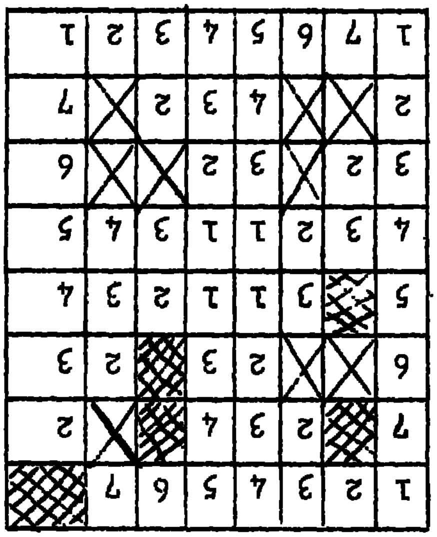


FIGURE 45-C.
(Grille in position 3)

indicated digraphs AN and RO in positions 2 and 4, respectively, are certain despite the fact that there is a space between the two apertures disclosing these letters, for the principle of exclusion has permitted the crossing off of this cell as a possibility for an aperture.

b. Enough has been shown of the procedure to make further demonstration unnecessary. Given the sequence OUR LI one begins to build on that, assuming a word such as LINE. This yields possibilities for the placement of additional apertures in the grille; these are tested in positions 2, 3, 4, and so on. When any 16 consecutive letters of plain text have been established all apertures have been ascertained and the problem has been completed. Subsequent cryptograms prepared by the same grille can be read at once.

c. If attempts at solution on the basis of the alpha method of using a grille have failed, the obvious modifications in procedure on the basis of the beta method can readily be made.

33. Concluding remarks on the solution of revolving grilles. - a. There is nothing about the mechanics of revolving grilles which prevents their employment in enciphering complete words instead of individual letters. However, the assembling of whole words in intelligible sequences and thus the reconstruction of the original plain text is a much easier matter than assembling single letters to form the words of the original plain text.

b. In case the same grille has been employed several times with separate grids to encipher a message that is considerably longer than a single grid will accommodate (see footnote 2, Par. 31b), the several sections each representing the set of letters enciphered on one grid may be superimposed and the general solution described in Paragraph 28 may then be applied.

c. In case the capacity of a grille is in excess of the number required by the length of the text to be enciphered, either of two procedures may be agreed upon. The grid cells which would otherwise be unoccupied may be filled by nulls, or the grid may be left incomplete. As regards the former procedure, little more need be said than that the presence of a few nulls will only delay solution a bit until the fact that nulls are being employed for this purpose becomes established. But the second type of procedure calls for more comment. If the grid is to be left incomplete it is necessary, before applying the grille, to count the number of plain-text letters and to cancel from the grid a number of cells equal to the number of cells in excess over the total number required. The position of the cells to be cancelled must be agreed upon; commonly they are those at the end of the grid. Such cells are marked so that when they become exposed during the rotations of the grille they will not be used. Thus, for example, the grille shown in Fig. 43-A is intended for a grid of 64 letters; if the message to be enciphered contains only 53 letters, 12 cells of the grid must be cancelled, and by agreement they may be cells 53 to 64, inclusive. The solution of a single cryptogram of this sort, or even of several of them of different lengths, may become a rather difficult matter. First of all, clues as to the dimensions of the grille are no longer afforded by the total number of letters in the cryptogram, so that this information can be obtained only by more or less laborious experimentation. Grilles of various dimensions must be assumed, one after the other, until the correct dimensions have been found. In the second place, the symmetrical relationships pointed out in Paragraph 31 no longer obtain, so that a single cryptogram cannot be handled as though it were constituted of two messages of identical length. Of course, in trying out any assumed dimensions, the 64 letters of the cryptogram may be written out in two superimposed lines, blanks being left for those positions which are unfilled. The procedure then follows the normal lines. About the most hopeful clues would be obtained from a knowledge of the circumstances surrounding the transmission and affording a basis for the assumption of probable words. However, were such a system employed for regular communication there would undoubtedly be cases of cryptograms of identical lengths, so that the type of solution given in Paragraph 28 will be applicable. Once a solution of this sort has been obtained, the dimensions of the grille may be ascertained. Subsequent cryptograms may then be attacked on the basis of the normal procedure, with such modifications as are indicated by the absence of the number of letters needed to make a completely-filled grid.

34. 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 Fig. 46. This grille contains 20 columns of cells and each column contains 5 apertures distributed at random in the column.

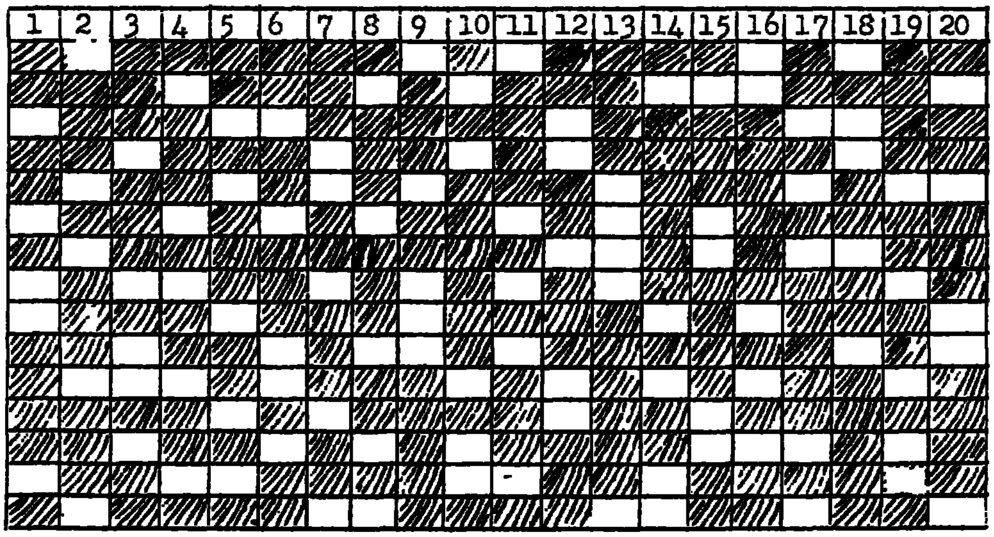


FIGURE 46.

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 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.

b. Such a grille can assume 4 positions, two obverse and two reverse. Arrangements must be made in advance as to which positions will be employed.

c. The solution of a single cryptogram enciphered by one and only one position of such a grille presents a hopeless problem, for the apertures being distributed at random throughout the grille there is nothing which may be seized upon as a guide to the reconstruction of either the grille or the plain text. It is conceivable, of course, that a person with an infinite amount of patience could produce an intelligible text and a grille conformable to that text, the grille having a definite number of columns and a fixed number of apertures distributed at random throughout the columns. But there would be no way of proving that the plain text so obtained is the actual plain text that was enciphered; for it would be possible to produce several "solutions" of the same character, any one of which might be correct.[4]

d. However, suppose a grille of this sort were employed to encipher a long message, requiring two or more applications of the grille. For example, in the case of the grille shown in Fig. 46, having a capacity of 100 letters per application, suppose a message of 400 letters were to be enciphered, requiring two obverse and two reverse applications of the grille. It is obvious that symmetrical relationships of the nature of those pointed out in Paragraph 31 can be established. Of course, if the grille is used several times in the same position to its full capacity, producing cryptograms of multiples of 100 letters, then the

[4] In this connection, see Military Cryptanalysis, Part III, Sec. XI, footnote 8.

sections of 100 letters may be superimposed and the solution in Paragraph 28 applied.

e. If the grille shown in Fig. 46 were used to encipher two messages, one of 80 letters,, the other of 85, it would be possible to solve these messages. For by eliminating 5 letters from the longer message, the two cryptograms can be superimposed and handled as in Paragraph 28. The difficulty would be in finding the 5 extra letters. Of course, if it should happen that one of the messages required 3 or 4 nulls and letters such as J, X or Z were employed for this purpose, the nulls would be likely characters for elimination. But regardless of this, even if letters of medium or high frequency were used as nulls, patient experimentation would ultimately lead to solution. The latter, it must be conceded, would be difficult but not impossible.

SECTION VII

COMBINED SUBSTITUTION-TRANSPOSITION SYSTEMS

35. Monoalphabetic substitution combined with transposition. - a. A message may undergo monoalphabetic substitution and the resulting text passed through a simple transposition. When this is the case a uniliteral frequency distribution will, of course, exhibit all the characteristics of monoalphabeticity, yet the cryptogram will resist all attempts at solution according to straightforward simple substitution principles. It is usually not difficult to detect that a transposition is involved because there will not only be long strings of low-frequency letters or high-frequency letters but what is more important, there will be very few or no repetitions of digraphs, trigraphs, and tetragraphs, since these will be broken up by the transposition. When a uniliteral distribution presents all the external evidences of monoalphabeticity and yet there are no repetitions, it is almost a positive indication of the presence of transposition superimposed upon the substitution, or vice versa. (The former is usually the case).

b. When confronted with such a situation the cryptanalyst usually proceeds by stages, first eliminating the transposition and then solving the monoalphabet. It is of course obvious that the general solution for transposition ciphers (cryptograms of identical length in the same key) will not be applicable here, for the reason that such a solution is based upon anagramming, which in turn is guided by the development of good digraphs, trigraphs, and polygraphs. Since the letters of a combined substitution-transposition cipher are no longer the same as the original plain-text letters, anagramming of columns formed by superimposing identical-length cryptograms can yield no results, because there is nothing to guide the cryptanaylst in his juxtaposition of columns.

c. Of course, if it should happen that the substitution process involves known alphabets, the cryptanalyst can remove the effects of the substitutive process before proceeding to eliminate the transposition, even if in the encipherment the substitution came first. For example, if a standard cipher alphabet were employed for the substitution the uniliteral frequency distribution would give indications thereof and the cipher letters could immediately be converted to the normal plain-text equivalents. The latter may then be studied as though merely transposition had been applied. But if unknown mixed cipher alphabets were employed, this initial comparison can not be accomplished and a solution must wait upon the removal of the transposition before the substitution can be attacked.

d. Of course, if nothing is known about the system of transposition that has been employed, there is hardly anything to do but experiment with various types of transposition in an attempt to bring about such an arrangement of the text as will show repetitions. If this can be done, then the problem can be solved. For example, suppose that a message has been enciphered by a single mixed cipher alphabet and the substitution text has then been inscribed within a rectangle of certain dimensions according to one of the usual routes mentioned in Paragraph 5.

Repetitions in the plain text will of course be preserved in the substitution text but will be destroyed after the transposition has been applied. The cryptanalyst, however, in his attempts to eliminate the transposition may experiment with route transpositions of the various types, employing rectangles of various dimensions as suggested by the total number of letters in the cryptogram. If he perseveres, he will find one route which he will know is correct as soon as he tries it <u>because it will disclose the repetitions in the plain text</u>, although the latter are still covered by a substitution.

<u>e</u>. Practically all the methods of transposition which may be applied to plain text may also be applied to a text resulting from an initial transformation by substitution. As already mentioned, route transposition may be used; reversed and rail-fence writing, columnar transposition with or without keying and with complete or incomplete rectangles are also possible. From a practical standpoint, keyed columnar transposition applied to a monoalphabetic substitution is not only a popular but also a fairly secure combination because in this case the elimination of the transposition is a rather difficult matter. If the rectangle is completely filled the problem is not insurmountable in the case of a long message transposed by means of transposition with a rectangle of fairly small dimensions. For by assuming rectangles of various dimensions suggested by the total number of letters, cutting the columns apart, and then combining columns on the basis of the number of repetitions produced within juxtaposed columns and between different sets of juxtaposed columns, it is possible to reconstruct the rectangle and thus remove the transposition phase. This, however, is

admittedly a slow and difficult process even under the most favorable conditions; and if the rectangle is incompletely filled the process is practically futile. For in the latter case the lack of absolutely clear-cut knowledge as to the lengths of the columns, the juxtaposition of columnar material becomes replete with uncertainties and engenders feelings of confusion, hopelessness, and inadequacy in the mind of the cryptanalyst. However, he need not be wholly in despair if he is confronted with a problem of this nature in war time, when many cryptograms become available for study. For there are special methods of solution suitable to the occasion, created by special circumstances attendant upon the interception of a voluminous traffic. In subsequent paragraphs the student will come to understand what is here meant by the special circumstances and will learn of these special solutions.

36. Other types of combined substitution-transposition systems. - a. There is no technical obstacle to the application of a transposition to the text resulting from any type of substitution, even if the latter is polyalphabetic or polygraphic in nature. The obstacles or rather objections to such combinations are practical in their character--they are too complex for ordinary use and the prevalence of errors makes them too difficult to handle, as a general rule. However, they have been and are sometimes used even as field ciphers. For instance, on the southeastern front during the World War the Central Powers made use of a somewhat irregular polyalphabetic substitution involving 4 standard alphabets and a keyed columnar transposition with incompletely filled rectangles of a relatively large number of columns. Nevertheless, messages in this system were solved by taking advantage of the possibility of devising special solutions.

b. Digraphic substitution, such as the Playfair cipher, may be combined with transposition to yield cryptograms of fair security. But here again the elimination of the transposition phase by taking advantage of special circumstances or by rearranging the text so as to uncover the repetitions which are inevitable in the Playfair cipher, will result in solution.

c. A particularly fruitful source of combined substitution-transposition is to be found in those methods generally designated as fractionating systems, wherein the substitution phase replaces each plain-text letter by an equivalent composed of two or more components or "fractions" and then these components are subjected to transposition in a second phase. This latter may be followed by a third phase, recombination of distributed components, and a fourth phase, the replacement of the recombined components by letters. Thus such a system comprises a first substitution, a transposition, a recombination, and a second substitution.[1] In the subsequent paragraphs certain systems of this sort will be dealt with in detail. They are interesting examples of practical systems of cryptography which have been used in the field of military operations in the past and may again be used in the future. The first one to be discussed is particularly interesting for this reason alone; but it is also of interest because it will serve as a model for the student to follow in his study of methods for the solution of combined substitution-transposition ciphers in general.

---

[1] See Special Text No. 166, Advanced Military Cryptography, Sec. XI.

SECTION VIII

SOLUTION OF THE ADFGVX SYSTEM

37. Introductory remarks. - a. One of the most interesting and practical of the many methods in which substitution and transposition are combined within a single system is that known in the literature as the ADFGVX cipher.[1] In this system a 36-character bipartite substitution checkerboard is employed, in the cells of which the 26 letters of the alphabet and the 10 digits are distributed in mixed order, often according to some keyword. The row and column indicators (coordinates) are the letters ADFGVX, and taken in pairs the latter are used as substitutes for the letters of the plain text. These substitutive pairs are then inscribed within a rectangle and a columnar transposition takes place, according to a numerical key. The cipher text consists then merely of the 6 letters A, D, F, G, V, and X.

b. The ADFGVX cipher system was inaugurated on the Western Front by the German Army on March 1, 1918, for communication between higher headquarters, principally between headquarters of divisions and corps. When first instituted on March 1, 1918, the checkerboard consisted of 25 cells, for a 25-letter German alphabet (J was omitted), and the 5

[1]Special Text No. 166, Advanced Military Cryptography, Sec. XI.

letters A, D, F, G, and X used as coordinates. On June 1 the letter V was added, the checkerboard having been enlarged to 36 cells, to take care of a 26-letter alphabet plus the 10 digits. Transposition keys ranged from 15 to 22 numbers (inclusive) and both the checkerboard and the transposition key were changed daily. The number of messages in this system varied from 25 a day upon the inception of the system to as many as 150 per day, during the last days of May, 1918. The first solution was made on April 6 by the French. The cipher continued in use rather extensively until late in June but from that time until the Armistice the volume of messages diminished very considerably. Although only 10 keys, covering a period of as many days were ever solved, the proportion of solved messages in the whole intercepted traffic was about 50%. This was true because of the fact that the keys solved were those for days on which the greatest number of messages was intercepted. The same system was employed on the southeastern front from July, 1918, to the end of the war. Keys were in effect at first for a period of 2 days and beginning on September 1, for a period of 3 days. In all 17 keys, covering a total of 44 days, were solved.

c. At the time that the Allied cryptanalytic offices were working with cryptograms in this system only three methods were known for their solution and all three of them are classifiable under the heading of special solutions, because certain conditions had to obtain before they could be applied. No general solution had been developed until after hostilities had ceased. Because they are interesting and useful some attention will be devoted to both the general and the special solutions. Since the special solutions are easy to understand and serve as a good introduction to the general solution, they will be taken up first.

38. Special solution by means of identical endings. - a. In Par. 24 it was demonstrated how the solution of keyed columnar transposition ciphers can be facilitated and simplified by the comparison of two cryptograms which are in the same key and the plain-text endings of which are identical. It was noted in that case that a study of the irregularly distributed cipher-text identities between the two cryptograms permits of not only cutting up the text into sections that correspond with the long and the short columns of the transposition rectangle but also of establishing the transposition key in a direct manner almost entirely mathematical in nature. When this has been accomplished the plain texts of these two messages are at once disclosed, and all other messages in the same key may be read by means of the key so reconstructed.

b. The same method of solution is applicable to the similar situation, if it can be found, in the case of the ADFGVX system, except that one more step intervenes between the reconstruction of the transposition rectangle and the appearance of the plain text in the rectangle: a monoalphabetic substitution must be solved, since the text in the rows of the rectangle does not consist of plain-text letters but of pairs of components representing these letters as enciphered by means of a bipartite substitution alphabet. Moreover, this latter step is comparatively simple when there is a sufficient amount of text in the two rectangles; if not, additional material for use in solving the monoalphabet can be obtained from other cryptograms in the same key, if they are available, since the transposition key, having already been reconstructed from the two cryptograms with identical endings, will permit of inscribing all other cryptograms in the same key within their proper rectangles.

c. A demonstration of the application of the principles involved in such a solution will be useful. The following cryptograms have been intercepted:

No. 1

```
X V A A X   V D D A G   D A D V F   A D A D A   F X G F V   X F A X A
X V A V F   A V X A D   G F F X F   F G A G F   D G D G D   D G A F D
A A D D D   X D A V G   G A A D X   A D F V F   F D F X F   G F G A V
A F A F X   F F X F X   F V D G X   A F F G X   A A A V A   V A F A G
D D F A G   V F A D V   F A V V X   G V A A A   F D F A X   X F A A G
D X
```

No. 2.

```
F D F F F   F V F A D   D V F V D   G A F D F   D A G A D   F D F A F
G A X G D   V X G F X   V X D X V   A A A A D   G X F F D   V F A A G
V G V F F   F D A F F   F X D A F   X G A F D   V F G X V   D D F A D
D A A A X   A A F F A   F V F X F   F A X X A   X D G X A   V D A V F
D F A V X   V A D X F   A X F F X   X A A V X   X A D X A   A A V V G
A G D X X   F D F A X   F D G D F   F X D G X   F A G D F   F D D V D
D X D A F   A G X X A   F G A V
```

d. The delimitation and marking of identities between these two cryptograms is a procedure similar to that explained in Par. 24b, except that a little more study may be necessary in this case because occasionally there may be considerable uncertainty as to exactly where an identity begins or ends. The reason for this is not difficult to understand. Whereas in Par. 24b the process involves "unfractionated" letters and there are about 18 or 20 different letters to deal with, so that an "accidental identity" is a rather rare occurrence, in the present problem the process involves fractions of letters (the components of the bipartite cipher equivalents), and there are only 6 different characters to deal with, so that such "accidental identities" are quite frequent. Now the cryptanalyst is not able at first to distinguish between these accidental identities and actual identities and this is what makes the process somewhat difficult. What is meant will become perfectly clear presently.

e. Taking the two illustrative cryptograms, the first step is to ascertain what identities can be found between them, and then mark off these identities. For example, it is obvious that if the messages end alike the last several letters in No. 1 should be found somewhere in No. 2, and likewise the last several letters in No. 2 should be found somewhere in No. 1. The number of letters in identical sequences will depend upon the length of the identical text and the width of the transposition rectangle. Searching through No. 2 for a sequence such as AGDX, or GDX, or at least DX, the tetragraph AGDX is found as letters 151-54. The last column of No. 2 ends with FGAV; searching through No. 1 for a sequence FGAV, or GAV, or at least AV, the tetragraph FGAV is found as letters 87-90. These identities are underlined or marked off in some fashion, and search is made for other identities. It would be a great help if the width of the transposition rectangle were known, for then it would be possible to cut up the text into lengths approximately corresponding to column lengths, and this would then restrict the search for identical sequences to those sections which correspond to the bottoms of the columns. Suppose the key to contain 20 numbers. Then the rectangle for No. 1, containing 152 letters, would consist of 12 long columns of 8 letters and 8 short ones of 7 letters; that for No. 2, containing 194 letters, would consist of 14 long columns of 10 letters and 6 short ones of 9 letters. If that were correct then in No. 1 the end of the first column would be either XVDD, or XVD. Searching through No. 2 for either of these a sequence XVDD is found as letters 84-7. Column 1 is probably a long column in No. 1. The word probably is used because the identity may extend only over the letters XVD, and the next D may be an accidental similarity, since the chances that D will appear by pure accident are 1 in 6, which is not at all improbable. It must also be pointed out that a certain number of telegraphic errors may be expected, and since there are only 6 different letters the chances that an F, for example, will be received or recorded as a D are fairly good. Column 1 of No. 2 ends either with VFAD or VFA. Searching through No. 1, a sequence VFAD is found as letters 14-17; a sequence VFA is found as letters 34-6; a sequence VFFD is found as letters 79-82; a sequence VFAD is also found as letters 126-130; a sequence VFA is found as letters 131-3. Here are several possibilities; which is the one to choose? Two of these possibilities coincide exactly with the full sequence being sought, VFAD. One of them is at 14-17, but this is rather unlikely to be the correct one. For if an hypothesis of a key of 20 columns is assumed, as has here been done, then column 2 must contain either 8 or 7 letters and to assume VFAD in positions 14-17 would make column 2 a column of 9 letters, which is inconsistent with that hypothesis. The other VFAD sequence, at 126-30, remains a candidate, since at this stage it is not possible to tell just where the ends of the columns are, and there is therefore nothing to indicate that this possibility may be ruled out. Another section of the text of one or the other cryptogram is selected, with a view to establishing additional identities. To go through the whole process here would consume too much space and time. Moreover, it is not necessary, for the only purpose in carrying the demonstration this far is to indicate to the student the general procedure and to show him some of the difficulties he will encounter in the identification of the similar portions when the text is composed of only a very limited number of different letters. In this case, after more or less tedious experimentation, the hypothesis of a key of 20 columns is established as correct when two sets of 20 identities are uncovered and the identities are found to be as shown in Fig. 47.

f. A table of equivalencies is then drawn up:

No. 1.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
No. 2.	9	6	8	10	13	11	17	2	19	15	7	20	14	12	5	18	1	4	3	16

Since the rectangle for No. 2 has 2 more letters in the last row than the rectangle for No. 1, two chains of equivalents at 2 intervals are constructed. Thus:

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

These chains must now be united into a single chain by proper interlocking. Since cryptogram No. 1 has 12 long columns, and since the identities of these 12 columns are now known (1, 3, 5, 7, 9, 12, 13, 14, 16, 17, 19, 20), the interlocking of the two chains and hence the transposition key must be this:

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

g. The two cryptograms may now be transcribed into their proper transposition rectangles, as shown in Fig. 48.

No. 1.

```
X V A A [X V D D]1 A G D A [D V F]2 A D A [D A F X G]3 F V X F [A X A]4
X V A V [F A V X]5 A D G F [F X F]6 F G A G [F D G D]7 G D [D G A F D]8
A A D [D D X D A]9 V G G A [A D X]10 A D F V [F F D]11 F X F G [F G A V]12
A F A F [X F F X]13 F X F V [D G X A]14 F F G X [A A A]15 V A V A [F A G
D]16 D F A G [V F A D]17 V F A V [V X G]18 V A A A [F D F A]19 X X F A [A G
D X]20
```

No. 2.

```
F D F F F F [V F A D]1 D V F V [D G A F D]2 F D A G A D [F D F A]3 F
G A X G D [V X G]4 F X V X D X V [A A A]5 A D G X F F [D V F]6 A A G
V G V F [F F D]7 A F F F X [D A F X G]8 A F D V F G [X V D D]9 F A D
D A A [A X A]10 A F F A F V [F X F]11 F A X X A X [D G X A]12 V D A V F
D [F A V X]13 V A D X F A [X F F X]14 X A A V X X [A D X]15 A A A V V G
[A G D X]16 X F D F A X [F D G D]17 F F X D G X [F A G D]18 F F D D V [D
D X D A]19 F A G X X A [F G A V]20
```

FIGURE 47.

No. 1.

```
7 5 17 13 1 14 9 12 19 20 3 16 8 18 2 4 6 10 11 15
F X D A X F A F V X A V G V A F A V A F
G V F F V X A X A X D A D F G V D G D F
A A A A A F D F A F A V D A D X G G F G
G V G F A V D G A A D A G V A F F A V X
F F V X X D D F F A A F A V D A F A F A
D A F F V G X G D G F A F X V X X D F A
G V A F D X D A F D X G D G F A F X D A
D X D X D A A V A X G D
```

No. 2.

```
7 5 17 13 1 14 9 12 19 20 3 16 8 18 2 4 6 10 11 15
A F X V F V A F F F F A A F D F A F A X
A X F D D A F A F A D A F F V G D A F A
G V D A F D D X D G A A F X F A G D F A
V X F V F X V X D X G V F D V X X D A V
G D A F F F F A V X A V X G D G F A F X
V X X D F A G X D A D G D X G D F A V X
F V F F V X X D D F F A A F A V D A F A
F A D A F F V G X G D G F A F X V X X D
F A G V A F D X D A F D X G D G F A F X
D A D X D X D A A V A X G D
```

FIGURE 48.

No. 1.

```
7 5 17 13 1 14 9 12 19 20 3 16 8 18 2 4 6 10 11 15
 H   A   V   E   O   R   D   E   R   E
F X D A X F A F V X A V G V A F A V A F

 D   C   O   M   M   A   N   D   I   N
G V F F V X A X A X D A D F G V D G D F

 G   G   E   N   E   R   A   L   2   3
A A A A A F D F A F A V D A D X G G F G

 D   B   R   I   G   A   D   E   T   O
G V G F A V D G A A D A G V A F F A V X

 C   O   U   N   T   E   R   A   T   T
F F V X X D D F F A A F A V D A F A F A

 A   C   K   W   I   T   H   O   U   T
D A F F V G X G D G F A F X V X X D F A

 D   E   L   A   Y   W   I   T   H   A
G V A F D X D A F D X G D G F A F X D A

 L   L   A   R   M   S
D X D X D A A V A X G D
```

No. 2.

```
7 5 17 13 1 14 9 12 19 20 3 16 8 18 2 4 6 10 11 15
 E   X   P   E   C   T   E   N   E   M
A F X V F V A F F F F A A F D F A F A X

 M   Y   A   T   T   A   C   K   A   T
A X F D D A F A F A D A F F V G D A F A

 D   A   Y   L   I   G   H   T   S   T
G V D A F D D X D G A A F X F A G D F A

 O   P   H   O   L   D   Y   O   U   R.
V X F V F X V X D X G V F D V X X D A V

 S   E   C   T   O   R   W   I   T   H
G D A F F F F A V X A V X G D G F A F X

 O   U   T   F   A   I   L   S   T   O
V X X D F A G X D A D G D X G D F A V X

 P   C   O   U   N   T   E   R   A   T
F V F F V X X D D F F A A F A V D A F A

 T   A   C   K   W   I   T   H   O   U
F A D A F F V G X G D G F A F X V X X D

 T   D   E   L   A   Y   W   I   T   H
F A G V A F D X D A F D X G D G F A F X

 A   L   L   A   R   M   S
D A D X D X D A A V A X G D
```

FIGURE 49.

h. A frequency distribution is now made of all the bipartite pairs, so as to solve the enciphering checkerboard. There is no necessity for going through this part of the solution, for it falls along quite normal lines of monoalphabetic substitution. The checkerboard is found to be as follows:[2]

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

i. The two plain-text rectangles are shown in Fig. 49.

j. Speculating upon the disposition of the letters within the enciphering checkerboard, it soon becomes evident that the key-phrase upon which it is based is GERMAN MILITARY CIPHERS. The digits are inserted immediately after the letters A, B, C, ..., as they occur in the mixed sequence, so that the complete checkerboard is as shown in Fig. 50:

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

FIGURE 50.

The transposition key was evidently derived from the first 20 letters of the mixed sequence:

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

The date (20th) indicates that the transposition key will have 20 numbers in it.

39. Special solution by means of identical beginnings. - a. In Par. 23 was demonstrated the method of solution based upon finding two cryptograms which are in the same key and the plain texts of which begin

---

[2]Since the 1st cryptogram is addressed to the CG 23d Brigade and the 2d cryptogram mentions that the commander of that brigade has been ordered to do so and so, the solution of the groups GG (= 2) and FG (= 3) is made by inference. This gives the placement of these two digits in the cipher square.

with the same words. The application of this method to the corresponding situation in the case of the ADFGVX system should by this time be obvious. The finding of identical sequences is somewhat easier in this case than in the case of identical endings because the identities can be found in parallel progression from the beginning to the end of the two cryptograms being compared. Moreover, the discovery of two cryptograms with similar beginnings is easier than that of two with similar endings because in the former case the very first groups in the two cryptograms contain identities, whereas in the latter case the identities are hidden and scattered throughout the texts of the two cryptograms. On the other hand, the complete solution of a case of identical endings is very much more simple than that involving identical beginnings because in the former case the establishment of the identities carries with it almost automatically the complete reconstruction of the transposition key, whereas in the latter this is far from true and additional cryptograms may be essential in order to accomplish this sine qua non for the solution.

b. The following represent 8 cryptograms of the same date, assumed to have been enciphered by the same key. The cryptograms have been

No. 1.

```
V D D F A  X F A A X  D X G G F  F V F X F  G X D X G  D G A G F
A G D A D  V G G D A  A A D X X  D X A F F  A A D A F  D F F D A
```

No. 2.

```
G X D D A  D D G D F  V G X A X  X X G X G  A A A A D  F A D D X
A V D X F  X A D
```

No. 3.

XDAAA GXDDX VFFVD GADFD XAAAG DFADG
AFDAD GVGDV FDFXA GFXAF AFAXD DDDFD
XAXVA DXFXF DGAGF GGADD AGDGX AVGDG
ADAFA XFAAG VAAGA FDVDV DXFDA XFDFF
GDXDV DADAV DADDD GADAG AAAFG GDXAX
FGVXD DGDDF AFAGV AFGXG VDDAX XDVFF
FFDXG VGDFG AVADA XDAFA AFDGF VFXXX
AAGAG AFDGX AFAFX XGGAG AAFFA AFDGA
GAFVX DGGFG DAAAF DADAD XVVAX FVADD
GAFFF GXAXD FDDFX AAAAA

No. 4.

AFGFX AGXAG XDDAF AAXAV GDDDD FAFGV
DGDXA FDXAX GFGDD VADXA XGFAX FDADD
GD

No. 5.

XAAAD DGAAG DDDXF FAVGA XDGGD FFAVA
DAAXA GDXDX XXXDG VFADA DFFFF VVGFD
XFDGG DAXDG ADFD

No. 6.

XDAAV DXDGF XVGDD AVGXA DXAAD XGGAA
GDFDA AAGAX DVFDF DFFDD FDDFX FXXFD
FDXAX GAXFF VDVAF GVDVD DDAGD GGDAA
GGFDD DVFFV VAGVA XAAGG XGXDD DADXF
ADFFG DGFDA AFGAX FFDVD DDAGA FADAV
DDDAV GAVAD FGDDF FDGDV DGGXA XAXDA
DXDVF FXVAX GFDAG XFFFF AAXDA FVDXG
XFDAG AGAVD VAGAF DGDAV VDDDD DFXGV
AFFAA FFFDV DFFAF DAGDG FAAAF DXAXA
VAXDA GADXD VFAFF FGDDA DDDFA GDFAX
DG

No. 7.

AGFGV DDDDF DDFXF DDGDF AXFDD VDVXA
DDAXX AADDF AGGFF AXDDG XDFAD DFDGD
DVAXA XFXDA FXDDG FXGDV GFFGX DADFA
DDAFF VDGXA ADXFX GVADA XGXAG AGDGV
XDDV

No. 8.

D F G F X D F A F F X D X A G A D G G G D D F G A X G V D F
V V F D A A A X G D A V D V A D D G V D A F A G

examined for identical beginnings, and numbers 3 and 6 apparently begin alike, identical portions being underlined as shown. Now the number of identical sections in the two cryptograms is 15; this indicates that the width of the transposition rectangle is 15. Therefore, No. 3 (290 letters) has 5 long columns of 20 letters and 10 short columns of 19 letters: [(15 x 20) - 10 = 290] No. 6 (302 letters has 2 long columns of 21 letters and 13 short columns of 20 letters. [(15 x 21) - 13 = 302]. The identical sections in No. 3 and No. 6 having been marked off as shown in Fig. 51, the next step is to transcribe the texts into their correct column lengths as given by the study of identical sections, writing them merely in their serial order, as shown in Fig. 52. In this transcription no serious difficulty is usually encountered in the division into correct column lengths, this process being guided by the identical sequences, the number of letters between the identical sequences, and the maximum and minimum lengths of the columns as calculated from the dimensions of the rectangle. Whenever difficulties are encountered in this process, they are brought about by accidental identities of letters before and after the true or actual identical sequences. In the present case no such difficulties arise except in going from column 12 to column 13. The identical sections for column 13 here consist of the sequence A F F A A F; if these sections are placed at the head of column 13, it leaves column 12 one letter short at the bottom in each diagram. This means that the initial A's in these identical

No. 3.

XDAAA GXDDX VFFVD GADFD XAAAG DFADG
1 2
AFDAD GVGDV FDFXA GFXAF AFAXD DDDFD
3 4
XAXVA DXFXF DGAGF GGADD AGDGX AVGDG
5
ADAFA XFAAG VAAGA FDVDV DXFDA XFDFF
6 7
GDXDV DADAV DADDD GADAG AAAFG GDXAX
8
FGVXD DGDDF AFAGV AFGXG VDDAX XDVFF
9 10
FFDXG VGDFG AVADA XDAFA AFDGF VFXXX
11
AAGAG AFDGX AFAFX XGGAG AAFFA AFDGA
12 13
GAFVX DGGFG DAAAF DADAD XVVAX FVADD
14
GAFFF GXAXD FDDFX AAAAA
15

No. 6.

XDAAV DXDGF XVGDD AVGXA DXAAD XGGAA
1 2
GDFDA AAGAX DVFDF DFFDD FDDFX FXXFD
3
FDXAX GAXFF VDVAF GVDVD DDAGD GGDAA
4 5
GGFDD DVFFV VAGVA XAAGG XGXDD DADXF
6
ADFFG DGFDA AFGAX FFDVD DDAGA FADAV
7 8
DDDAV GAVAD FGDDF FDGDV DGGXA XAXDA
9
DXDVF FXVAX GFDAG XFFFF AAXDA FVDXG
10 11
XFDAG AGAVD VAGAF DGDAV VDDDD DFXGV
12
AFFAA FFFDV DFFAF DAGDG GAAAF DXAXA
13 14
VAXDA GADXD VFAFF FGDDA DDDFA GDFAX
15
DG

FIGURE 51.

No. 3

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
X	D	D	F	D	A	D	D	G	X	A	A	F	A	A
D	X	V	D	D	G	F	A	D	D	X	G	F	A	F
A	A	F	X	A	V	F	G	D	V	D	A	A	A	F
A	A	D	A	G	A	G	A	F	F	A	F	A	F	F
A	A	F	X	D	A	D	A	A	F	F	D	F	D	G
G	G	X	V	G	G	X	A	F	F	A	G	D	A	X
X	D	A	A	X	A	D	F	A	F	A	X	G	D	A
D	F	G	D	A	F	V	G	G	D	F	A	A	A	X
D	A	F	X	V	D	D	G	V	X	D	F	G	D	D
X	D	X	F	G	V	A	D	A	G	G	A	A	X	F
V	G	A	X	D	D	D	X	F	V	F	F	F	V	D
F	A	F	F	G	V	A	A	G	G	V	X	V	V	D
F	F	A	D	A	D	V	X	X	D	F	X	X	A	F
V	D	F	G	D	X	D	F	G	F	X	G	D	X	X
D	A	A	A	A	F	A	G	V	G	X	G	G	F	A
G	D	X	G	F	D	D	V	D	A	X	A	G	V	A
A	G	D	F	A	A	D	X	D	V	A	G	F	A	A
D	V	D	G	X	X	D	D	A	A	A	A	G	D	A
F	G	D	G	F	F	G	D	X	D	G	A	D	D	A
		D	A	A		A							G	

No. 6

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
X	D	D	F	D	A	D	D	G	X	A	A	F	A	A
D	X	V	D	D	G	F	A	D	D	X	G	F	A	F
A	A	F	X	A	V	F	G	D	V	D	A	A	A	F
A	A	D	A	G	A	G	A	F	F	A	F	A	F	F
V	D	F	X	D	X	D	F	F	F	F	D	F	D	G
D	X	D	G	G	A	G	A	D	X	V	G	F	X	D
X	G	F	A	G	A	F	D	G	V	D	D	F	A	D
D	G	F	X	D	G	D	A	D	A	X	A	D	X	A
G	A	D	F	A	G	A	V	V	X	G	V	V	A	D
F	A	D	F	A	X	A	D	D	G	X	V	D	V	D
X	G	F	V	G	G	F	D	G	F	F	D	F	A	D
V	D	D	D	G	X	G	D	G	D	D	D	F	X	F
G	F	D	V	F	D	A	A	X	A	A	D	A	D	A
D	D	F	A	D	D	X	V	A	G	G	D	F	A	G
D	A	X	F	D	D	F	G	X	X	A	D	D	G	D
A	A	F	G	D	A	F	A	A	F	G	F	A	A	F
V	A	X	V	V	D	D	V	X	F	A	X	G	D	A
G	G	X	D	F	X	V	A	D	F	V	G	D	X	X
X	A	F	V	F	F	D	D	A	F	D	V	G	D	D
A	X	D	D	V	A	D	F	D	A	V	A	G	V	G
				V									F	

FIGURE 52.

sequences represent an accidental identity; these A's belong at the bottom of column 12 in each diagram, and the true identical sequences are F F A A F, and not A F F A A F. In some cases there may be many more instances of such accidental identities before and after the true identical sequences. Another thing to be noted is that the identical beginnings in this case run along for at least 4 complete rows and part of the 5th row in the transposition rectangle. Therefore, the identical sequences should consist of not less than 4, and not more than 5 letters; any letters in excess of 5 in any identical sequence are accidental identities. There are several such accidental identities in the case under study, viz, in columns 5 and 12.

c. Now comes the attempt to place the columns in proper sequence in the respective transposition rectangles. Since No. 6 has only 2 long columns, viz, 5 and 12, it is obvious that these two columns belong at the extreme left of the rectangle. Their order may be 5-12 or 12-5; there is no way of telling which is correct just yet. Since No. 3 has 5 long columns, viz, 3,4,5,7,12, and since from No. 6 it has been ascertained that 5 and 12 go to the extreme left, it is obvious that columns 3, 4, and 7 occupy the 3d, 4th, and 5th positions in the rectangles. Their order may be any permutation of the three numbers 3, 4, and 7; their exact order must be ascertained by further study.

d. In this study to fix the exact order of the columns and thus to reconstruct the transposition key, advantage can be taken of the diverse lengths of other cryptograms that may be available in the same key. In this case there are 6 additional cryptograms, Nos. 1, 2, 4, 5, 7, and 8, suitable for the purpose. The following calculations are made:

Cryptogram No.	Total No. of letters	Lengths of columns	No. of columns Long	Short
1	60	4	All same length	
2	38	3 and 2	8	7
4	62	5 and 4	2	13
5	74	5 and 4	14	1
7	124	9 and 8	4	11
8	54	4 and 3	9	6

Now No. 7 has 4 long columns, and these must consist of four columns from among the five already ascertained as falling at the extreme left, viz, 3, 4, 5, 7, and 14. Columns 5 and 14 have furthermore been placed in positions 1, 2, leaving columns 3, 4, and 7 for positions 3, 4, and 5. Which of these three possibilities is to be omitted as a long column in No. 7? A means of answering this question involves certain considerations of general importance in the cryptanalysis of this type of system.

e. Consider a transposition rectangle in which the number of columns is <u>even</u>, and consider specifically the 1st pair of columns in such a rectangle. The combinations of bipartite components formed by the juxtaposition of these 2 columns correspond to plain-text letters, and therefore the distribution of the bipartite digraphs in these columns will be monoalphabetic in character. The same is true with respect to the bipartite components in the 3d and 4th columns, the 5th and 6th columns, and so on. Hence, if a long cryptogram of this nature is at hand, and if the two columns which belong at the extreme left can be ascertained, then a distribution of the bipartite digraphs formed by juxtaposing these columns should not only be monoalphabetic, but also <u>this distribution, if it is at all normal, will afford a basis for matching other columns which will produce similar distributions</u>, for the text as a whole is monoalphabetic. In this way, by proper matching of columns, those which really go together to form the pairs containing the bipartite equivalents of the plain-text letters can be ascertained. From that point on, the solution of the problem is practically the same as that of solving a columnar transposition cipher with non-fractionated letters.

<u>f</u>. But now consider a plain-text rectangle in the ADFGVX system, in which the number of columns is <u>odd</u>, and consider specifically the 1st pair of columns in the rectangle. Now only the alternate combinations of bipartite components in these columns form the units of plain-text letters. The same is true of the bipartite components of the 3d and 4th, the 5th and 6th columns, and so on. In all other respects, however, the remarks contained in subparagraph <u>e</u> apply equally to this case where the width of the rectangle is odd.

g. Returning to the problem under study, it has been ascertained that columns 5 and 14 fall at the extreme left. Whether their correct order is 5-14 or 14-5 cannot at the moment be ascertained, nor is it essential. The thing to do is to make a distribution of the bipartite pairs and see what it is like. Since the width of the rectangle here is odd, only the 1st, 3d, 5th, ... pairs down the columns can be distributed in a frequency square. The results are shown in Fig. 53.

	No. 3 Col. 5	-	No. 3 Col. 14		No. 6 Col. 5	-	No. 6 Col. 14
1	D		A	1	D		A
	D		A		D		A
3	A		A	3	A		A
	G		F		G		F
5	D		D	5	D		D
	G		A		G		X
7	X		D	7	G		A
	A		A		D		X
9	V		D	9	A		A
	G		X		A		V
11	D		V	11	G		A
	G		V		G		X
13	A		A	13	F		D
	D		X		D		A
15	A		F	15	D		G
	F		V		D		A
17	A		A	17	V		D
	X		D		F		X
19	F		D	19	F		D
	A		G		V		V
				21	V		F

2d

1st	A	D	F	G	V	X
A	𝍸		𝍷			
D	𝍷𝍷	𝍷𝍷		𝍷	𝍷	
F		𝍷𝍷𝍷				
G	𝍷𝍷					
V		𝍷𝍷	𝍷			
X		𝍷				

FIGURE 53.

h. The distribution is fairly good. Five occurrences of AA are noted, 3 of FD. These must represent high-frequency letters. The ϕ test for monoalphabeticity may be applied.

$$E(\phi_p) = .0667 \times 21 \times 20 = 28.01$$

$$E(\theta_r) = .0385 \times 21 \times 20 = 16.17$$

$$\phi = (5 \times 4) + (2 \times 1) + (2 \times 1) + (3 \times 2) + (2 \times 1) + (2 \times 1) = 34$$

The observed value of ϕ is considerably greater than the expected value for plain text and more than twice as much as the expected value for random text. Using the distribution in Fig. 53 as a basis, an attempt is made to add to the 5-14 combination a column selected from among columns 3, 4, and 7, so that the 2d, 4th, 6th ... pairs down the 2d and 3d columns in the rectangle will give bipartite pairs that will conform to the distribution noted in Fig. 53. Since the results sought will be very materially affected if the combination 5-14 should really be 14-5, all possible combinations of 5-14 and 14-5 with 3, 4, and 7 must be tried. The various combinations tested are shown in Fig. 54.

i. Frequency distributions are now made. If combination 5-14-3 is correct for No. 3, it is also correct for No. 6; hence, a single distribution is made of the bipartite pairs in lines 1, 3, 5, ... of columns 5-14, and of the pairs in lines 2, 4, 6, ... of columns 14-3. Similar distributions are made of the pairs given under each of the other combinations. These distributions are shown in Fig. 55.

j. These distributions are now tested for monoalphabeticity, by applying the ϕ test. The number of occurences in each distribution is 41. Then $41 \times 40 \times .0667 = 109.4$ is the expected value of ϕ for plain text; $41 \times 40 \times .0385 = 63.1$ is the expected value of ϕ for random text. Here are the calculations for the first distribution (combination 5-14-3) yielding the observed value of ϕ as 76:

$$(5 \times 4) + (1 \times 0) + (1 \times 0) + (1 \times 0) + (2 \times 1) + (2 \times 1) + (2 \times 1) + (3 \times 2) + (1 \times 0) + (1 \times 0) + (5 \times 4) + (2 \times 1) + (1 \times 0) + (3 \times 2) + (3 \times 2) + (1 \times 0) + (2 \times 1) + (3 \times 2) + (2 \times 1) = 76.$$

The observed values for all 6 frequency distributions are shown herewith:

(1) 76 (3) 88 (5) 70 (2) 76 (4) 108 (6) 110

No. 3.

	(1)	(2)	(3)	(4)	(5)	(6)
	5-14-3	5-14-4	5-14-7	14-5-3	14-5-4	14-5-7
1	D A D	D A F	D A D	A D D	A D F	A D D
2	D A V	D A D	D A F	A D V	A D D	A D F
3	A A F	A A X	A A F	A A F	A A X	A A F
4	G F D	G F A	G F G	F G D	F G A	F G G
5	D D F	D D X	D D D	D D F	D D X	D D D
6	G A X	G A V	G A X	A G X	A G V	A G X
7	X D A	X D A	X D D	D X A	D X A	D X D
8	A A G	A A D	A A V	A A G	A A D	A A V
9	V D F	V D X	V D D	D V F	D V X	D V D
10	G X X	G X F	G X A	X G X	X G F	X G A
11	D V A	D V X	D V D	V D A	V D X	V D D
12	G V F	G V F	G V A	V G F	V G F	V G A
13	A A A	A A D	A A V	A A A	A A D	A A V
14	D X F	D X G	D X D	X D F	X D G	X D D
15	A F A	A F A	A F A	F A A	F A A	F A A
16	F V X	F V G	F V D	V F X	V F G	V F D
17	A A D	A A F	A A D	A A D	A A F	A A D
18	X D D	X D G	X D D	D X D	D X G	D X D
19	F D D	F D G	F D G	D F D	D F G	D F G
20	A G D	A G A	A G A	G A D	G A A	G A A

No. 6.

	(1)	(2)	(3)	(4)	(5)	(6)
	5-14-3	5-14-4	5-14-7	14-5-3	14-5-4	14-5-7
1	D A D	D A F	D A D	A D D	A D F	A D D
2	D A V	D A D	D A F	A D V	A D D	A D F
3	A A F	A A X	A A F	A A F	A A X	A A F
4	G F D	G F A	G F G	F G D	F G A	F G G
5	D D F	D D X	D D D	D D F	D D X	D D D
6	G X D	G X G	G X G	X G D	X G G	X G G
7	G A F	G A A	G A F	A F G	A G A	A G F
8	D X F	D X X	D X D	X D F	X D X	X D D
9	A A F	A A F	A A A	A A F	A A F	A A A
10	A V D	A V F	A V A	V A D	V A F	V A A
11	G A D	G A V	G A F	A G D	A G V	A G F
12	G X F	G X D	G X G	X G F	X G D	X G G
13	F D D	F D V	F D A	D F D	D F V	D F A
14	D A D	D A A	D A X	A D D	A D A	A D X
15	D G F	D G F	D G F	G D F	G D F	G D F
16	D A X	D A G	D A F	A D X	A D G	A D F
17	V D V	V D V	V D D	D V F	D V V	D V D
18	F X X	F X D	F X V	X F V	X F D	X F V
19	F D X	F D V	F D D	D F X	D F V	D F D
20	V V F	V V D	V V D	V V F	V V D	V V D
21	V F D	V F	V F	F V	F V	F V

FIGURE 54.

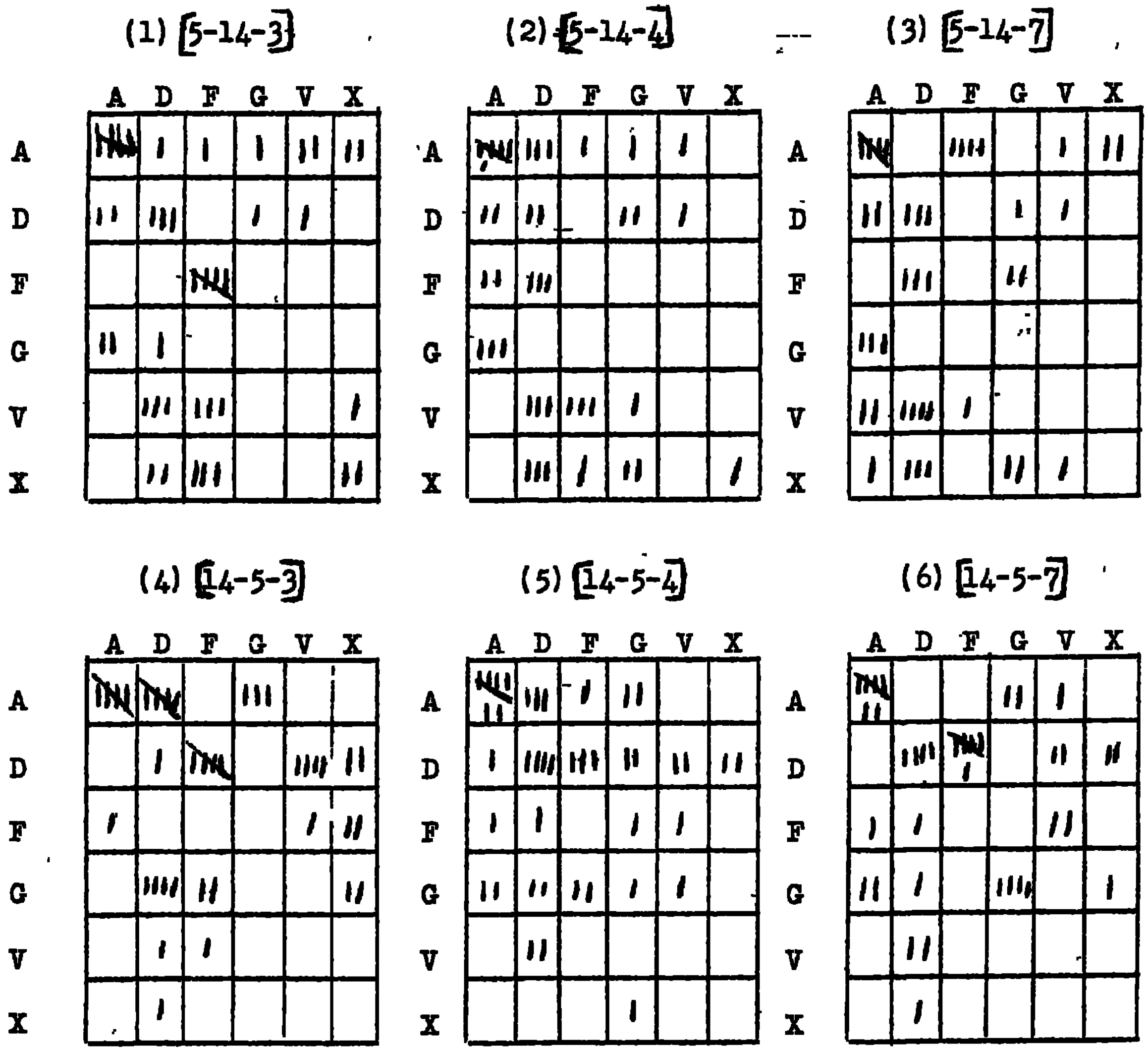


FIGURE 55.

Only two of these distributions give close approximations to 109, the expected value of ϕ, and they may be retained for further experiment. They are the ones for combinations (4) and (6), with values of 108 and 110, respectively.

k. Selecting combinations (4) and (6) viz, 14-5-3, and 14-5-7, since columns 14, 3, 4, 5 and 7 form the group of 5 columns at the left of the transposition rectangle, the following combinations are possible:

1) 14-5-3-4-7	(3) 14-5-7-3-4
2) 14-5-3-7-4	(4) 14-5-7-4-3

l. The following sets of columns correspond to these 4 combinations in the 2 cryptograms (Fig. 56).

No. 3.

	(1)	(2)	(3)	(4)
	14-5-3-4-7	14-5-3-7-4	14-5-7-3-4	14-5-7-4-3
1	A D D F D	A D D D F	A D D D F	A D D F D
2	A D V D F	A D V F D	A D F V D	A D F D V
3	A A F X F	A A F F X	A A F F X	A A F X F
4	F G D A G	F G D G A	F G G D A	F G G A D
5	D D F X D	D D F D X	D D D F X	D D D X F
6	A G X V X	A G X X V	A G X X V	A G X V X
7	D X A A D	D X A D A	D X D A A	D X D A A
8	A A G D V	A A G V D	A A V G D	A A V D G
9	D V F X D	D V F D X	D V D F X	D V D X F
10	X G X F A	X G X A F	X G A X F	X G A F X
11	V D A X D	V D A D X	V D D A X	V D D X A
12	V G F F A	V G F A F	V G A F F	V G A F F
13	A A A D V	A A A V D	A A V A D	A A V D A
14	X D F G D	X D F D G	X D D F G	X D D G F
15	F A A A A	F A A A A	F A A A A	F A A A A
16	V F X G D	V F X D G	V F D X G	V F D G X
17	A A D F D	A A D D F	A A D D F	A A D F D
18	D X D G D	D X D D G	D X D D G	D X D G D
19	D F D G G	D F D G G	D F G D G	D F G G D
20	G A D A A	G A D A A	G A A D A	G A A A D

No. 6.

	(1)	(2)	(3)	(4)
	14-5-3-4-7	14-5-3-7-4	14-5-7-3-4	14-5-7-4-3
1	A D D F D	A D D D F	A D D D F	A D D F D
2	A D V D F	A D V F D	A D F V D	A D F D V
3	A A F X F	A A F F X	A A F F X	A A F X F
4	F G D A G	F G D G A	F G G D A	F G G A D
5	D D F X D	D D F D X	D D D F X	D D D X F
6	X G D G G	X G D G G	X G G D G	X G G G D
7	A G F A F	A G F F A	A G F F A	A G F A F
8	X D F X D	X D F D X	X D D F X	X D D X F
9	A A F F A	A A F A F	A A A F F	A A A F F
10	V A D F A	V A D A F	V A A D F	V A A F D
11	A G D V F	A G D F V	A G F D V	A G F V D
12	X G F D G	X G F G D	X G G F D	X G G D F
13	D F D V A	D F D A V	D F A D V	D F A V D
14	A D D A X	A D D X A	A D X D A	A D X A D
15	G D F F F	G D F F F	G D F F F	G D F F F
16	A D X G F	A D X F G	A D F X G	A D F G X
17	D V F V D	D V F D V	D V D F V	D V D V F
18	X F X D V	X F X V D	X F V X D	X F V D X
19	D F X V D	D F X D V	D F D X V	D F D V X
20	V V F D D	V V F D D	V V D F D	V V D D F
21	F V	F V	F V	F V

FIGURE 56.

m. The additional bipartite pairs given by adding columns 4-7 to the basic combination 14-5-3 are distributed in the 4th frequency distribution square of Fig. 55, yielding the distribution shown in square (1) of Fig. 57. The other squares in Fig. 57 are constructed in the same way, for the other combinations of Fig. 56.

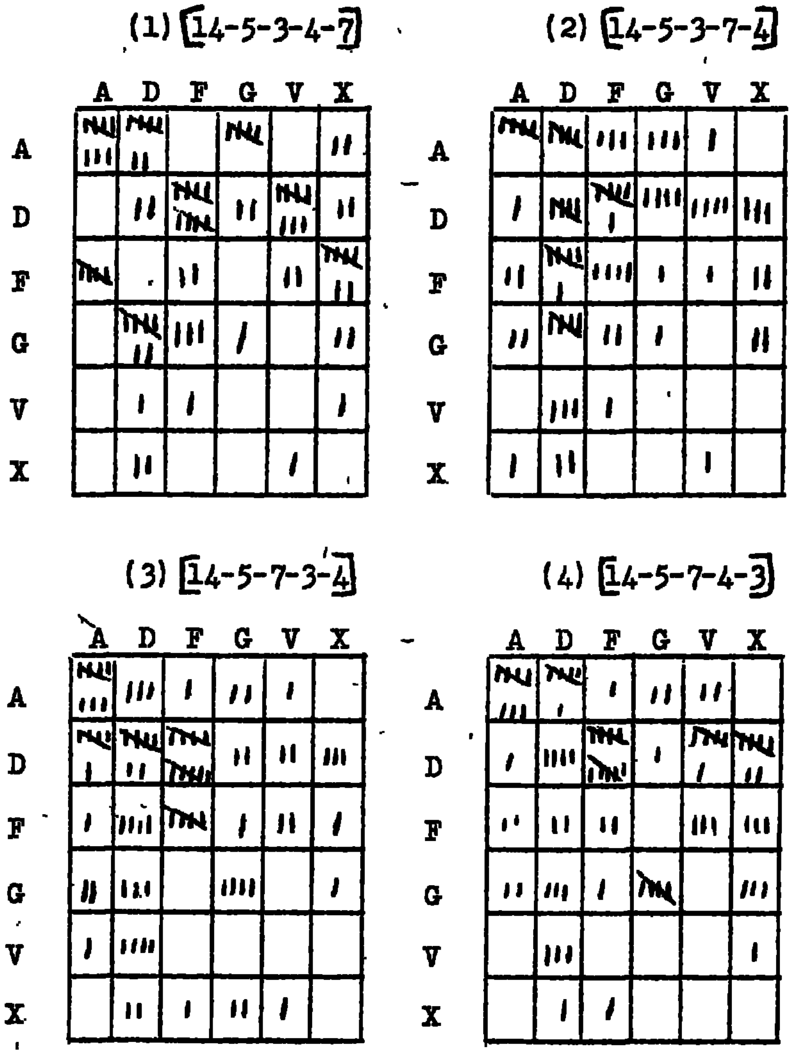


FIGURE 57.

n. Again applying the ϕ-test, the expected value of ϕ is $81 \times 80 \times .0667 = 432$. The observed values for the four combinations of Figs. 56 and 57 are as follows:

(1) For combination 14-5-3-4-7, $\phi = 390$

(2) For combination 14-5-3-7-4, $\phi = 270$

(3) For combination 14-5-7-3-4, $\phi = 326$

(4) For combination 14-5-7-4-3, $\phi = 342$

The combination 14-5-3-4-7, giving the greatest value for ϕ, is very probably the correct one.

o. Examining the other cryptograms that are available, it is seen that No. 7 is the third longest one of the entire set, with 124 letters; moreover, the dimensions of the rectangle [(15 x 9) - 11 = 124] are such as to bring about 4 long columns of 9 letters and 11 columns of 8 letters. The first 5 columns are definitely fixed in position, since it is known that the first 5 key numbers are 14-5-3-4-7. The resulting diagram is shown in Fig. 58. There is now a section consisting of 10 columns which are to be anagrammed to ascertain their correct sequence. The column to follow column 7 is ascertained on the basis of the repetitions which are brought about when the selected column is placed on the right. These repetitions should fall into those cells of frequency distribution (1), Fig. 57, which are of high frequency. In other words, the process is one of selecting from among columns 1, 2, 6, 8, 9, 10, 11, 12, 13, and 15 that column which will yield the most repetitions of bipartite digraphs with the digraphs given by the juxtaposition of columns 14-5-3-4-7, as distributed in frequency square (1) of Fig. 57. The column thus selected turns out to

14	5	3	4	7	1	2	6	8	9	10	11	12	13	15
A	X	D	V	D	A	D	F	D	X	F	G	D	A	G
D	A	G	D	F	G	F	F	D	D	X	X	A	A	D
A	A	D	V	A	F	D	A	V	A	G	D	F	D	G
X	D	F	X	D	G	D	X	A	F	D	A	F	X	V
G	D	A	A	D	V	F	D	X	X	V	D	V	F	X
X	F	X	D	F	D	X	D	A	D	G	F	D	X	D
A	A	V	D	D	D	F	G	X	D	F	A	G	G	D
G	G	D	A	G	D	D	X	F	G	F	D	X	V	V
A	G	D	X											

FIGURE 58.

be number 10. Then other columns are added by proceeding along the same lines, the work becoming progressively more easy as the number of available candidates decreases. Sometimes the discovery of what appears to be a long repetition within one of the cryptograms or between two cryptograms facilitates the process. In this case the results obtained from the 3 cryptograms under study are shown in Fig. 59.

No. 3.

14-5	3-4	7-10	15-12	13-1	2-8	6-9	11
A D	D F	D X	A A	F X	D D	A G	A
A D	V D	F D	F G	F D	X A	G D	X
A A	F X	F V	F A	A A	A G	V D	D
F G	D A	G F	F F	A A	A A	A F	A
D D	F X	D F	G D	F A	A A	A A	F
A G	X V	X F	X G	D G	G A	G F	A
D X	A A	D F	A X	G X	D F	A A	A
A A	G D	V D	X A	A D	F G	F G	F
D V	F X	D X	D F	G D	A G	D V	D
X G	X F	A G	F A	A X	D D	V A	G
V D	A X	D V	D F	F V	G X	D F	F
V G	F F	A G	D X	V F	A A	V G	V
A A	A D	V D	F X	X F	F X	D X	F
X D	F G	D F	X G	D V	D F	X G	X
F A	A A	A G	A G	G D	A G	F V	X
V F	X G	D A	A A	G G	D V	D D	X
A A	D F	D V	A G	F A	G X	A D	A
D X	D G	D A	A A	G D	V D	X A	A
D F	D G	G D	A A	D F	G D	F X	G
G A	D A	A					

FIGURE 59.

Figure 59 - Continued.

No. 6.

14-5	3-4	7-10	15-12	13-1	2-8	6-9	11
A D	D F	D X	A A	F X	D D	A G	A
A D	V D	F D	F G	F D	X A	G D	X
A A	F X	F V	F A	A A	A G	V D	D
F G	D A	G F	F F	A A	A A	A F	A
D D	F X	D F	G D	F V	D F	X F	F
X G	D G	G X	D G	F D	X A	A D	V
A G	F A	F V	D D	F X	G D	A G	D
X D	F X	D A	A A	D D	G A	G D	X
A A	D F	A X	D V	V G	A V	G V	G
V A	D F	A G	D V	D F	A D	X D	X
A G	F V	F F	D D	F X	G D	G G	F
X G	D D	G D	F D	F V	D D	X G	D
D F	D V	A A	A D	A G	F A	D X	A
A D	F A	X G	G D	F D	D V	D A	G
G D	X F	F X	D D	D D	A G	D X	A
A D	F G	F F	F F	A A	A A	A A	G
D V	X V	D F	A X	G V	A V	D X	A
X F	X D	V F	X G	D G	G A	X D	V
D F	F V	D F	D V	G X	A D	F A	D
V V	D D	D A	G A	G A	X F	A D	V
F V							

No. 7.

14-5	3-4	7-10	15-12	13-1	2-8	6-9	11
A X	D V	D F	G D	A A	D D	F X	G
D A	G D	F X	D A	A G	F D	F D	X
A A	D V	A G	G F	D F	D V	A A	D
X D	F X	D D	V F	X G	D A	X F	A
G D	A A	D V	X V	F V	F X	D X	D
X F	X D	F G	D D	X D	X A	D D	F
A A	V D	D F	D G	G D	F X	G D	A
G G	D A	G F	V X	V D	D F	X G	D
A G	D X						

p. What the cryptanalyst now has before him is a monoalphabetic substitution cipher, the solution of which presents no difficulties. The cipher square is reconstructed as completely as possible, blanks being left where there are no occurrences to give clues as to the character involved, usually some of the digits and the very infrequent letters. In this case the only letters which do not occur in the plain text are

Q, X, and Z. The digits 5 and 7 are recovered from the context, in message number 6, where the caliber of a gun is mentioned and the digits are confirmed at other places in the message. The square that is obtained is seen in Fig. 60. Examination of the mixed sequence discloses that it is based upon the phrase THE FLOWERS THAT BLOOM IN THE SPRING. This permits of the establishment of the transposition key and of the position of the digits in the checkerboard (as in Par. 38j). The results are shown in Fig. 61. The completely solved messages are shown in Fig. 62.

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

	A	D	F	G	V	X
A	T	H		E	5	F
D		L	O	W	R	S
F	A		B		M	I
G		N	P	G	7	C
V		D		J		K
X		U	V		Y	

FIGURE 60.

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

FIGURE 61.

No. 1.

```
14-5  3-4  7-10  15-12  13-1  2-8  6-9  11
 R     E     G     I     M     E     N     T
DV    AG    GG    FX    FV    AG    GD    A

    I     N     P     O     S     I     T
AF    XG    DG    FD    FD    XF    XA    A

 I     O     N     S     H     A     L     L
FX    DF    GD    DX    AD    FA    DD    D

    I     A     T     T     A     C     K
DF    XF    AA    AA    AF    AG    XV    X
```

No. 2.

```
14-5  3-4  7-10  15-12  13-1  2-8  6-9  11
 R     E     Q     U     E     S     T     I
DV    AG    XA    XD    AG    DX    AA    F

    N     S     T     R     U     C     T
XG    DD    XA    AD    VX    DG    XA    A

 I     O     N     S
FX    DF    GD    DX
```

Figure 62 - Continued.

No. 3.

```
14-5  3-4  7-10 15-12 13-1  2-8  6-9  11
 H     O     S     T     I     L     E     T
 AD    DF    DX    AA    FX    DD    AG    A
    R     O     O     P     S     E     S
 AD    VD    FD    FG    FD    XA    GD    X
 T     I     M     A     T     E     D     O
 AA    FX    FV    FA    AA    AG    VD    D
    N     E     B     A     T     T     A
 FG    DA    GF    FF    AA    AA    AF    A
 L     I     O     N     A     T     T     A
 DD    FX    DF    GD    FA    AA    AA    F
    C     K     I     N     G     E     A
 AG    XV    XF    XG    DG    GA    GF    A
 S     T     O     F     C     O     T     T
 DX    AA    DF    AX    GX    DF    AA    A
    E     R     S     T     O     P     P
 AA    GD    VD    XA    AD    FG    FG    F
 R     I     S     O     N     E     R     S
 DV    FX    DX    DF    GD    AG    DV    D
    C     A     P     T     U     R     E
 XG    XF    AG    FA    AX    DD    VA    G
 D     F     R     O     M     C     O     M
 VD    AX    DV    DF    FV    GX    DF    F
    P     A     N     Y     A     5     7
 FG    FF    AG    DX    VF    AA    VG    V
 T     H     D     I     V     I     S     I
 AA    AD    VD    FX    XF    FX    DX    F
    O     N     I     N     D     I     C
 XD    FG    DF    XG    DV    DF    XG    X
 A     T     E     E     N     E     M     Y
 FA    AA    AG    AG    GD    AG    FV    X
    I     N     T     E     N     D     S
 VF    XG    DA    AA    GG    DV    DD    X
 T     O     R     E     A     C     H     H
 AA    DF    DV    AG    FA    GX    AD    A
    U     N     T     E     R     S     T
 DX    DG    DA    AA    GD    VD    XA    A
 O     W     N     T     O     N     I     G
 DF    DG    GD    AA    DF    GD    FX    G
    H     T
 GA    DA    A
```

Figure 62 - Continued.

No. 4.

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

T H I R T Y S I
AA AD FX DV AA XV DX F

X T H F A L E
XX GA AA DA XF AD DA G

A V I N G G O L
FA XF FX GD GG GG DF D

D E N V I L L
DV DA GG DX FF XD DD D

E
AG

No. 5.

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

C O R P S W I L
GX DF DV GF DX DG FX D

L T A K E O V
DD DA AF AV XA GD FX F

E R T R A F F I
AG DV AA DV FA AX AX F

C C O N T R O
XG XG XD FG DA AD VD F

L A T O N C E
DD FA AA DF GD GX AG

Figure 62 - Continued.

No. 6.

```
14-5  3-4   7-10  15-12 13-1  2-8   6-9   11
H     O     S     T     I     L     E     T
AD    DF    DX    AA    FX    DD    AG    A
   R     O     O     P     S     E     S
AD    VD    FD    FG    FD    XA    GD    X
T     I     H     A     T     E     D     O
AA    FX    FV    FA    AA    AG    VD    D
   N     E     B     A     T     T     A
FG    DA    GF    FF    AA    AA    AF    A
L     I     O     N     M     O     V     I
DD    FX    DF    GD    FV    DF    XF    F
   N     G     U     P     S     T     R
XG    DG    GX    DG    FD    XA    AD    V
E     A     M     L     I     N     E     S
AG    FA    FV    DD    FX    GD    AG    D
   O     U     T     H     W     E     S
XD    FX    DA    AA    DD    GA    GD    X
T     O     F     R     J     5     7     7
AA    DF    AX    DV    VG    AV    GV    G
   H     A     N     D     A     S     S
VA    DF    AG    DV    DF    AD    XD    X
E     M     B     L     I     N     G     I
AG    FV    FF    DD    FX    GD    GG    F
   N     W     O     O     D     S     N
XG    DD    GD    FD    FV    DD    XG    D
O     R     T     H     E     A     S     T
DF    DV    AA    AD    AG    FA    DX    A
   O     F     G     O     L     D     E
AD    FA    XG    GD    FD    DV    DA    G
N     V     I     L     L     E     S     T
GD    XF    FX    DD    DD    AG    DX    A
   O     P     B     A     T     T     E
AD    FG    FF    FF    AA    AA    AA    G
R     Y     O     F     7     5     S     F
DV    XV    DF    AX    GV    AV    DX    A
   I     R     I     N     G     F     R
XF    XD    VF    XG    DG    GA    XD    V
O     M     O     R     C     H     A     R
DF    FV    DF    DV    GX    AD    FA    D
   D     L     E     E     F     A     R
VV    DD    DA    GA    GA    XF    AD    V
M
FV
```

Figure 62 - Continued.

No. 7.

```
14-5  3-4  7-10 15-12 13-1  2-8  6-9  11
 F     R     O     N     T     L     I     N
AX    DV    DF    GD    AA    DD    FX    G

    E     O     U     T     P     O     S
DA    GD    FX    DA    AG    FD    FD    X

 T     R     E     P     O     R     T     S
AA    DV    AG    GF    DF    DV    AA    D

    O     U     R     I     N     F     A
XD    FX    DD    VF    XG    DA    XF    A

 N     T     R     Y     M     I     S     S
GD    AA    DV    XV    FV    FX    DX    D

    I     O     N     S     S     H     O
XF    XD    FG    DD    XD    XA    DD    F

 T     D     O     W     N     I     N     E
AA    VD    DF    DG    GD    FX    GD    A

    N     E     M     Y     L     I     N
GG    DA    GF    VX    VD    DF    XG    D

 E     S
AG    DX
```

No. 8

```
14-5  3-4  7-10 15-12 13-1  2-8  6-9  11
 W     I     R     E     L     I     N     E
DG    FX    DV    AG    DD    FX    GD    A

    T     O     B     R     I     G     A
GA    AD    FF    FD    VF    XG    GF    A

 D     I     N     T     E     R     R     U
VD    FX    GD    AA    AG    DV    DV    X

    P     T     E     D
DG    FA    AA    GV    D
```

40. Special solution by the exact factor method. - a. The student who has comprehended the successive steps in the solution of the example discussed in the preceding paragraph is in a position to grasp at once

the mechanics of the special solution by the exact factor method. The latter is based upon the interception of a number of cryptograms, preferably lengthy ones, which have been enciphered by rectangles in which the last row is completely filled with letters. The total number of bipartite components in the case of such a cryptogram will yield clues as to the dimensions of the transposition rectangle. Then the text is transcribed into columns of appropriate length, all being equal in this respect, and the process of combining columns, as explained in Par. 39e, is applied in order to produce the best monoalphabetic distribution of bipartite digraphs down the juxtaposed columns. There is nothing to prevent the simultaneous use of all cryptograms that have been enciphered by completely-filled rectangles, for it is clear that if, for example, columns 15 and 4 are to be paired in one cryptogram, the same columns will be paired in all the other cryptograms. Hence, even if the rectangles are small in depth they can be used in this process; it is necessary only that all columns of any rectangle be of the same length. Now if only two or three such pairs of columns can be set up correctly, solution follows almost as a matter of course. No additional or new principles need be brought into play, beyond those already possessed by the student.

b. In this special solution, the important step is, of course, the initial one of experimenting with rectangles of various dimensions until the correct size has been hit upon. In some cases, excessive experimentation may not be necessary if the total number of characters is such as to yield only one or two possibilities with regard to the length of the columns. For example, suppose that previous work has established the fact that the enemy uses transposition rectangles not less than 15 and not more than 22 columns in width. A message totaling 703 letters would indicate a rectangle of 19 columns of 37 letters, since these two numbers are the only factors of 703. If this then were corroborated by other cryptograms of 76 (19 x 4), 152 (19 x 8), 190 (19 x 10) letters, the probability that 19 is the width of the transposition rectangle becomes quite persuasive. Of course, there will be and there should be other cryptograms of lengths that do not factor exactly; these represent the ones in which the rectangles are not completely filled in their last row. They do not enter into the solution at first, but just as soon as the positions of two or three key numbers become fixed, the data afforded by these messages become available for use in the later stages in the solution.

c. The exact-factor method is a useful one to know. For despite all instructions that may be drawn up insisting upon the advisability of not completing the last row of a transposition rectangle, the tendency to violate such a rule is quite marked, especially where a large cryptographic personnel must be employed. It is not astonishing to find that the temptation to fill the rectangle completely is particularly hard for lazy or ignorant clerks to resist when it happens that a message falls just one, two, or three letters short of forming a completely-filled rectangle: it is so much easier for such clerks to handle a rectangle with equal-length columns than one in which this is not the case. Moreover, the number of errors and therefore the number of times a shiftless or careless clerk must go over his work to correct errors is reduced to a minimum. Hence, it often happens that in such cases an enciphering clerk adds one, two, or three letters to complete the last row, thus leading to the transmission of not a few cryptograms enciphered by completely-filled rectangles.

d. Space forbids giving an example of such a solution. For students who desire to exercise their skill in executing the procedure, there is given in Appendix 2 a set of 44 cryptograms which were actually solved by this method. The text is in German, but a knowledge of the language is not essential to the reconstruction of the transposition key and of the various transposition rectangles involved.

41. General solution for the ADFGVX system. - a. All three of the foregoing methods of solving cryptograms in the ADFGVX system fall in the category of special solutions and therefore are dependent upon the fortuitous existence of the special conditions required under each case. What is really desired in the practical situation is a method of solution which is not so dependent upon chance or good fortune for success. A search for a general solution was, of course, made during the time that the system was under minute study by the cryptanalytic agencies of the Allies, but no general solution was devised. All the solutions made during actual hostilities and for a number of weeks thereafter were of the special types described in the preceding paragraphs. The first published description of a general solution is to be found in Givierge's Cours de Cryptographie, 1925, but only in broad outlines. A complete general solution was independently conceived by a group of cryptanalysts in the office of the Chief Signal Officer[3] and will be described in Paragraphs 42 and 43.

[3] See footnote 5 below.

b. The attention of the student is directed to the comments made in Paragraph 18, with regard to the significance of the term general solution in cryptanalysis. He must be cautioned not to expect that in practical work a general solution will, in the cryptanalytic as in the mathematical field, invariably lead to a solution. If there is a sufficient amount of text and if the text contains no abnormalities, the attempt to apply the general solution will usually be successful. But the cryptanalyst must remember that the ADFGVX system is by no means a simple one to solve even under the best of conditions and if there is only a small amount of text, if it happens that the transposition key is unusually long, or if the text is abnormal, he may not succeed in solving the messages by the straightforward method to be set forth below, and he may have to introduce special modifications. For the latter he can only rely upon his own ingenuity and intuition.

42. Basic principles of the general solution. - a. Every transposition rectangle in the ADFGVX system must conform to one or the other of two and only two fundamental types: the number of columns must be either odd or even. A number of important consequences follow from this simple fact, some of which have already been pointed out in Paragraph 39e. They will be elaborated upon in the next subparagraphs.

b. Consider a rectangle with an even number of columns. Each of its rows contains an even number of bipartite components, half of which are initial components, half, final components, alternating in a regular order from left to right in the rows. When the transposition is applied, all the components within a given column are of the same class, either initial or final. No intermixture or alternation of the two classes is possible. On the other hand, consider a rectangle with an odd number of columns. Each of its rows contains an odd number of bipartite components, the 1st row containing one more initial component than final components, the 2d row containing one more final component than initial components, and so on, this arrangement alternating regularly in the successive rows of the rectangle. When one studies the various columns of the rectangle, it is seen that in each column there is a perfectly regular alternation of initial and final components, the odd columns (1st, 3d, 5th, ...) beginning with an initial component, the even columns (2d, 4th, 6th, ...) beginning with a final component. This alternation in components remains true even after the transposition is applied. These remarks become very clear if one studies Fig. 63. Two transposition rectangles are shown, one with an even number of columns, the other with an odd number. Instead of the actual components (ADFGVX), the symbols θ_1 and θ_2 are used to indicate the two classes of components, initial and final, because in this analysis interest centers not upon the actual identity of a component but upon the class to which it belongs, initial or final. At the top of each column is placed a "plus" to denote a column occupying an odd-numbered position in the rectangle, or a "minus" to denote a column occupying an even-numbered position.

Even no. of columns

+	-	+	-	+	-	+	-	+	-
θ_1	θ_2	θ_1	θ_2	θ_1	θ_2	θ_1	θ_2	θ_1	θ_2
θ_1	θ_2	θ_1	θ_2	θ_1	θ_2	θ_1	θ_2	θ_1	θ_2
θ_1	θ_2	θ_1	θ_2	θ_1	θ_2	θ_1	θ_2	θ_1	θ_2

a

Odd no. of columns

+	-	+	-	+	-	+	-	+	-	+
θ_1	θ_2	θ_1	θ_2	θ_1	θ_2	θ_1	θ_2	θ_1	θ_2	θ_1
θ_2	θ_1	θ_2	θ_1	θ_2	θ_1	θ_2	θ_1	θ_2	θ_1	θ_2
θ_1	θ_2	θ_1	θ_2	θ_1	θ_2	θ_1	θ_2	θ_1	θ_2	θ_1

b

FIGURE 63.

c. In what follows, the term "odd column" will mean merely that the column in question occupies an odd position (1st, 3d, 5th, ...) in the transposition rectangle; the term "even column", that it occupies an even position (2d, 4th, 6th, ...) in the rectangle. The odd or even designation has no reference whatever to the nature of the transposition key number applicable to that column, whether it is odd or even. Now when the transposition is applied to the even-width rectangle a, Fig. 63, the cryptographic text will consist of a number of sections of letters, each section corresponding to a column of the rectangle, and therefore the number of sections in this case will be even. Moreover, all the components in a section corresponding to an odd column in rectangle a will be initial components, all those in a section corresponding to an even column, final components. The sections or columns are completely homogeneous with respect to the class to which their constituent components belong. On the other hand, when the transposition is applied to odd-width rectangle b, the cryptographic text will consist of an odd number of sections, each corresponding to a column of the rectangle. The components in the sections consist of members of both classes of components in a regular alternation; in a section corresponding to an odd column the order is $\theta_1 \rightarrow \theta_2 \rightarrow \theta_1$ ...; in a section corresponding to an even column the order is $\theta_2 \rightarrow \theta_1 \rightarrow \theta_2$ ... . The sections or columns are not homogeneous in this case as they are in the former.

d. Now if there were some way of distinguishing between initial components as a class and final components as a class it is clear that it may be possible first of all to ascertain whether the transposition rectangle contains an even or an odd number of columns. Secondly it may be possible to identify those columns which are even and those which are odd. Finally, it may be possible to ascertain which are the long columns and which are short, thus yielding the exact outlines of the rectangle in case the last row is incompletely filled. From that point on, solution follows along the same lines as explained in paragraph 40, with the modification that in the pairing of columns the number of possibilities is greatly reduced, since it is useless to pair two columns both containing initial components or final components.

e. The foregoing depends then upon the possibility of being able to distinguish as a class between initial and final components of the bipartite cipher equivalents in this system, or at least between letters belonging to one or the other of these two general classes of components. Now if the substitution checkerboard has not been consciously manipulated with a view to destroying certain properties normally characterizing its rows and columns, the sort of differentiation indicated above is quite possible. For example, if in the checkerboard shown in Fig. 61 the normal frequencies of the letters as they appear in English telegraphic plain text[4] are inserted in the cells and totals are obtained vertically and horizontally, these totals will permit of assigning frequency weights to the letters ADFGVX as initial and as final letters of the bipartite cipher equivalents of the plain-text letters. This is shown below in Fig. 64. The bipartite letter A has a frequency value of 284 as an initial component of the bipartite cipher equivalents of plain-text letters, and a frequency value of only 169 as a final component.

[4] As given in Fig. 3, page 13, Military Cryptanalysis, Part I.

	A	D	F	G	V	X	Sums
A	T 92	H 34		E 130		F 28	284
D		L 36	O 75	W 16	R 76	S 61	264
F	A 74		B 10		M 25	I 74	183
G		N 79	P 27	G 16		C 31	153
V		D 42		J 2		K 3	47
X	Q 3	U 26	V 15	X 5	Y 19	Z 1	69
Sums	169	217	127	169	120	198	1000

FIGURE 64.

Similarly, the letters V and X have frequency values of 47 and 69, respectively, as initial components and 120 and 198 as final components. It is obvious, then, that in this checkerboard the weighted frequency values of the letters A, V, and X as initial components differ considerably from the values of these same letters as final components, the value for G as an initial is only a little less than its value as a final, the values of D and F as initials are only a little more than their values as finals. But it is the wide variations in the weighted frequency values of certain of the letters as initial components and as final components, exemplified in the case of A, V, and X, which form the basis of the general solution, because these wide variations afford a means for making the various differentiations noted in subparagraph d.

f. Of course, in working with an unknown example, the composition of the checkerboard is unknown and therefore no accurate frequency weights may be assigned to the ADFGVX components in the cryptograms. However, it is still possible to arrive at some approximations for these weights in case there are several cryptograms available for study, as would normally be true in actual practice. How this can be done will be shown very soon, by studying an example. For the purposes of this study the set of 12 cryptograms given below will be used.

I

```
VDDGG GVFDF VDVVF VDGAD DAFFF
VDXFD DXDVX ADVDV FXGDF VADDG
DGDGV GDDDF XFADA VDVGD GADXV
DADAD FXAVF VDDAA VDFFD FVGDF
VDDGV DDDDA VADAF ADDXA DDGAD
FVGFV DGADV FXVXD GDDAG GDDXF
FDDXA DFGDA GXDDA VFDAF GVFVF
AFFVF AFXGF XDGVA DFVDG GAVGG
DDGDV XAXFD DX (212 letters)
```

II

```
VDAAV DDFXF XDDAX GXFXD DFXAD
VAGDD FAXDV AVDVD DFVFV FFGDG
FVAXV XAVGD VDXFD XDGAX GFGGF
VFGDF VDXAV XDDVG DDVGV AGFXF
AAAXD DXG (108 letters)
```

III

```
DAGAA FGAGV DAFGG XFDXD FVVXG
FXFDX DDAGA DDGVA DDVDD GAFGA
VGDGX DDDAV FVDDF DAAAA DXAGD
XAGGD DAVGV FGDVF VDGGX GGAFF
VFDAX GDDDG DAFDA DGGAD DGDXA
FVDFD XFVGD DVAVF DDDVF AGDFF
FXAAD FADGG VFDAV DGXFV DAAVG
DXFGG DDXGD A (186 letters)
```

IV

```
ADXVF XVGGV FDDVA FGAAV FDGVD
DDGDG FDVVA FGXFX FDDDD VGDAX
DAXDD DAGVF FAADV GDFXG XGVGD
DDDAD VXVFA VDAXX DFAAF AVDVG
VDVDD AXDAA (110 letters)
```

V

D F X F D D V V V D X F X F X F F F V A G F D X A
V D A G F D V D G F A D A A D F D V F G D A D F V
F V F X G X D D A G D V G V F D G X X D F F G D G
X G V D D V D D F G F V G D D V F V A G X X D F V
D X A V F G A G A G A X D V D F X G V G D A D D X
A G X D A D F D G X F D G G F V G X V V G D D D A
G X V D G V D V G X D D F D D V A G A A D G D D F
D G A G D F D D D D X G V G V G G G D G X D F G F
A D (202 letters)

VI

G D G F X A G V F V D D X G X D V D D A X D A A X
F A G V G D X F F V X F A D G F F D X A A F V X F
D F X F V G D G F X F D V V X V G D F V D D V F D
F V V D V D G G V F X F G V X F F V G V D D G D D
D D G D D A V G V X G A F F X F V D D D (120 letters)

VII

G A F G F F X F V F G F X A V A G G X D X X D D F
A G V D D V D V F F A D A V A V F V G G A D A A F
V F D F V D X F X X G D X D D F V D F F X D V F X
V A D X V A X D V X A F F V D F D G X F D G F D D
F V D V V A A F V F F V X D G F D D V A D D F D D
D X F F A G F X F X A A G V D G G V D F G G G X D
F D F V A F F G F X G D A X D G D G G D D A V D X
A D F A F V F X D D X V A G D V V D D F X D G X X
D V F V F D D D D A A F D F X D X G D A A F V D F
D V D D V A D D V D V A V D G A F V F X F A A V D
D F V D (254 letters)

VIII

D G V V G F X G G G A D F A F V V V A X A V G G V
V D V G V V D A V G D G D G A V F D D A D D D X X
D X F V F X G V G G D G D F G G D A D F D D X A V
F D D V F A D X G D A D G V A F F X A D F A D X D
G F A D F D D G V D V X A V A D D X F F A G D X F
F V F G F G F D F D V D X X D D G G D (144 letters)

IX

G D D D D X V G V D V D A V G F G D F V D V A V D
G F A G X A V F F G V A D D D A X X A X D G A D G
X A V V D G X X A A A V A D A D G X D V G D D D D
G V F X A A V G G V F X D A F D G V G A F G D D F
A V V G D D V D F X D V D G F V A A G D X F D V A
A D A G D A X F V G D D D A G V A V F G X X F D D
G X F V D G G D A V D A G G F D A X D X F F V G F
A X X A D D F (182 letters)

X

D G D D F V F A V D V F D A D G F V G V G G D F V
D V V X D D F D D V G X G V D X G V G D X D G D X
F X F D X V D A A D D F X D D A F F A A F V F A G
D A A G G F A X G V X X F X A D G D F D G X G D A
D A X G V V V D A A G G V F G V A V F V A A G A X
G X D G A (130 letters)

XI

V F D D V A X G D A D F G G G G F G D D F X X D A
F D D X G G A V G A G D V D F D F D D D G A F A F
D A A A G V A V F G G V A D D G D D F G F V D D A
D F G A F D F V D D F V V V A D A G D X F X X X F
F D X G D F D G F D D F G D A G F A A G G A D X D
G V D G A V G V D F D D F X G A G X F G V F V V D
G V D X D F F F X G X G X A G A G V G D V V X G F
V D X D D X F V D D X (186 letters)

XII

X F D F X V V D V D A V D A D V F A G D G V A D D
F D A A D X A D F V G V D G F X F G D V F V D D D
D G D V V A V V V F A D D A X A V F V A D A X D V
G D D F A X D D G X G V F X A V X V F D G D X D F
D V X A D V A V A V G V D D D A F D F A D V F F V
V G D A G F X D D F A D V X V D F X F F V V G F X
X G F V A V F A G G D A V V D X D X G D D V V A D
D D A G A A G X F G D D D G V F G F V G V X G V F
D F F D A A D V D D X G D F D D V D D G A F G D
(224 letters)

43. Illustration of solution.[5] - a. Since the initial letters of all 12 cryptograms are in the same class, that is, either initial or final components, they may all be combined into a single distribution. Furthermore, since it is certain that regardless of whether the transposition rectangle has an odd or an even number of columns the 3d, 5th, ... letters of the cryptograms are in the same class as the first letter,

---

[5] This illustration uses the same cryptograms and follows quite closely along the lines employed in a technical paper of the Signal Intelligence Service entitled General Solution for the ADFGVX Cipher, prepared by Messrs. Rowlett, Kullback, and Sinkov, in 1934.

the 3d, 5th, ... letters may be added to the distribution, so long as these odd letters come from the same section (column 1). It is, however, necessary to limit the number of letters taken from the beginning of any one cryptogram to a reasonable length of column, depending on the size of the cryptogram. Assuming it is known that the enemy is using transposition keys of not less than 15 nor more than 22 numbers, the latter could be taken as the maximum possible size. But to be on the safe side it will be here assumed that a transposition rectangle of not more than 25 columns is being used. Hence, so far as concerns cryptogram 1, which has 212 letters, on the basis of a key of 25 numbers [(25 x 9) - 13 = 212] there will be 12 columns of 9 letters and 13 columns of 8 letters. Since there is no way of telling which are long and which are short columns, it will be safer to work on the basis of columns of 8 letters. Therefore, the first 8 letters of cryptogram I are to be taken. In the case of cryptogram II, with 108 letters, its first 4 letters will be taken, and so on, through the 12 cryptograms, the number of letters to be taken in each case being governed by the length of the cryptogram. The sections taken in the case of the 12 cryptograms are shown in Fig. 65.

Cryptogram	Length	Letters taken	Cryptogram	Length	Letters taken
I	212	VDDGGGVF	VII	254	GAFGFFXFVF
II	108	VDAA	VIII	144	DGVVG
III	186	DAGAAFG	IX	182	GDDDDXV
IV	110	ADXV	X	130	DGDDF
V	202	DFXFDDVV	XI	186	VFDDVAX
VI	120	GDGF	XII	224	XFDFXVVDV

FIGURE 65.

b. The odd and the even letters of these 12 sections are then distributed separately, the results being shown in Figs. 66 and 67. A consideration of the mechanics of this system leads to the expectation that if the transposition rectangle has an even number of columns the two distributions will be similar; if it has an odd number, they will be different. The similarity or difference between the two distributions is usually discernible, with as few as 20 or 25 letters.

Odd (1st, 3d, ...) letters

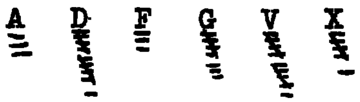


FIGURE 66.

Even (2d, 4th, ...) letters

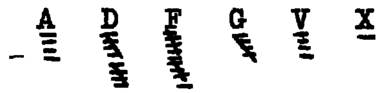


FIGURE 67.

c. Letters V and X are of high frequency in the odd positions (Fig. 66) but of low frequency in the even positions, (Fig. 67) whereas the letter F is of low frequency in the odd positions and of high frequency in the even positions. There can be no question that the two distributions are dissimilar, and the indications are clear that the transposition rectangle involves an odd number of columns.

d. Now the letters in Fig. 66 may be initial components, those in Fig. 67, final components, or the reverse may be the case. At the present stage of the study it is impossible to ascertain which of these alternative hypotheses is correct. However, this information is really immaterial at this stage. Suppose the letters in Fig. 66 are arbitrarily designated as class 1 components, those in Fig. 67 are class 2 components. Class 1 components (Fig. 66) are characterized by a predominance of V's and X's (over their frequencies in Fig. 67); class 2 components (Fig. 67) are characterized by a predominance of F's (over its frequency in Fig. 66.)

e. The two distributions in Figs. 66 and 67 apply to the letters which come from Column 1 of the transposition rectangles for the 12 cryptograms under study. In this column, the V's and X's fall predominantly in the odd positions, the F's fall predominantly in the even positions. Therefore, beginning with position 1, the components in this column show an alternation of the type $\theta_1 \rightarrow \theta_2 \rightarrow \theta_1$. By referring to Fig. 63 it will become clear that if class 1 components are initial components, then it must follow that column 1 occupies an odd position in the transposition rectangle; but if class 1 components are final components, then it must follow that column 1 occupies an even position in the transposition rectangle. Which of these alternatives is true cannot be ascertained at the moment. But the important point to be noted is that a definite reversal in the type of alternation of class 1 and class 2 components indicates the progress, in the transposition, from the end of one column to the beginning of the next column. That is, if it is found that from the beginning of the cryptogram the alternation of components is $\theta_1 \rightarrow \theta_2 \rightarrow \theta_1$ and after a number of letters this alternation changes to $\theta_2 \rightarrow \theta_1 \rightarrow \theta_2$, the point where this change occurs marks the end of column 1 and the beginning of the column 2. For the sake of brevity in reference, in the subsequent paragraphs the type of alternation $\theta_1 \rightarrow \theta_2 \rightarrow \theta_1$ will be designated as the "+ type", and this type of alternation characterizes columns which fall in odd-numbered positions in the transposition rectangle. The other type, $\theta_2 \rightarrow \theta_1 \rightarrow \theta_2$ will be designated as the "- type", and this type of alternation characterizes columns which fall in even-numbered positions in the transposition rectangle.

f. With these principles in mind, let cryptograms III and XI, each containing 186 letters, be studied. They may be superimposed, since they have identical numbers of letters and therefore the columns end at exactly the same points in both cryptograms.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
III.	D	A	G	A	A	F	G	A	G	V	D	A	F	G	G	X	F	D	X	D	F	V	V
XI.	V	F	D	D	V	A	X	G	D	A	D	F	G	G	G	G	F	G	D	D	F	X	X

	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
III.	X	G	F	X	F	D	X	D	D	A	G	A	D	D	G	V	A	D	D	V	D	D	G
XI.	D	A	F	D	D	X	G	G	A	V	G	A	G	D	V	D	F	D	F	D	D	D	G

	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69
III.	A	F	G	A	V	G	D	G	X	D	D	D	A	V	F	V	D	D	F	D	A	A	A
XI.	A	F	A	F	D	A	A	A	G	V	A	V	F	G	G	V	A	D	D	G	D	D	F

	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92
III.	A	D	X	A	G	D	X	A	G	G	D	D	A	V	G	V	F	G	D	V	F	V	D
XI.	G	F	V	D	D	A	D	F	G	A	F	D	F	V	D	D	F	V	V	V	A	D	A

	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115
III.	G	G	X	G	G	A	F	F	V	F	D	A	X	G	D	D	D	G	D	A	F	D	A
XI.	G	D	X	F	X	X	X	F	F	D	X	G	D	F	D	G	F	D	D	F	G	D	A

	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138
III.	D	G	G	A	D	D	G	D	X	A	F	V	D	F	D	X	F	V	G	D	D	V	A
XI.	G	F	A	A	G	G	A	D	X	D	G	V	D	G	A	V	G	V	D	F	D	D	F

	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161
III.	V	F	D	D	D	V	F	A	G	D	F	F	F	X	A	A	D	F	A	D	G	G	V
XI.	X	G	A	G	X	F	G	V	F	V	V	D	G	V	D	X	D	F	F	F	X	G	X

	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184
III.	F	D	A	V	D	G	X	F	V	D	A	A	V	G	D	X	F	G	G	D	D	X	G
XI.	G	X	A	G	A	G	V	G	D	V	V	X	G	F	V	D	X	D	D	X	F	V	D

	185	186
III.	D	A
XI.	D	X

FIGURE 68.

g. It has already been noted that beginning with the first letter of any one of the cryptograms, the type of alternation for column 1 is +. It is therefore not astonishing to find, within the first 10 letters, an alternation of the + type. Note how the V's and X's fall in the odd positions, the F's in the even. Thus:

	1	2	3	4	5	6	7	8	9	10
III.	D	A	G	A	A	F	G	A	G	V
XI.	V	F	D	D	V	A	X	G	D	A

It is seen that there are 2 V's which fall in odd positions (1 and 5), but one V falls in an even position (10). There is an X, which falls in an odd position (7); there are 2 F's, which fall in even positions (2 and 6). Unquestionably, then, the type of alternation, at least for the first 10 letters in each of these cryptograms, is +.

h. Take the next section of 10 letters in these two cryptograms. The letters are as follows:

	11	12	13	14	15	16	17	18	19	20
III.	D	A	F	G	G	X	F	D	X	D
XI.	D	F	G	G	G	G	F	G	D	D

Here there are 4 F's; 3 of them fall in odd positions (13, 17, 17), and one falls in an even position (12). There are 2 X's; one falls in an odd position (19), one in an even position. There are no V's among these letters. So far as the evidence afforded by the F's is concerned, it would appear that this section of text shows the type 2 or "- type" of alternation of components, since in type 1 or "+ type" the F's occupy even positions and here the majority of them occupy odd positions. But so far as the X's are concerned, the evidence is equally balanced: one X falls in an odd position, one in an even position. There being no V's, no conclusions can be drawn from this letter. To be guided solely by the evidence afforded by the 3 F's may be unwarranted. Is it not possible to weight the frequencies of the letters so that it will be unnecessary to rely merely upon a few of them and the evidence afforded by all the letters can be taken into account? Why not assign frequency weights according to the two distributions in Figs. 66 and 67? The figures then become as follows:

Odd (1st, 3d, ...) letters

A	D	F	G	V	X
3	11	3	8	11	6

Total - 42 letters

Even (2d, 4th, ...) letters

A	D	F	G	V	X
4	10	11	5	4	1

Total - 35 letters

FIGURE 69.

Since the odd letters have a total frequency of 42, the even, a total frequency of 35, for purposes of equalizing the distributions in applying the weights it seems advisable to deduct 1/6 from the total when applying the weights to odd letters.

i. Now in applying these weights to the letters, it must be borne in mind that since a transposition rectangle with an odd number of columns is involved, half of the letters are class 1 components, the other half are class 2 components. Hence, in finding the frequency value of the letters it is necessary to apply the weighted frequencies to alternate letters in the sections, as shown in Fig. 70.

	11	12	13	14	15	16	17	18	19	20
III.	D	A	F	G	G	X	F	D	X	D
XI.	D	F	G	G	G	G	F	G	D	D

Distribution of odd letters

A	D	F	G	V	X

0-3-3-3-0-1

Distribution of even letters

A	D	F	G	V	X

1-3-1-4-0-1

FIGURE 70.

These distributions, when evaluated in accordance with Fig. 69, yield a total frequency value of 126; when evaluated in accordance with Fig. 69 reversed, yield a total frequency value of 143. The detailed calculations are as follows:

Fig. 69 normal

(Odd letters as θ_1's, even letters as θ_2's)

$$\begin{cases} 0\,(3) + 3\,(11) + 3\,(3) + 3\,(8) + 0\,(11) + 1\,(6) = 72 \\ 1\,(4) + 3\,(10) + 1\,(11) + 4\,(5) + 0\,(4) + 1\,(1) = 66. \quad 72 - \frac{72}{6} = 60;\ 60 + 66 = 126. \end{cases}$$

Fig. 69 reversed

(Even letters as θ_1's, odd letters as θ_2's)

$$\begin{cases} 1\,(3) + 3\,(11) + 1\,(3) + 4\,(8) + 0\,(11) + 1\,(6) = 77 \\ 0\,(4) + 3\,(10) + 3\,(11) + 3\,(5) + 0\,(4) + 1\,(1) = 79. \quad 77 - \frac{77}{6} = 64;\ 64 + 79 = 143. \end{cases}$$

j. Now the frequency sums here obtained (148 vs 156) indicate that an alternation of the type $\theta_2 \rightarrow \theta_1 \rightarrow \theta_2$ is in effect, that is, if a beginning is made with position 11, the type of alternation is "-". Since the type of alternation for the first 10 letters is "+" and for the second 10 letters "-", the reversal in alternation would indicate that column 1 of the transposition rectangle ends somewhere near the 10th letter. This same sort of reversal takes place after the 20th letter, as shown by the calculation in Fig. 71.

	21	22	23	24	25	26	27	28	29	30
III.	F	V	V	X	G	F	X	F	D	X
XI.	F	X	X	D	A	F	D	D	X	G

Distribution of odd letters

A	D	F	G	V	X
1	2	2	1	1	3

1-2-2-1-1-3

Distribution of even letters

A	D	F	G	V	X
0	2	3	1	1	3

0-2-3-1-1-3

Fig. 69 normal

(Odd letters θ_1's, even letters as θ_2's)

$1\ (3) + 2\ (11) + 2\ (3) + 1\ (8) + 1\ (11) + 3\ (6) = 68;$ deduct 1/6 $= 57$

$0\ (4) + 2\ (10) + 3\ (11) + 1\ (5) + 1\ (4) + 3\ (1)$ $= 65$

$\overline{122}$

Fig. 69 reversed

(Even letters as θ_1's, odd letters as θ_2's)

$0\ (3) + 2\ (11) + 3\ (3) + 1\ (8) + 1\ (11) + 3\ (6) = 68;$ deduct 1/6 $= 57$

$1\ (4) + 2\ (10) + 2\ (11) + 1\ (5) + 1\ (4) + 3\ (1)$ $= 58$

$\overline{115}$

FIGURE 71.

Beginning with 21st position, the alternation is of type $\theta_1 \rightarrow \theta_2 \rightarrow \theta_1$; hence it is of the "+" type. Again the reversal in type of alternation occurs in passing from the 2d set of 10 letters to the 3d set, and this indicates that column 2 of the transposition rectangle ends somewhere near the 20th letter. But, fortunately, this time the exact location of the break is definitely indicated: the simultaneous appearance of V and X in the sequent positions 22 and 23 leads to the idea that letter 22 marks the end of column 2 and letter 23 marks the beginning of column 3. <u>There is nothing of an absolute nature in this point</u>: it is merely an indication based upon probabilities and does not constitute a conclusive proof by any means. Now if there is this definite break at the end of 22 letters it means that columns 1 and 2 must each contain 11 letters. The calculations have heretofore been based upon sections of 10 letters and the results are therefore modified as shown in the following calculation:

FIRST SECTION (Letters 1-11)

	1	2	3	4	5	6	7	8	9	10	11
III.	D	A	G	A	A	F	G	A	G	V	D
XI.	V	F	D	D	V	A	X	G	D	A	D

Distribution of odd letters

A D F G V X

1-5-0-3-2-1

Distribution of even letters

A D F G V X

5-1-2-1-1-0

Weighted values of distributions:

On basis of Fig. 69 normal (odd letters as θ_1's, even letters as θ_2's):

1 (3) + 5 (11) + 0 (3) + 3 (8) + 2 (11) + 1 (6) = 110; deduct 1/6 = 92

5 (4) + 1 (10) + 2 (11) + 1 (5) + 1 (4) + 0 (1) = 62 62

Total 154

On basis of Fig. 69 reversed (even letters as θ_1's, odd letters as θ_2's):

5 (3) + 1 (11) + 2 (3) + 1 (8) + 1 (11) + 0 (6) = 51; deduct 1/6 = 42

1 (4) + 5 (10) + 0 (11) + 3 (5) + 2 (4) + 1 (1) = 78 78

Total 120

The type of alternation is $\theta_1 \rightarrow \theta_2 \rightarrow \theta_1$, or "+".

SECOND SECTION (Letters 12-22)

	12	13	14	15	16	17	18	19	20	21	22
III.	A	F	G	G	X	F	D	X	D	F	V
XI.	F	G	G	G	G	F	G	D	D	F	X

Distribution of odd letters

A D F G V X

0-1-5-3-0-1

Distribution of even letters

A D F G V X

1-3-1-4-1-2

Weighted values of distributions:

On basis of Fig. 69 normal (odd letters as θ_1's, even letters as θ_2's):

0 (3) + 1 (11) + 5 (3) + 3 (8) + 0 (11) + 1 (6) = 56; deduct 1/6 = 47

1 (4) + 3 (10) + 1 (11) + 4 (5) + 1 (4) + 2 (1) = 71 71
Total 118

On basis of Fig. 69 reversed (even letters as θ_1's, odd letters as θ_2's):

1 (3) + 3 (11) + 1 (3) + 4 (8) + 1 (11) + 2 (6) = 94; deduct 1/6 = 78

0 (4) + 1 (10) + 5 (11) + 3 (5) + 0 (4) + 1 (1) = 81 81
Total 159

Since the best values are obtained on the basis of Fig. 69 reversed, the type of alternation for the 2d section of 11 letters is therefore again $\theta_1 \rightarrow \theta_2 \rightarrow \theta_1$, or "+".

THIRD SECTION (Letters 23-33)

	23	24	25	26	27	28	29	30	31	32	33
III.	V	X	G	F	X	F	D	X	D	D	A
XI.	X	D	A	F	D	D	X	G	G	A	V

Distribution of odd letters

A D F G V X

2-3-0-2-2-3

Distribution of even letters

A D F G V X

1-3-3-1-0-2

Weighted values of distributions:

On basis of Fig. 69 normal (odd letters as θ_1's, even letters as θ_2's):

2 (3) + 3 (11) + 0 (3) + 2 (8) + 2 (11) + 3 (6) = 95; deduct 1/6 = 79

1 (4) + 3 (10) + 3 (11) + 1 (5) + 0 (4) + 2 (1) = 74 74
Total 153

On basis of Fig. 69 reversed (even letters as θ_1's, odd letters as θ_2's):

1 (3) + 3 (11) + 3 (3) + 1 (8) + 0 (11) + 2 (6) = 65; deduct 1/6 = 54

2 (4) + 3 (10) + 0 (11) + 2 (5) + 2 (4) + 3 (1) = 59 59
Total 113

Since the best values are obtained on the basis of Fig. 69 normal, the type of alternation for the 3d section of 11 letters is $\theta_1 \rightarrow \theta_2 \rightarrow \theta_1$, or "+".

k. Now if columns 1 and 2 contain 11 letters, and the total number of letters is 186, the transposition rectangle obviously has 17 columns, there being 16 long columns of 11 letters and one short column of 10 letters [(17 x 11) - 1 = 186].

l. There is another cryptogram which also contains but one short column, viz, VII, of 254 letters, [(17 x 15) - 1 = 254]. The columns of this cryptogram contain 4 more letters than the corresponding columns of III and XI. Assuming, momentarily, the last column to be the short one, cryptogram VII may be added to the superposition of III and XI, provided those sets of 4 additional letters are accounted for. This has been done in Fig. 72. In that figure the 4 extra letters pertaining to cryptogram VII are shown as falling under the last letters of the columns of cryptograms III and XI, but this is only an arbitrary placement. It is sufficient to place these extra letters in such positions as will make the first one of the series begin in an even position.

m. Since the transposition rectangle is now known to be 17 columns wide, the data in Fig. 69 may be enlarged to correspond to this information For example, whereas in originally constructing Fig. 69 the first column of cryptogram I was assumed to have only 8 letters (to correspond to a key of 25 numbers), it may now be extended to a column of 12 letters, and so on. The additional portions used to make the distributions in Fig. 74 are shown underlined in Fig. 73.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
III.	D	A	G	A	A	F	G	A	G	V	D	A	F	G	G	X	F	D	X	D	F	V
XI.	V	F	D	D	V	A	X	G	D	A	D	F	G	G	G	G	F	G	D	D	F	X
VII.	G	A	F	G	F	F	X	F	V	F	G	A	G	G	X	D	X	X	D	D	F	A
								F	X	A	V								G	V	D	D

	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
III.	V	X	G	F	X	F	D	X	D	D	A	G	A	D	D	G	V	A	D	D	V	D
XI.	X	D	A	F	D	D	X	G	G	A	V	G	A	G	D	V	D	F	D	F	D	D
VII.	V	D	V	F	F	A	D	A	V	A	V	A	D	A	A	F	V	F	D	V	F	D
								F	V	G	G								X	F	X	X

	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66
III.	D	G	A	F	G	A	V	G	D	G	X	D	D	D	A	V	F	V	D	D	F	D
XI.	D	G	A	F	A	F	D	A	A	A	G	V	A	V	F	G	G	V	A	D	D	G
VII.	G	D	X	D	D	F	V	D	F	F	X	V	A	D	X	V	A	X	D	V	X	A
								D	V	F	X								F	F	V	D

	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88
III.	A	A	A	A	D	X	A	G	D	X	A	G	G	D	D	A	V	G	V	F	G	D
XI.	D	D	F	G	F	V	D	D	A	D	F	G	A	F	D	F	V	D	D	F	V	V
VII.	F	D	G	X	F	D	G	F	D	D	F	A	A	F	V	F	F	V	X	D	G	F
								V	D	V	V								D	D	V	A

	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110
III.	V	F	V	D	G	G	X	G	G	A	F	F	V	F	D	A	X	G	D	D	D	G
XI.	V	A	D	A	G	D	X	F	X	X	X	F	F	D	X	G	D	F	D	G	F	D
VII.	D	D	F	D	D	D	X	F	F	A	G	A	A	G	V	D	G	G	V	D	F	G
								F	X	F	X								G	G	X	D

	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132
III.	D	A	F	D	A	D	G	G	A	D	D	G	D	X	A	F	V	D	F	D	X	F
XI.	D	F	G	D	A	G	F	A	A	G	G	A	D	X	D	G	V	D	G	A	V	G
VII.	F	D	F	V	A	F	F	G	F	X	G	G	D	G	G	D	D	A	V	D	X	A
								D	A	X	D								D	F	A	F

	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154
III.	V	G	D	D	V	A	V	F	D	D	D	V	F	A	G	D	F	F	F	X	A	A
XI.	V	D	F	D	D	F	X	G	A	G	X	F	G	V	F	V	V	D	G	V	D	X
VII.	V	F	X	D	D	X	V	A	G	D	V	X	D	G	X	X	D	V	F	V	F	D
								V	D	D	F								D	D	D	A

	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176
III.	D	F	A	D	G	G	V	F	D	A	V	D	G	X	F	V	D	A	A	V	G	D
XI.	D	F	F	F	X	G	X	G	X	A	G	A	G	V	G	D	V	V	X	G	F	V
VII.	A	F	D	F	X	D	X	G	D	A	A	D	V	D	D	V	A	D	D	V	D	V
								F	V	D	V								A	V	D	G

	177	178	179	180	181	182	183	184	185	186
III.	X	F	G	G	D	D	X	G	D	A
XI.	D	X	D	D	X	F	V	D	D	X
VII.	A	F	V	F	X	F	A	A	V	D
							D	F	V	D

FIGURE 72.

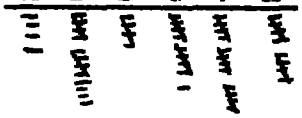
Cryptogram	Length	Letters taken	Cryptogram	Length	Letters taken
I	212	VDDGGGVFDFVD	VII	254	GAFGFFXFVFGFXA
II	108	VDAAVD	VIII	144	DGVVGFXG
III	186	DAGAAFGAGV	IX	182	GDDDDXVGVD
IV	110	ADXVFX	X	130	DGDDFVF
V	202	DFXFDDVVVDX	XI	186	VFDDVAXGDA
VI	120	GDGFXAG	XII	224	XFDFXVVDVDAVD

FIGURE 73.

The new frequency weights are therefore as follows:

Odd (1st, 3d, ...) letters

A D F G V X

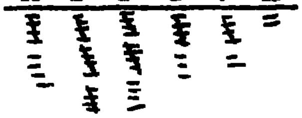


4 14 5 11 15 10

Total = 59.

Even (2d, 4th, ...) letters

A D F G V X



9 15 14 8 7 2

Total = 55.

FIGURE 74.

Since the two totals are quite close together, no correction need be made of the nature of that made in preceding calculations, where 1/6 was deducted from the total values of odd letters.

n. Beginning with position 23, in the case of cryptograms III and XI the next 11 letters, and in the case of cryptogram VII the next 15 letters are clearly of the "+" type of alternation. The data are as follows:

	23	24	25	26	27	28	29	30	31	32	33
III.	V	X	G	F	X	F	D	X	D	D	A
XI.	X	D	A	F	D	D	X	G	G	A	V
VII.	V	D	V	F	F	A	D	A	V	A	V
								F	V	G	G

Distribution of odd letters

A D F G V X

2-4-1-3-7-3

Distribution of even letters

A D F G V X

4-4-5-2-0-2

Weighted values of distributions:

On basis of Fig. 74 normal (odd letters as θ_1's, even letters as θ_2's):

$2\ (4) + 4\ (14) + 1\ (5) + 3\ (11) + 7\ (15) + 3\ (10) = 237$

$4\ (9) + 4\ (15) + 5\ (14) + 2\ (8) + 0\ (7) + 2\ (2) = 186$

Total 423

On basis of Fig. 74 reversed (even letters as θ_1's, odd letters as θ_2's):

$4\ (4) + 4\ (14) + 5\ (5) + 2\ (11) + 0\ (15) + 2\ (10) = 139$

$2\ (9) + 4\ (15) + 1\ (14) + 3\ (8) + 7\ (7) + 3\ (2) = 171$

Total 310

Since the greatest total is obtained on the basis of Fig. 74 normal, the type of alternation for the 3d section of letters is $\theta_1 \rightarrow \theta_2 \rightarrow \theta_1$, or "+".

o. Continuing the foregoing process with the letters beyond position 33, the data are as follows:

	34	35	36	37	38	39	40	41	42	43	44
III.	G	A	D	D	G	V	A	D	D	V	D
XI.	G	A	G	D	V	D	F	D	F	D	D
VII.	A	D	A	A	F	V	F	D	V	F	D
								X	F	X	X

Distribution of odd letters

A D F G V X

3-8-1-0-3-2

Distribution of even letters

A D F G V X

3-5-5-4-2-1

Weighted values of distributions:

On basis of Fig. 74 normal (odd letters as θ_1's, even letters as θ_2's):

$3\ (4) + 8\ (14) + 1\ (5) + 0\ (11) + 3\ (15) + 2\ (10) = 194$

$3\ (9) + 5\ (15) + 5\ (14) + 4\ (8) + 2\ (7) + 1\ (2) = 220$

Total 414

On basis of Fig. 74 reversed (even letters as θ_1's, odd letters as θ_2's):

$3\ (4) + 5\ (14) + 5\ (5) + 4\ (11) + 2\ (15) + 1\ (10) = 191$

$3\ (9) + 8\ (15) + 1\ (14) + 0\ (8) + 3\ (7) + 2\ (2) = \underline{189}$

Total ...380

Since the distribution begins here with an even-numbered position (34), and the greatest total is obtained on the basis of Fig. 74 normal, hence the alternation for the 4th section or column is of the type $\theta_2 \rightarrow \theta_1 \rightarrow \theta_2$. or "-".

p. (1) The data for letters beyond position 44:

	45	46	47	48	49	50	51	52	53	54	55
III.	D	G	A	F	G	A	V	G	D	G	X
XI.	D	G	A	F	A	F	D	A	A	A	G
VII.	G	D	X	D	D	F	V	D	F	F	X
								D	V	F	X

Distribution of odd letters

A	D	F	G	V	X

4-5-1-3-3-4

Distribution of even letters

A	D	F	G	V	X

3-4-6-4-0-0

Weighted values of distributions:

On basis of Fig. 74 normal (odd letters as θ_1's, even letters as θ_2's):

$4\ (4) + 5\ (14) + 1\ (5) + 3\ (11) + 3\ (15) + 4\ (10) = 209$

$3\ (9) + 4\ (15) + 6\ (14) + 4\ (8) + 0\ (7) + 0\ (2) = \underline{203}$

Total ...412

On basis of Fig. 74 reversed (even letters as θ_1's, odd letters as θ_2's):

$3\ (4) + 4\ (14) + 6\ (5) + 4\ (11) + 0\ (15) + 0\ (10) = 142$

$4\ (9) + 5\ (15) + 1\ (14) + 3\ (8) + 3\ (7) + 4\ (2) = \underline{178}$

Total 320

Since the distribution starts with an odd position (45) and the greatest total is obtained on the basis of Fig. 74 normal, the type of alternation for the 5th section or column is $\theta_1 \rightarrow \theta_2 \rightarrow \theta_1$, or "+".

q. The types of alternation for the first 5 columns, which are all long columns, is therefore + + + - +. Since cryptograms III and XI contain but one short column, it is advisable to be on the lookout for it as the work progresses. It is possible to continue with the process detailed above. For example, the calculations for the next or 6th section of 11 letters are shown below:

	56	57	58	59	60	61	62	63	64	65	66
III.	D	D	D	A	V	F	V	D	D	F	D
XI.	V	A	V	F	G	G	V	A	D	D	G
VII.	V	A	D	X	V	A	X	D	V	X	A
								F	F	V	D

Distribution of odd letters

A	D	F	G	V	X

5-4-4-1-1-2

Distribution of even letters

A	D	F	G	V	X

1-7-1-2-8-1

Weighted values of distributions:

On basis of Fig. 74 normal (odd letters as θ_1's, even letters as θ_2's):

5 (4) + 4 (14) + 4 (5) + 1 (11) + 1 (15) + 2 (10) = 142

1 (9) + 7 (15) + 1 (14) + 2 (8) + 8 (7) + 1 (2) = 202

Total.....344

On basis of Fig. 74 reversed (even letters as θ_1's, odd letters as θ_2's):

1 (4) + 7 (14) + 1 (5) + 2 (11) + 8 (15) + 1 (10) = 259

5 (9) + 4 (15) + 4 (14) + 1 (8) + 1 (7) + 2 (2) = 180

Total 439

Since the distribution starts with an even position (56) and the greatest total is obtained on the basis of Fig. 74 reversed, the type of alternation for the 6th section or column is $\theta_1 \rightarrow \theta_2 \rightarrow \theta_1$, or "+".

r. But perhaps advantage should be taken of the availability of additional cryptograms. For example, cryptogram V, of 202 letters, has 2 short columns [(17 x 12) - 2 = 202], whereas the cryptograms thus far dealt with each have but one. That is, cryptogram V has one short column in common with cryptograms III, XI, and VII, and one additional short column not possessed by the latter. Can this additional short column of cryptogram V be located?

s. Suppose column 1 of cryptogram V is the additional short column. Then the letters of this column are F X F X F F F V A G F D. These letters when evaluated on the basis of Fig. 74 normal yield a total of 77; when weighted on the basis of Fig. 74 reversed, a total of 144. The calculation is as follows:

Distribution of odd letters

A	D	F	G	V	X

1-0-5-0-0-0

Distribution of even letters

A	D	F	G	V	X

0-1-1-1-1-2

On basis of Fig. 74 normal:

$$1\ (4) + 5\ (5) + 1\ (15) + 1\ (14) + 1\ (8) + 1\ (7) + 2\ (2) = 77$$

On basis of Fig. 74 reversed:

$$1\ (9) + 5\ (14) + 1\ (14) + 1\ (5) + 1\ (11) + 1\ (15) + 2\ (10) = 144$$

According to this calculation column 2 of cryptogram V seems to correspond to the type of alternation $\theta_2 \rightarrow \theta_1 \rightarrow \theta_2$, that is "-". But from previous work it is fairly certain that column 2 is of the "+" type. Hence, column 1 of cryptogram V is not the additional short column of that message. Assuming column 2 to be the extra short column, no such contradiction is obtained, for the calculation is as follows:

Assuming column 2 to be short, the letters of column 3 are X A V D A G F D V D F G. The weighted frequency value for a $\theta_1 \rightarrow \theta_2 \rightarrow \theta_1$ sequence (letters X V A F V G and A D G D D F) = 136. The weighted frequency value for a $\theta_2 \rightarrow \theta_1 \rightarrow \theta_2$ sequence (letters A D G D D F and X V A F V G) = 109. Hence column 3 is a "+" column, which is consistent with the formula + + + - + for columns 1 to 5, as previously ascertained.

If all the foregoing reason is correct, and column 2 is the additional short column for cryptogram V, it must be the next to the last column of the transposition rectangle. Since it is a "+" column, the last column must be a "-" one; therefore, there are 9 "-" columns and 8 "+" columns. This definitely determines that the "-" columns are the odd ones, the "+" columns the even ones, since in an odd-width rectangle there is one more odd column than even columns.

t. The single short column which is common to cryptograms III, XI, and VII is one of the columns beyond column 5. Assuming each possibility in turn, there is obtained for the type of alternation in each column the distributions of "+" and "-" shown in Fig. 75.

u. The correct assumption must satisfy the following conditions:

(a) There must be 9 "-" and 8 "+" columns.

(b) The short column must be "-".

Only assumptions (3) and (5), in which column 8 and column 10 are short columns, satisfy these conditions. Therefore, column 2 is followed by either column 8 or 10. Testing the combination 2-8 for monoalphabeticity of bipartite pairs, the distribution shown in Fig. 76 is obtained. When combination 2-10 is tested, the distribution shown in Fig. 77 is obtained. Obviously, the 2-8 combination is the better.

Assumption		Column 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	Summation of +'s and -'s
(1)	6th short ...	+	+	+	-	+	+	+	+	-	+	+	+	-	-	-	-	-	10+, 7-
(2)	7th short ...	+	+	+	-	+	+	-	+	-	+	+	+	-	-	-	-	-	9+, 8-
(3)	8th short ...	+	+	+	-	+	+	-	-	-	+	+	+	-	-	-	-	-	8+, 9-
(4)	9th short ...	+	+	+	-	+	+	-	-	+	+	+	+	-	-	-	-	-	9+, 8-
(5)	10th short ...	+	+	+	-	+	+	-	-	+	-	+	+	-	-	-	-	-	8+, 9-
(6)	11th short ...	+	+	+	-	+	+	-	-	+	-	-	+	-	-	-	-	-	7+,10-
(7)	12th short ...	+	+	+	-	+	+	-	-	+	-	-	-	-	-	-	-	-	6+,11-
(8)	13th short ...	+	+	+	-	+	+	-	-	+	-	-	-	+	-	-	-	-	7+,10-
(9)	14th short ...	+	+	+	-	+	+	-	-	+	-	-	-	+	+	-	-	-	8+, 9-
(10)	15th short ...	+	+	+	-	+	+	-	-	+	-	-	-	+	+	+	-	-	9+, 8-
(11)	16th short ...	+	+	+	-	+	+	-	-	+	-	-	-	+	+	+	+	-	10+, 7-
(12)	17th short ...	+	+	+	-	+	+	-	-	+	-	-	-	+	+	+	+	+	11+, 6-

FIGURE 75.

	A	D	F	G	V	X
A						
D		-			-	-
F				≡	≡	
G	=	≡				
V						
X			-		=	

$E(\phi) = .0667 \times 17 \times 16 = 18.14$

$\phi = 22$

FIGURE 76.

	A	D	F	G	V	X
A						
D		-			-	-
F		=	=		-	-
G	-	-	-	-		-
V						
X		-		-	-	

$E(\phi) = .0667 \times 17 \times 16 = 18.14$

$\phi = 4$

FIGURE 77.

v. It is possible by introducing cryptograms with additional short columns to determine more of the key. Thus, it was found by using cryptograms XII and VI that the first 3 numbers of the transposition key are 16-5-7. But the process of anagramming will yield the solution at least as rapidly. In this process, of course, advantage may be taken of the fact that the columns have been classified into the "+" and "-" types and no combinations of two "+" or two "-" columns need be tested, since only combinations of the type "+ -" or "- +" are permissible.

w. The final transposition key and the substitution checkerboard are shown in Fig. 78.

16	5	7	6	9	3	14	1	13	11	17	10	4	12	15	2	8
V	I	K	I	N	G	S	C	R	O	W	N	H	O	T	E	L

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

FIGURE 78.

x. All the foregoing details concern a case in which the transposition rectangle has an odd number of columns. Now if the rectangle contains an even number of columns, this type of solution is, of course, still applicable, and in fact is easier, since the letters of the ~~text~~ of the respective sections do not have to be distributed into odd and even letters. It is only necessary to identify a section as being composed of initial components or of final components. This analysis then produces a series of sections corresponding in number with the number of columns in the transposition rectangle. This number will, of course, be even. By a careful study of where alternations in composition of components (θ_1 or θ_2) occur, the division of the text into sections corresponding to long and short columns can be accomplished. The remaining steps are obvious and follow the lines elucidated in Par. 39e-j.

y. The entire structure upon which this general solution rests is destroyed if the substitution checkerboard has been consciously manipulated to impart a homogeneity to the sums of the weighted frequencies of the letters in its rows and columns. For example, note the following checkerboard, which is not "perfect" but gives fairly homogeneous frequencies in its rows and columns.

	A	D	F	G	V	X	
A	S 58	Q 3	L 36		I 76		173
D		T 90		W 14	C 33	P 27	164
F	G 18		A 72			N 76	166
G		V 13	J 2	E 126	B 11	K 3	155
V	R 83	Y 21	F 30			M 25	159
X	X 5	D 40	Z 1	U 30	O 74	H 33	183
	164	167	141	170	194	164	

FIGURE 79.

SECTION IX

SOLUTION OF THE BIFID FRACTIONATING SYSTEM

44. Review of principles underlying the cryptographic method. - a. Several bifid fractionating systems have been explained in previous texts of this series.[1] In certain of these systems four basic steps are involved, two of substitution and two of transposition. Those steps may be briefly described as follows: (1) a process of decomposition (substitution), in which each plain-text letter is replaced by two components, θ_c^1 and θ_c^2, of a bifid or bipartite alphabet; (2) a process of separation (transposition), in which the $\theta^1\theta_c^2$ components originally paired together are separated; (3) a process of recombination (transposition), in which the separated components are combined to form new pairs; (4) a process of recomposition (substitution), in which each new pair of components is given a letter value according to the original or a different bifid alphabet.

b. One of the simplest and most efficient of the fractionating systems of the foregoing nature is that in which the processes involved are applied to groupings or periods of fixed length, as exemplified below. Let the bipartite alphabet be based upon the 25-cell substitution checkerboard shown in Fig. 80. Let the message to be enciphered be ONE PLANE REPORTED LOST AT SEA. Let it also be assumed that, by

[1]See Special Text No. 166, Advanced Military Cryptography, Sec. XI and Military Cryptanalysis, Part I, Sec. IX.

(2)

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

FIGURE 80.

preagreement between correspondents, periods of 5 letters will constitute the units of encipherment. The bipartite equivalents of the plain-text letters are set down vertically below the letters. Thus:

```
ONEPL ANERE PORTE DLOST ATSEA
41344 11323 44223 34442 12431
23331 23333 32323 21252 22532
```

Recombinations are effected horizontally within the periods, by joining components in pairs, the first period yielding the pairs 41, 34, 42, 33, 31. These pairs are then replaced by letters from the original checkerboard, yielding the following:

```
ON EP L   AN ER E   PO RT E   DL OS T   AT SE A
41 34 4   11 32 3   44 22 3   34 44 2   12 43 1
23 33 1   23 33 3   32 32 3   21 25 2   22 53 2
LH OE B   MD DE E   QT ER R   HQ TA W   AP AG D
```

45. General principles underlying the solution. - a. It will be noted that the periods in the foregoing example contain an odd number of letters. The result of adopting odd-length periods is to impart a much greater degree of cryptographic security to the system than is the case when even-length periods are involved. This point is worth while elaborating upon to make its cryptanalytic significance perfectly clear. Note what happens when an even period is employed:

```
ONEPLA   NEREPO   RTEDLO   ...
413441   132344   223344   ...
233312   333332   323212   ...
LHLREA   NRQEED   TEQDDA
```

Now if each 6-letter cipher group is split in the middle into two sections and the letters are taken alternately from each section (Ex. L H L R E A → L R H E L A) the result is exactly the same as is obtained in case a simple digraphic encipherment were in effect with the 2-square checkerboard shown in Fig. 81.

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
J	I	H	Q	Y
F	G	K	S	Z

O N E P L A - N E R E P O ...
L R H E L A   N E R E Q D ...

FIGURE 81.

For example, $ON_p = LR_c$; $EP_p = HE_{cl}$ and so on. Encipherment of this sort brings about a fixed relationship between the plain-text digraphs and their cipher equivalents, so that the solution of a message of this type falls under the category of the cryptanalysis of a case of simple digraphic substitution, once the length of the period has been established.[2] The latter step can readily be accomplished, as will be seen presently. In brief, then, it may be said that in this system when encipherment is based upon even periods the cipher text is purely and simply digraphic in character, each plain-text digraph having one and only one cipher-text digraph as its equivalent.

b. But the latter statement is no longer true in the case of odd periods. Note, in the example under Par. 44b, that the cipher equivalent of the 1st plain-text digraph, of the 1st group, ON, is composed of the initial and final components of the letter L_c, the final component of the letter O_c, and the initial component of the letter E_c. That is, three different cipher letters, L, O, and E, are involved in the

---

[2] An example of the solution of a cryptogram of this type was given in Military Cryptanalysis, Part I, Sec. IX.

composition of the cipher equivalent of one plain-text digraph, ON. Observe now, in the following examples, that variants may be produced for the digraph ON_p.

ON EP L	ON TH E	ON CR U	PR ON G	CO NT I	PO NG I	AT IO N
41 34 4	41 23 3	41 22 1	42 41 2	24 12 2	44 12 2	12 24 1
23 33 1	23 24 3	23 13 4	33 23 5	12 32 4	32 35 4	22 42 3
LH OE B	LR DD P	LT AB H	OL RD K	IA CR I	QA RR Y	AI AI R

c. The foregoing examples fall into two classes. In the first, where the O of ON_p falls in an odd position in the period, the first letter of the trigraphic cipher equivalent must be an L_c, the second must be one of the 5 letters in the 2d column of the substitution checkerboard, the third must be one of the 5 letters in the 3d row of the checkerboard. Therefore, L_c may combine with 5 x 5 or 25 pairs of letters to form the 2d and 3d letters of the 3-letter equivalent of ON_p. In the other class, where the O of ON_p falls in an even position in the period, the 1st letter of the equivalent must be one of the 5 letters in the 4th column of the checkerboard, the second must be one of the 5 letters in the 1st column, and the 3d letter must be R_c. Therefore, R_c may combine with 5 x 5 or 25 pairs of letters to form the 1st and 2d letters of the 3-letter equivalent of ON_p in this position in the period. Hence, ON_p may be represented by 50 trigraphic combinations; the same is true of all other plain-text digraphs. Now if the system based upon even periods is considered as a simple digraphic substitution, the foregoing remarks lead to characterizing the system based upon odd periods as a special type of digraphic substitution with variants, in which 3 letters represent 2 plain-text letters.

d. However, further study of the odd-period system may show that there is no necessity for trying to handle it as a digraphic system with variants, which would be a rather complex affair. Perhaps the matter can be simplified. Referring again to the example of encipherment in Par. 44b:

```
O N  E P  L    A N  E R  E    P O  R T  E    D L  O S  T    A T  S E  A
4 1  3 4  4    1 1  3 2  3    4 4  2 2  3    3 4  4 4  2    1 2  4 3  1
2 3  3 3  1    2 3  3 3  3    3 2  3 2  3    2 1  2 5  2    2 2  5 3  2
L H  O E  B    M D  D E  E    Q T  E R  R    H Q  T A  W    A P  A G  D
```

Now suppose that only the cipher letters are at hand, and that the period is known. The 1st cipher letter is L, and it is composed of two numerical components that come from the 1st and 2d positions in the upper row of components in the period. These components are not known, but whatever they are the first of them is the 1st component of L, the second of them is the 2d component of L. Therefore, for cryptanalytic purposes, the actual but unknown numerical components, may be represented by the symbols L_1 and L_2, the former referring to the row coordinate of the substitution checkerboard, the latter to the column coordinate. The same thing may be done with the components of the 2d cipher letter, the 3d, 4th, and 5th, the respective components being placed into their proper positions in the period. Thus:

$$\begin{array}{ll} \text{Components} & \left\{\begin{array}{ccccc} L_1 & L_2 & H_1 & H_2 & O_1 \\ \underline{O_2} & \underline{E_1} & \underline{E_2} & \underline{B_1} & \underline{B_2} \end{array}\right. \\ \text{Cipher .....} & \begin{array}{ccccc} L & H & O & E & B \end{array} \end{array}$$

Now let the actual plain-text letters be set into position, as shown at the right in the two diagrams below.

$$\begin{array}{ll} \text{Plain text ...} & \begin{array}{ccccc} O & N & E & P & L \end{array} \\ \text{Components ...} & \left\{\begin{array}{ccccc} 4 & 1 & 3 & 4 & 4 \\ 2 & 3 & 3 & 3 & 1 \end{array}\right. \\ \text{Cipher ....} & \begin{array}{ccccc} L & H & O & E & B \end{array} \end{array} \qquad \begin{array}{ccccc} O & N & E & P & L \\ \hline L_1 & L_2 & H_1 & H_2 & O_1 \\ O_2 & E_1 & E_2 & B_1 & B_2 \\ \hline L & H & O & E & B \end{array}$$

By comparing the two diagrams it becomes obvious that L_1, H_2 and O_1 all represent the coordinate 4; H_1, E_1, E_2, and B_1 all represent the coordinate 3, and so on. If this equivalency were known for all the 50 combinations of the 25 letters with subscript 1 or 2 there would be no problem, for the text of a cryptogram could be reduced to 25 pairs of digits representing monoalphabetic encipherment. But this equivalency is not known in the case of a cryptogram that is to be solved; basically the problem is to establish the equivalency.

e. It is obvious that the vertical pair of components $\begin{matrix}L_1\\O_2\end{matrix}$ represents O_p, the vertical pair $\begin{matrix}L_2\\E_1\end{matrix}$ represents N_p, and so on. The complete example therefore becomes:

Plain ..	O	N	E	P	L	A	N	E	R	E	P	O	R	T	E	D	L	O	S	T	A	T	S	E	A
Com-	L_1	L_2	H_1	H_2	O_1	M_1	M_2	D_1	D_2	D_1	Q_1	Q_2	T_1	T_2	E_1	H_1	H_2	Q_1	Q_2	T_1	A_1	A_2	P_1	P_2	A_1
ponents.	O_2	E_1	E_2	B_1	B_2	D_2	E_1	E_2	E_1	E_2	E_2	R_1	R_2	R_1	R_2	T_2	A_1	A_2	W_1	W_2	A_2	G_1	G_2	D_1	D_2
Cipher .	L	H	O	E	B	M	D	D	E	E	Q	T	E	R	R	H	Q	T	A	W	A	P	A	G	D

f. Note that a plain-text letter in an odd position in the period has its components in the order $\theta_1\theta_2$; in an even position in the period the components of a plain-text letter are in the order $\theta_2\theta_1$. For example, note the O_p in the 1st period $\begin{pmatrix}= L_1\\ Q_2\end{pmatrix}$ and in the 3d period $\begin{pmatrix}= Q_2\\ R_1\end{pmatrix}$. This distinction must be retained since the component indicators for rows and columns are not interchangeable in this system. From this it follows that the vertical pairs of components representing a given plain-text letter are of two classes: $\theta_1\theta_2$ and $\theta_2\theta_1$, and the two must be kept separate in cryptanalysis.

g. Now consider the equivalent of O_p in the 1st period. It is composed of $\begin{matrix}L_1\\O_2\end{matrix}$. This is only one of a number of equivalents for O_p in an odd position in the period. The row of the substitution checkerboard indicated by L_1 may be represented by 4 other components, since that row contains 5 letters. Therefore the upper component of the $\frac{\theta_1}{\theta_2}$ equivalent of O_p may be any one of 5 letters. The same is true of the lower component. Hence, O_p in an odd position in the period may be represented by any one of 5 x 5 = 25 combinations of vertical components in the sequence $\theta_1 \rightarrow \theta_2$. O_p in an even position in the period may be represented by any one of a similar number of combinations of vertical components in the reverse sequence $\theta_2 \rightarrow \theta_1$. Thus, disregarding the position in the period, this system may be described as a monoalphabetic substitution with variants, in which every plain-text letter may be represented by any one of 50 different component-pairs. But in studying an actual cryptogram in this system, since the position (odd or even) occupied by a cipher letter in the period is obvious after the length of the period has been established, a proper segregation of the cipher letters will permit of handling the cipher letters in the two classes referred to above, in which case one has to deal with only 25 variants for each plain-text letter. Obviously, the 25 variants are related to one another by virtue of their having been produced from a single checkerboard of but 25 letters. This relationship can be used to good advantage in reconstructing the checkerboard in the course of the solution and will be discussed in its proper place.

h. Now if the foregoing encipherment is studied intently several important phenomena may be observed. Note, for instance, how many times either the θ_1 or the θ_2 component coincides with the plain-text letter of which it is a part. In the very first period the O_p has an O_2 under it; in the same period the E_p has an E_2 under it. The same phenomenon is observed in columns 3 and 5 of the 2d period, in column 3 of the 3d period, and in column 1 of the 5th period. In column 5 of the 3d, 4th, and 5th periods the θ_1 components coincide with the respective plain-text letters involved. There are, in this short example, 9 cases of this sort, giving rise to instances of what seems to be a sort of self-encipherment of plain-text letters. How does this come about? And is it an accident that all these cases involve plain-text letters in odd positions in the periods?

i. If the periods in the foregoing example in subparagraph e are studied closely the following observations may be made. Because of the mechanics of encipherment in this system the 1st cipher letter and the 1st plain-text letter must come from the same row in the substitution checkerboard. Since there are only 5 letters in a row in the checkerboard the probability that the two letters referred to will be identical is 1/5. (The identity will occur every time that the coordinate of the row in which the 2d plain-text letter stands in the checkerboard is the same as the coordinate of the column in which the 1st plain-text letter stands.) The same general remark applies to the 2d cipher letter and the 3d plain-text letter; as well as to the 3d cipher letter and the 5th plain-text letter: in these cases the two letters must come from the same row in the checkerboard and the probability that they will be identical is likewise 1/5. (The identity in the former case will occur every time that the coordinate of the row in which the 4th plain-text letter stands in the checkerboard is the same as that of the column in which the 3d plain-text letter stands; in the latter case the identity will occur every time that the coordinate of the column in which the 1st plain-text letter stands is the same as that of the column in which the 5th plain-text letter stands.) The last of the foregoing sources of identity is exemplified in only 4 of the 9 cases mentioned in subparagraph h above. These involve the 5th plain-text letter in the 3d, 4th and 5th periods, and the 1st letter in the 5th period, wherein it will be noted that the θ_1 component standing directly under the plain-text letter is identical with the latter in each case.

j. But how are the other 5 cases of identity brought about? Analysis along the same lines as indicated above will be omitted. It will be sufficient to observe that in each of those cases it is the θ_2 component which is identical with the plain-text letter involved, and again the probability of the occurrence of the phenomenon in question is 1/5.

k. Since the probability of the occurrence of the event in question is 1/5 for θ_1 components and 1/5 for θ_2 components, the total probability from either source of identity is 2/5. This probability applies only to the letters occupying odd positions in the period, and it may be said that in 40% of all cases of letters in odd positions in the periods the one or the other of the two cipher components will be identical with the plain-text letter.

l. As regards the plain-text letters in even positions, analysis will show why only in a very few cases will either of the cipher components coincide with the plain-text letter to which they apply. Now the method of finding equivalents in the substitution checkerboard is to take the 1st component as the row coordinate indicator and the 2d component as the column indicator; a reversal of this order will give wholly different letters, except in those 5 cases in which both components are identical. (The letters involved are those which occupy the 5 cells along the diagonal from the upper left-hand corner to the lower right-hand corner of the checkerboard.) Now in every case of a letter in an odd position in a perioc the two vertical components are in the $\theta_1\theta_2$ order, corresponding to the order in which they are normally taken in finding letter equivalents in the checkerboard. But in every case of a letter in an even position in a period, the two vertical components are in the order $\theta_2\theta_1$, which is a reversal of the normal order. It has been seen that in the case of letters in odd positions in the periods the probability that one of the components will coincide with the plain-text letter is 40%. The reason which led to this determination in the case of the odd letters is exactly the same as that in the case of letters in even positions, except that in the final recombination-substitution process, since the components in the even positions are in the $\theta_2\theta_1$ order, which is the reverse of the normal order, identity between one of the components and the plain-text letter can occur in only 1/5 of the 40% or 8% of the cases. It may be said then that in this system 48% of all the letters of the plain text will be "self-enciphered" and represented by one or the other of the two components; in the case of the letters in odd positions, the amount is 40%, in the case of letters in even positions, it is 8%.

m. Finally, what of the peculiar phenomenon to be observed in the case of the 1st column of the 5th period of the example in subparagraph h? Here is a case wherein the plain-text value of a pair of superimposed components is unmistakably indicated directly by the cipher components themselves. Studying the cipher group concerned it is noted that it contains 2 A_c's separated by one letter, that is, the A's are 2 intervals apart. This situation is as though the plain-text letter were entirely self-enciphered in this case. Now it is obvious that this phenomenon will occur in the case of periods of 5 letters every time that within a period a cipher letter is repeated at an interval of 2, for this will bring about the superimposition of a θ_1 and θ_2 with the same principal letter and therefore the plain-text letter is indicated directly. This question may be pertinent: how many times may this be expected to happen? Analysis along the lines already indicated will soon bring the answer that the phenomenon in question may be expected to happen 4 times out of 100 in the case of letters in odd positions and only 8 times out of 1000 in the case of letters in even positions. In the latter cases the letters involved are those falling in the diagonal sloping from left to right in the substitution checkerboard.

n. All of the foregoing phenomena will be useful when the solution of an example is undertaken. But before coming to such an example it is necessary to explain how to ascertain the period of a cryptogram to be solved.

46. Ascertaining the period. - a. There are several methods available for ascertaining the length of the period. The simplest, of course, is to look for repetitions of the ordinary sort. If the period is a short one, say 3, 5, 7 letters, and if the message is fairly long, the chances are good that a polygraph which occurs several times within the message will fall in homologous positions within two different periods and therefore will be identically enciphered both times. There will not be many such repetitions, it is true, but factoring the intervals between such as do occur will at least give some clue, if it will not actually disclose the length of the period. For example, suppose that a 7-letter repetition is found, the two occurrences being separated by an interval of 119. The factors of 119 are 7 and 17; the latter is unlikely to be the length of the period, the former, quite likely.

b. If a polygraph is repeated but its two occurrences do not fall in homologous positions in two periods, there will still be manifestations of the presence of repetition but the repeated letters will be separated by one or more intervals in the periods involved. The number of repeated letters will be a function of the length of the polygraph and the length of the period; the interval between the letters constituting the repetition will be a function of the length of the period and the position of the repeated polygraph in two periods in which the two polygraphs occur. Note what happens in the following example:

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

Cryptogram .. P N R G E T P E N N P B E T V I B D D R D L B D T X D L O T L D T D T

Here the plain text contains the trigraph END 4 times. The END_p in the
1 2 3 4 5 6 7
1st period gives rise to the cipher letters . N . . E . .; in the 2d
1 2 3 4 5 6 7
period this trigraph also produces . . N . . E . The interval between the N_c and the E_c is 3 in both cases. Two times this interval plus one gives the length of the period. In this case the initial letter of the repeated trigraph falls in an even position in the period in both occurrences. The END_p in the 3d period gives rise to the cipher letters
1 2 3 4 5 6 7
. . B . . . D; in the 4th period it also produces
1 2 3 4 5 6 7
. B . . . D . The interval between the B_c and the D_c is 4 in both cases. Two times this interval minus one gives the length of the period. In this case the initial letter of the repeated trigraph falls in an odd position in the period in both occurrences.

c. The foregoing properties of repetitions in this system afford a means of ascertaining the length of the period in an unknown example.

First, it is evident that a repeated trigraph in the plain text produces two different pairs of cipher equivalents according to whether the initial letter of the trigraph occurs in an odd or an even position in the period. The two letters constituting the repetition in the cryptogram will not be sequent but will be separated by an interval of 1, 2, 3, ... letters depending upon the length of the period. This interval, however, is half of the period plus or minus one.[3] Conversely, if in a cryptogram there are repetitions of pairs of letters separated by an interval x, it is probable that these repetitions represent repetitions of plain-text trigraphs which occupy homologous positions in the period. The interval x (between the letters constituting the repetition in the cipher text) then gives a good clue to the length of the period: p (length of period) = $2x \pm 1$.

d. A special kind of index is prepared to facilitate the search for repetitions of the nature indicated. If tabulating machinery is available, an alphabetically-arranged index showing say 10 succeeding letters after each A_c, B_c, C_c, ... Z_c is prepared for the cryptogram. Then this index is studied to see how many coincidences occur at various intervals under each letter. For example, under A_c one looks to see if there are 2 or more cases in which the same letter appears 2, 3, 4, ... intervals to the right of A, a record being kept of the number of such cases under each interval. The same thing is done with reference to B_c, C_c, and so on. The tallies representing coincidences may be amalgamated for all the letters A, B, C, ... Z, only the intervals being kept segregated. When

[3] The student must remember that the text is here concerned only with cases in which the period is odd. In the case of even periods the interval separating the 2 letters is always exactly half of the length of the period.

tabulating machinery is not available, the search for repetitions may be made by transcribing the cryptogram on two long strips of cross-section paper, juxtaposing the strips at A, B, C, ... Z, and noting the coincidences occurring 1, 2, 3, ... up to say 10 letters beyond the juxtaposed letters. For example, beginning with A_c, the two strips are juxtaposed with the 1st A on one against the 1st A on the other. Note is made of any coincidences found within 10 letters beyond the A's, and a record is kept of such coincidences according to intervals. Keeping one strip in position the other is slid along to the 2d A, and again coincidences are sought. All the A's are treated in this way, then the B's, C's, ... Z's. The record made of the coincidences may consist merely of a tally stroke written under the intervals 1, 2, 3, ... 10. That interval which occurs more frequently than all the others is probably the correct one. This interval times 2 plus or minus 1 is the length of the period. There are, therefore, only two alternatives. A choice between the two alternatives may then be made by transcribing the text or a portion of it according to each hypothesis. That transcription which will most often throw the two members constituting a repetition into one and the same period is most likely to be correct.

e. Finally, for ascertaining the period there is one method which is perhaps the most laborious but surest. It has been pointed out that this system reduces to one that may be described as monoalphabetic substitution with variants. If the cipher text is transcribed into θ_1 and θ_2 components according to various assumed periods, and then a frequency distribution is made of the pairs of vertical components for each hypothesis, that period which gives the best approximation to the sort of distribution to be expected for a system of monoalphabetic substitution with 25 variants for each letter may be taken to be correct. For in the case of an incorrect period the resultant vertical bipartite components are not the equivalents of the actual plain-text letters; hence such repetitions as occur are purely accidental and the number of such cases would be rather small. But in the case of the correct period the resultant vertical pairs of components are the equivalents of the actual plain-text letters; hence repetitions are causal and fairly frequent. Were it not for variants, of course, the distribution would be perfectly monoalphabetic.

47. Illustration of solution. - a. With the foregoing principles in mind, the following cryptogram will be studied.

```
KZFBE ILYYM OCBRB LZDOT GBLPK YWCUC CEPQL
AMEYL ZQXWH LRWQY ARWBM TIZEB ELAYE SOBRY
QVBBL NXNAB QBDOY MQDLW LNACO XCRRG ASWQB
FDDTE BAMFD ETENA KGDFO QDUBN DCLYD VWBAX
CAUGG XOART XXTSD AYXHK OLSXA BRKRP UZWHO
MTDHT SGMLS LQPOU NHCIC KKAQB DOFLE KAPRG
SXUPO WALMA VQHLM LAXKP WSTMC XKQVH SIXSL
LWXLX RSGZD FKLNY BXMRB NADKT TBAEO BHWVL
YSXMB OWPGX KORZI UCEAD YIDBL ZMITA NHCAI
DNCID DOYIB CNOLY UUMCE POTDM GBFUN AHLBD
WXNXK KCSCT OXTSD AYXHK CNLDK RRFAY APMHC
ANMBV GREZQ ATCYI MNDLR LGMTW ETRCV VKTED
UFDEL XHEQV CBLYU DUGYA FHNQL KFRUC NVDLH
LZDRE LKXKU PSEMC TNKTK EBOEE PGVQT GWERH
LZDRE LKFAX IYDAK ZLXXO RRPER RRRNC IE
```

b. The long repetitions noted in the text indicate a period of either 5 or 7. By transcribing several lines of text into their θ_1 and θ_2 components according to both of these alternatives and distributing the vertically superimposed pairs, it is soon found that a period of 7 produces many more repetitions than does a period of 5. The entire text is then transcribed into its θ_1 and θ_2 components according to a period of 7 (see Fig. 82) and complete distributions of $\theta_1\theta_2$ and $\theta_2\theta_1$ vertical pairs are made, the distributions being, of course, kept separate. They are shown in Figs. 83 and 84. The individual distributions show many repetitions and the distributions as a whole are very favorable for a period of 7.

c. The text is accordingly entirely transcribed into periods of 7, with the θ_1 and θ_2 components indicated by the cipher letters in each period. Then the vertical pairs of components are examined to locate cases in which the basic letter of the θ_1 and θ_2 superimposed components are identical, whereupon the plain-text letters indicated are at once inserted into position. In this example 10 such cases are found, one each in periods 14, 22, 26, 35, 36, 52, 59, 68, and two in period 74. All of these, of course, involve letters in odd positions in the periods. The plain-text letters thus inserted may serve as clues for assuming probable words.

d. Now if only a few equivalencies can be established between a few of the θ_1 components, or between a few of the θ_2 components, or between a few θ_1 and θ_2 components a long step forward may be taken in the solution. Perhaps some information can be found by studying Figs. 83 and 84. A consideration of Fig. 83 will soon lead to the idea that each row of frequencies can indicate only 5 different plain-text letters, one of which coincides with the indicating letter at the left of the row. Moreover, in this same figure, while there are 25 rows in all, there are really only 5 different categories of rows, each category corresponding

1 K Z F B E I L $K_1K_2Z_1Z_2F_1F_2B_1$ $B_2E_1E_2I_1I_2L_1L_2$	2 Y Y M O C B R $Y_1Y_2Y_1Y_2M_1M_2O_1$ $O_2C_1C_2B_1B_2R_1R_2$	3 B L Z D O T G $B_1B_2L_1L_2Z_1Z_2D_1$ $D_2O_1O_2T_1T_2G_1G_2$	4 B L P K Y W C $B_1B_2L_1L_2P_1P_2K_1$ $K_2Y_1Y_2W_1W_2C_1C_2$	5 U C C E P Q L $U_1U_2C_1C_2C_1C_2E_1$ $E_2P_1P_2Q_1Q_2L_1L_2$
6 A M E Y L Z Q $A_1A_2M_1M_2E_1E_2Y_1$ $Y_2L_1L_2Z_1Z_2Q_1Q_2$	7 X W H L R W Q $X_1X_2W_1W_2H_1H_2L_1$ $L_2R_1R_2W_1W_2Q_1Q_2$	8 Y A R W B M T $Y_1Y_2A_1A_2R_1R_2W_1$ $W_2B_1B_2M_1M_2T_1T_2$	9 I Z E B E L A $I_1I_2Z_1Z_2E_1E_2B_1$ $B_2E_1E_2L_1L_2A_1A_2$	10 Y E S O B R Y $Y_1Y_2E_1E_2S_1S_2O_1$ $O_2B_1B_2R_1R_2Y_1Y_2$
11 Q V B B L N X $Q_1Q_2V_1V_2B_1B_2B_1$ $B_2L_1L_2N_1N_2X_1X_2$	12 N A B Q B D O $N_1N_2A_1A_2B_1B_2Q_1$ $Q_2B_1B_2D_1D_2O_1O_2$	13 Y M Q D L W L $Y_1Y_2M_1M_2Q_1Q_2D_1$ $D_2L_1L_2W_1W_2L_1L_2$	14 N A C O X C R $N_1N_2A_1A_2C_1C_2O_1$ $O_2X_1X_2C_1C_2R_1R_2$	15 R G A S W Q B $R_1R_2G_1G_2A_1A_2S_1$ $S_2W_1W_2Q_1Q_2B_1B_2$
16 F D D T E B A $F_1F_2D_1D_2D_1D_2T_1$ $T_2E_1E_2B_1B_2A_1A_2$	17 M F D E T E N $M_1M_2F_1F_2D_1D_2E_1$ $E_2T_1T_2E_1E_2N_1N_2$	18 A K G D F O Q $A_1A_2K_1K_2G_1G_2D_1$ $D_2F_1F_2O_1O_2Q_1Q_2$	19 D U B N D C L $D_1D_2U_1U_2B_1B_2N_1$ $N_2D_1D_2C_1C_2L_1L_2$	20 Y D V W B A X $Y_1Y_2D_1D_2V_1V_2W_1$ $W_2B_1B_2A_1A_2X_1X_2$
21 C A U G G X O $C_1C_2A_1A_2U_1U_2G_1$ $G_2G_1G_2X_1X_2O_1O_2$	22 A R T X X T S $A_1A_2R_1R_2T_1T_2X_1$ $X_2X_1X_2T_1T_2S_1S_2$	23 D A Y X H K O $D_1D_2A_1A_2Y_1Y_2X_1$ $X_2H_1H_2K_1K_2O_1O_2$	24 L S X A B R K $L_1L_2S_1S_2X_1X_2A_1$ $A_2B_1B_2R_1R_2K_1K_2$	25 R P U Z W H O $R_1R_2P_1P_2U_1U_2Z_1$ $Z_2W_1W_2H_1H_2O_1O_2$
26 M T D H T S G $M_1M_2T_1T_2D_1D_2H_1$ $H_2T_1T_2S_1S_2G_1G_2$	27 M L S L Q P O $M_1M_2L_1L_2S_1S_2L_1$ $L_2Q_1Q_2P_1P_2O_1O_2$	28 U N H C I C K $U_1U_2N_1N_2H_1H_2C_1$ $C_2I_1I_2C_1C_2K_1K_2$	29 K A Q B D O F $K_1K_2A_1A_2Q_1Q_2B_1$ $B_2D_1D_2O_1O_2F_1F_2$	30 L E K A P R G $L_1L_2E_1E_2K_1K_2A_1$ $A_2P_1P_2R_1R_2G_1G_2$
31 S X U P O W A $S_1S_2X_1X_2U_1U_2P_1$ $P_2O_1O_2W_1W_2A_1A_2$	32 L M A V Q H L $L_1L_2M_1M_2A_1A_2V_1$ $V_2Q_1Q_2H_1H_2L_1L_2$	33 M L A X K P W $M_1M_2L_1L_2A_1A_2X_1$ $X_2K_1K_2P_1P_2W_1W_2$	34 S T M C X K Q $S_1S_2T_1T_2M_1M_2C_1$ $C_2X_1X_2K_1K_2Q_1Q_2$	35 V H S I X S L $V_1V_2H_1H_2S_1S_2I_1$ $I_2X_1X_2S_1S_2L_1L_2$
36 L W X L X R S $L_1L_2W_1W_2X_1X_2L_1$ $L_2X_1X_2R_1R_2S_1S_2$	37 G Z D F K L N $G_1G_2Z_1Z_2D_1D_2F_1$ $F_2K_1K_2L_1L_2N_1N_2$	38 Y B X M R B N $Y_1Y_2B_1B_2X_1X_2M_1$ $M_2R_1R_2B_1B_2N_1N_2$	39 A D K T T B A $A_1A_2D_1D_2K_1K_2T_1$ $T_2T_1T_2B_1B_2A_1A_2$	40 E O B H W V L $E_1E_2O_1O_2B_1B_2H_1$ $H_2W_1W_2V_1V_2L_1L_2$
41 Y S X M B O W $Y_1Y_2S_1S_2X_1X_2M_1$ $M_2B_1B_2O_1O_2W_1W_2$	42 P G X K O R Z $P_1P_2G_1G_2X_1X_2K_1$ $K_2O_1O_2R_1R_2Z_1Z_2$	43 I U C E A D Y $I_1I_2U_1U_2C_1C_2E_1$ $E_2A_1A_2D_1D_2Y_1Y_2$	44 I D B L Z M I $I_1I_2D_1D_2B_1B_2L_1$ $L_2Z_1Z_2M_1M_2I_1I_2$	45 T A N H C A I $T_1T_2A_1A_2N_1N_2H_1$ $H_2C_1C_2A_1A_2I_1I_2$
46 D N C I D D O $D_1D_2N_1N_2C_1C_2I_1$ $I_2D_1D_2D_1D_2O_1O_2$	47 Y I B C N O L $Y_1Y_2I_1I_2B_1B_2C_1$ $C_2N_1N_2O_1O_2L_1L_2$	48 Y U U M C E P $Y_1Y_2U_1U_2U_1U_2M_1$ $M_2C_1C_2E_1E_2P_1P_2$	49 O T D M G B F $O_1O_2T_1T_2D_1D_2M_1$ $M_2G_1G_2B_1B_2F_1F_2$	50 U N A H L B D $U_1U_2N_1N_2A_1A_2H_1$ $H_2L_1L_2B_1B_2D_1D_2$

FIGURE 82.

Figure 82 - Continued.

51	52	53	54	55
W X N X K K C	S C T O X T S	D A Y X H K C	N L D K R R F	A Y A P M H C
$W_1W_2X_1X_2N_1N_2X_1$	$S_1S_2C_1C_2T_1T_2O_1$	$D_1D_2A_1A_2Y_1Y_2X_1$	$N_1N_2L_1L_2D_1D_2K_1$	$A_1A_2Y_1Y_2A_1A_2P_1$
$X_2K_1K_2K_1K_2C_1C_2$	$O_2X_1X_2T_1T_2S_1S_2$	$X_2H_1H_2K_1K_2C_1C_2$	$K_2R_1R_2R_1R_2F_1F_2$	$P_2M_1M_2H_1H_2C_1C_2$
56	57	58	59	60
A N M B V G R	E Z Q A T C Y	I M N D L R L	G M T W E T R	C V V K T E D
$A_1A_2N_1N_2M_1M_2B_1$	$E_1E_2Z_1Z_2Q_1Q_2A_1$	$I_1I_2M_1M_2N_1N_2D_1$	$G_1G_2M_1M_2T_1T_2W_1$	$C_1C_2V_1V_2V_1V_2K_1$
$B_2V_1V_2G_1G_2R_1R_2$	$A_2T_1T_2C_1C_2Y_1Y_2$	$D_2L_1L_2R_1R_2L_1L_2$	$W_2E_1E_2T_1T_2R_1R_2$	$K_2T_1T_2E_1E_2D_1D_2$
61	62	63	64	65
U F D E L X H	E Q V C B L Y	U D U G Y A F	H N Q L K F R	U C N V D L H
$U_1U_2F_1F_2D_1D_2E_1$	$E_1E_2Q_1Q_2V_1V_2C_1$	$U_1U_2D_1D_2U_1U_2G_1$	$H_1H_2N_1N_2Q_1Q_2L_1$	$U_1U_2C_1C_2N_1N_2V_1$
$E_2L_1L_2X_1X_2H_1H_2$	$C_2B_1B_2L_1L_2Y_1Y_2$	$G_2Y_1Y_2A_1A_2F_1F_2$	$L_2K_1K_2F_1F_2R_1R_2$	$V_2D_1D_2L_1L_2H_1H_2$
66	67	68	69	70
L Z D R E L K	X K U P S E M	C T N K T K E	B O E E P G V	Q T G W E R H
$L_1L_2Z_1Z_2D_1D_2R_1$	$X_1X_2K_1K_2U_1U_2P_1$	$C_1C_2T_1T_2N_1N_2K_1$	$B_1B_2O_1O_2E_1E_2E_1$	$Q_1Q_2T_1T_2G_1G_2W_1$
$R_2E_1E_2L_1L_2K_1K_2$	$P_2S_1S_2E_1E_2M_1M_2$	$K_2T_1T_2K_1K_2E_1E_2$	$E_2P_1P_2G_1G_2V_1V_2$	$W_2E_1E_2R_1R_2H_1H_2$
71	72	73	74	75
L Z D R E L K	F A X I Y D A	K Z L X X O R	R P E R R R R	N C I E
$L_1L_2Z_1Z_2D_1D_2R_1$	$F_1F_2A_1A_2X_1X_2I_1$	$K_1K_2Z_1Z_2L_1L_2X_1$	$R_1R_2P_1P_2E_1E_2R_1$	$N_1N_2C_1C_2$
$R_2E_1E_2L_1L_2K_1K_2$	$I_2Y_1Y_2D_1D_2A_1A_2$	$X_2X_1X_2O_1O_2R_1R_2$	$R_2R_1R_2R_1R_2R_1R_2$	$I_1I_2E_1E_2$

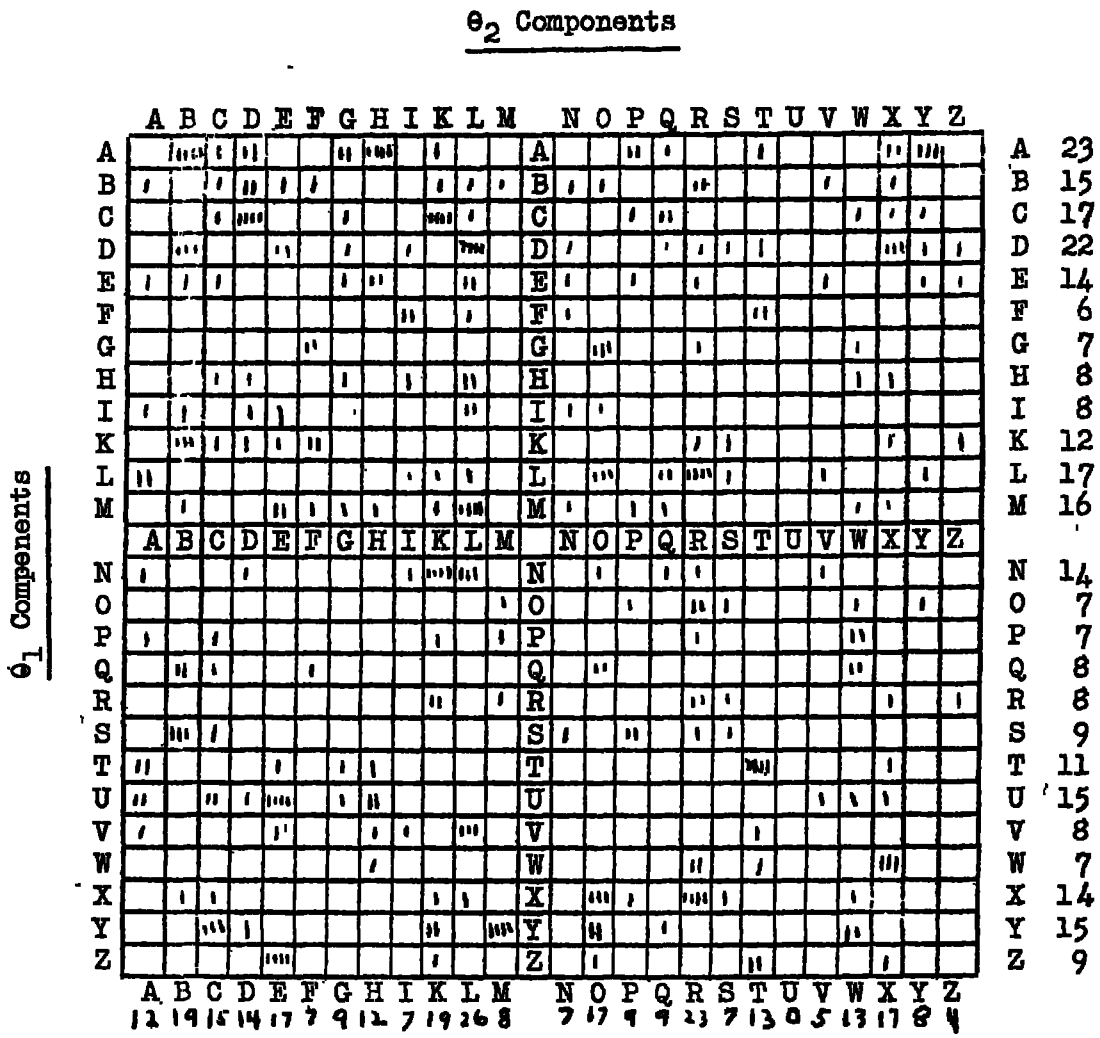


FIGURE 83.

to a row in the substitution checkerboard. If the rows belonging to the same category can be ascertained a large step forward in solution can be taken. Why not try to match the distributions in the rows? For example, rows D and M appear to be similar:

θ_1 Components

θ_2 Components

	A	B	C	D	E	F	G	H	I	K	L	M		N	O	P	Q	R	S	T	U	V	W	X	Y	Z		
A	|	|	||	|||		|				||	||	||	A		|					|		|	|	||			A	20
B		|							|		|||		B		||	|								|	|		B	10
C							|				||		C		|		|	|		|||					|		C	10
D	|||	||		||		||	|	|||		||		|	D	||													D	18
E	|	|											E				|	|||		|		|	|				E	9
F					||						|		F											|	|		F	5
G					|			|		|			G				||	|									G	6
H										||			H				|		|								H	4
I	|				|						|		I		|											|	I	5
K	|			|	||		|						K		|									|			K	7
L		|			||								L			|||	|	||		|			|	|			L	12
M								|		|			M				||	|||		|||			|			|	M	12
	A	B	C	D	E	F	G	H	I	K	L	M		N	O	P	Q	R	S	T	U	V	W	X	Y	Z		
N		||	||	|	|	|	|	|	|		|		N					|						|			N	13
O							||						O									|					O	3
P			|					|					P		|			|									P	4
Q					|	|					|||		Q					|							|		Q	7
R													R					|		||			||				R	5
S											|		S		|||			|						|	|		S	7
T		|	|							||			T					||	|||								T	9
U	|		|	||	|	|			|		||	|	U		||	||									|		U	15
V				|	|								V	|										||	|		V	6
W										|			W					|					|				W	3
X	|									||			X	|				|	||				||			|	X	10
Y		|||||	|||					|			|		Y	|	|			|									Y	13
Z			|				|		|		||||		Z		|												Z	8
	A	B	C	D	E	F	G	H	I	K	L	M		N	O	P	Q	R	S	T	U	V	W	X	Y	Z		
	9	14	11	10	12	6	7	8	4	13	21	4		5	14	6	8	20	6	11	0	3	9	10	7	3		

FIGURE 84.

	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	
D_1		- - -			- -		-		-			- - - - -		-			-	-	-	-				- - -	-	-	N = 22
M_1		-			- -	-	-	-			-	- - - -		-		-	-						-	-			N = 16

FIGURE 85.

Applying the X-test, the observed value of X = 34, the expected value is 23. An excellent match is obtained, and the hypothesis that D and M are in the same row in the checkerboard seems promising. Can any confirmation be found in the cryptogram itself?

e. It has already been pointed out that this system reduces to monoalphabetic substitution with variants. This being the case it should be possible to find manifestations of equivalency between some of the $\begin{matrix}\theta_1\\ \theta_2\end{matrix}$ vertical pairs in the cryptogram. Note the following instances of apparent equivalency between D_1 and M_1:

Period 16	D_2B_1	D_1B_2
20	Y_2B_1	D_1B_2
49	T_2B_1	D_1B_2
2	Y_2B_1	M_1B_2
16	F_2E_1	D_1E_2
17	F_2E_1	D_1E_2
59	G_2E_1	M_1E_2
3	Z_2G_1	D_1G_2
56	N_2G_1	M_1G_2
13	Q_2L_1	D_1L_2
37	Z_2L_1	D_1L_2
58	N_2L_1	D_1L_2
66	Z_2L_1	D_1L_2
71	Z_2L_1	F_1L_2
6	A_2L_1	M_1L_2
13	Y_2L_1	M_1L_2
58	I_2L_1	M_1L_2

Period 18	G_2Q_1	D_1Q_2	
32	L_2Q_1	M_1Q_2	
12	A_1B_2	A_2D_1	B_1D_2
50	A B	A D	H D
8	A_1B_2	A_1M_1	R_1M_2
19	D_1N_2	D_2D_1	U_1D_2
46	D I	D D	N D
44	D_1Z_2	D_2M_1	B_1M_2
43	U_1A_2	U_2D_1	C_1D_2
67	U_1E_2	U_2M_1	P_1M_2

It may be assumed the $D_1 = M_1$ and the two distributions in Fig. 85 may be amalgamated.

$D_1 + M_1$ 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

The only other row in Fig. 83 which gives indications of being similar to this distribution is the A row. A search is made through the text to see if any equivalence between A_1, D_1 and M_1 appears.

Note the following cases:

Period	8	Y_2B_1	A_1B_2	A_2M_1
	12	N_2B_1	A_1B_2	A_2D_1
	50	N_2B_1	A_1B_2	A_2D_1
	16	D_2B_1	D_1B_2	D_2A_1
	20	Y_2B_1	D_1B_2	D_2A_1
	49	T_2B_1	D_1B_2	D_2F_1
	2	Y_2B_1	M_1B_2	M_2R_1
	21	C_2G_1	A_1G_2	A_2X_1
	30	K_2G_1	A_1G_2	S_1P_2
	3	Z_2G_1	D_1G_2	B_1K_2
	56	N_2G_1	M_1G_2	M_2R_1
	24	X_2K_1	A_1K_2	R_1Z_2
	34	T_2K_1	M_1K_2	M_2Q_1
	33	L_2P_1	A_1P_2	A_2W_1
	48	U_2P_1	M_1P_2	O_1M_2
	15	G_2Q_1	A_1Q_2	A_2B_1
	18	G_2Q_1	D_1Q_2	D_1N_2
	32	L_2Q_1	M_1Q_2	M_2H_1
	14	N_2X_1	A_1X_2	A_2G_1
	61	F_2X_1	D_1X_2	D_2H_1
	57	Q_2Y_1	A_1Y_2	I_1D_2
	72	F_2Y_1	A_1Y_2	A_2D_1
	63	U_2Y_1	D_1Y_2	A_2A_1

It certainly seems as though $A_1 = D_1 = M_1$, and this will be assumed to be correct. Among the most frequent combinations is the pair Y_2B_1, appearing in the following sequences:

Period	2	Y_2C_1	Y_1C_2	Y_2B_1	M_1B_2	M_2R_1
	8	L_1Q_2	Y_1W_2	Y_2B_1	A_1B_2	A_2M_1
	10	B_1A_2	Y_1O_2	Y_2B_1	E_1B_2	E_2R_1
	20	N_1L_2	Y_1W_2	Y_2B_1	D_1B_2	D_2A_1
	41	H_1L_2	Y_1M_2	Y_2B_1	S_1B_2	S_2O_1

Note how M_1, A_1, E_1, D_1, and S_1 all appear to be interchangeable. Are these the 5 letters which belong in the same row? The probable equivalence among A_1, D_1, and M_1 has been established by noting cases of equivalency in the text. A further search will be made to see if E_1 and S_1 also show equivalencies with A_1, D_1, and M_1.

Note the following:

Period 21	C_2G_1	A_1G_2
30	K_2G_1	A_1G_2
3	Z_2G_1	D_1G_2
69	O_2G_1	E_1G_2
56	N_2G_1	M_1G_2
23	$D_1X_2D_2H_1$	A_1H_2
32	$M_1Q_2M_2H_1$	A_1H_2
61	$D_1X_2D_2H_1$	E_1H_2

Here are indications that E_1 belongs to the same series, but not enough cases where S_1 is interchangeable with A, D, E, or M can be found to be convincing. But perhaps it is best not to go too fast in these early stages. Let it be assumed for the present that A, D, E, and M are in the same row of the substitution checkerboard. In period 16 there is the pair of vertical components D_1 E_2. Since $D_1 = E_1$ this pair may be written E_1E_2, whereupon the plain-text letter E is immediately indicated. All cases of this sort are sought in the text and the plain-text letters are inserted in their proper places, there being 7 such instances in all, but these yield the important letters, A, D, and E.

f. In a similar manner, by an intensive search for cases in which components appear to be equivalent because they occur in repetitions which are identical save for one or two components, it is established that C, O, M, and W are in the same column in the checkerboard. Note the bracketing of these letters occurring as θ_2 components in the next to the last list of sequences in subparagraph e. Likewise, B, H, and N are established as being in the same row. Again the text is examined for cases in which plain-text letters C, O, M, W, B, H, and N may be inserted. By carrying out this process to its full extent possible, the skeletons of words will soon begin to appear.

g. Enough has been demonstrated to show this line of attack. Of course, if there is a large volume of text at hand, the simplest procedure would be to construct frequency distributions of the types shown in Figs. 83 and 84, and use the statistical method to match the individual distributions. For this method to be reliable it would be necessary to have several hundred letters of text, but this in actual practice would not be too much to expect.

h. There is, however, another line of attack, based upon the probable-word method. It has been pointed out that in the case of letters in odd positions in the periods 40% of the time the plain-text letter involved is indicated by either its θ_1 or θ_2 component. This property affords a fair basis for assuming a probable word. For example, the cryptogram here studied shows the following two periods:

	S	L
Periods 35	$V_1V_2H_1G_2S_1S_2I_1$	$L_1L_2W_1W_2X_1X_2L_1$
and 36	$I_2X_1X_2S_1S_2L_1L_2$	$L_2X_1X_2R_1R_2S_1S_2$
	V H S I X S L	L W X L X R S

Two letters are quite definite, S_p and L_p. Suppose the possible plain-text letters be indicated.

Possible plain-	V	.	H	.	S	.	I	L	.	W	.	X	.	L
text letters	I		X				L			X		R		S
Components	V_1	V_2	H_1	H_2	S_1	S_2	I_1	L_1	L_2	W_1	W_2	X_1	X_2	L_1
	I_2	X_1	X_2	S_1	S_2	L_1	L_2	L_2	X_1	X_2	R_1	R_2	S_1	S_2
Cipher text	V	H	S	I	X	S	L	L	W	X	L	X	R	S

The word HOSTILE is suggested by the letters H . S . I L . . This word will be assumed to be correct and it will be written out with its components under the cipher components. Thus:

	35							36	
Plain text			H	O	S	T	I	L	E
Cipher-text Components	V_1	V_2	H_1	H_2	S_1	S_2	I_1	L_1	L_2
	I_2	X_1	X_2	S_1	S_2	L_1	L_2	L_2	X_1
Plain-text Components			H_1	O_1	S_1	T_1	I_1	L_1	E_1
			H_2	O_2	S_2	T_2	I_2	L_2	E_2

This word, if correct, yields the following equivalencies: $H_2 = X_2 = O_1$; $S_1 = O_2$; $T_1 = S_2$; $L_1 = T_2$; $I_2 = L_2 = E_1$; $X_1 = E_2$. Again the text is examined for cases in which the plain-text letters may now be directly inserted; but only one case is found, in period 44, where $I_1L_2 = I_1I_2 = I_p$. This is unfortunate, so that additional words will have to be assumed. The 14th period shows a C_p and the components after it suggest that the word CROSSROADS may be present. Thus:

					C	R	O	S	S	R	O	A	D	S
Periods 14 and 15	N_1	N_2	A_1	A_2	C_1	C_2	O_1	R_1	R_2	G_1	G_2	A_1	A_2	S_1
	O_2	X_1	X_2	C_1	C_2	R_1	R_2	S_2	W_1	W_2	Q_1	Q_2	B_1	B_2
	N	A	C	O	X	C	R	R	G	A	S	W	Q	B

Take the first letter R_p, represented by C_2R_1.

Since $R_p = C_2R_1$,

Therefore, $R_1R_2 = C_2R_1$

Hence $R_1 = C_2$ and $R_2 = R_1$

Therefore, $R_1 = R_2 = C_2$

Again, in the case of the 1st O_p,

$O_p = O_1R_2$

But $O_p = O_1O_2 = O_1R_2$

$O_2 = R_2$

Therefore, $R_1 = R_2 = O_2 = C_2$

The various equivalencies yielded are as follows:

$C_2 = R_1 = O_2 = S_1 = R_2 = C_1 = W_2$
$S_2 = W_1 = B_2$
$O_1 = G_2$
$O_2 = Q_1$
$Q_2 = A_2 = D_1$
$B_1 = D_2$

i. Let all the equivalencies found thus far be collected in two tables, as shown in Fig. 86.

$\theta_1\theta_2$ Combinations

A_1	B_1	C_1	D_1	E_1	F_1	G_1	H_1	I_1	K_1	L_1	M_1	N_1	O_1	P_1	Q_1	R_1	S_1	T_1	U_1	V_1	W_1	X_1	Y_1	Z_1
D_1	H_1		A_1	A_1		O_2	B_1			T_2	A_1	B_1	H_2			G_1	O_2	S_2				E_2		
E_1	N_1		E_1	D_1		C_2	N_1				D_1	H_1	X_2			C_2	C_2							
M_1			M_1	M_1		M					E_1					O_2	M_2							
I_2			I_2	I_2		W_2					I_2					M_2	W_2							
L_2			L_2	L_2		R_1					L_2					W_2	R_1							
						R_2										R_2	R_2							
						S_1										S_1	G_1							

$\theta_2\theta_1$ Combinations

A_2	B_2	C_2	D_2	E_2	F_2	G_2	H_2	I_2	K_2	L_2	M_2	N_2	O_2	P_2	Q_2	R_2	S_2	T_2	U_2	V_2	W_2	X_2	Y_2	Z_2
		M_2		X_1			X_2	L_2		I_2	C_2		C_2			C_2	T_1	L_1			C_2	H_2		
		O_2					O_1	A_1		A_1	O_2		M_2			M_2					M_2	O_1		
		W_2						D_1		D_1	W_2		W_2			O_2					O_2			
		R_1						E_1		E_1	R_1		S_1			W_2					S_1			
		S_1						M_1		M_1	S_1		R_1			S_1					R_1			
		R_2									R_2		R_2			R_1					R_2			
		G_1									G_1		G_1			G_1					G_1			

FIGURE 86.

A study of the equivalencies indicated that

(1) A_1 D_1 E_1 M belong in the same row

(2) B_1 H_1 N belong in the same row

(3) G_1 R_1 S belong in the same row

(4) C_1 O_1 M_1 W belong in the same column

(5) I_1 L belong in the same column

(6) X_1 H belong in the same column

(7) The coordinates of R are identical and hence this letter occupies a cell along a diagonal sloping from left to right.

j. Since a row or a column can contain only 5 letters, it is obvious that A D E M, B H N, and G R S fall in 3 different rows; C O M W and I L fall in different columns. A start may be made by an arbitrary placement of R in the position 1-1, and since $R_1 = O_2 = C_2 = M_2 = W_2$, this means that R, O, C, M, and W form one column in the substitution checkerboard, as shown in Fig. 87. The data also indicate that R, G and S must be in row 1, A, D, and E must be in row 4, H and X must be in column 3. This means that θ_1 for A, D, and E must be 4, and that θ_2 for H and X must be 3. And since $M_1 = I_2 = L_2$, θ_2 for I and L must be 4.

	1	2	3	4	5	
1	R					GS
2	C					
3	O					X
4	M					ADE
5	W					
			H X	I L		

FIGURE 87.

Substituting in the text the coordinates for the known values, soon additional plain-text words become evident. For example, taking the periods with the word HOSTILE, it becomes

	H	O	S	T	I			L	E					
Periods 35 and 36	V_1 I_2	V_2 X_1	H_1 X_2	H_2 S_1	S_1 S_2	S_2 L_1	I_1 L_2	L_1 L_2	L_2 X_1	W_1 X_2	W_2 R_1	X_1 R_2	X_2 S_1	L_1 S_2
	V	H	S	I	X	S	L	L	W	X	L	X	R	S

possible to insert the letters R_p and O_p as the 2d and 4th letters after E_p, suggesting that the word after HOSTILE is TROOP. This gives $W_1 X_2 = T_p$, which permits of placing T in position 5-3. Since T in HOSTILE $= S_2L_1$, therefore $S_2 = 5$ and $L_1 = 3$. Since S is in row 1, and $S_2 = 5$, S must go in position 1-5. Since $L_2 = 4$ and $L_1 = 3$, L must go in position 3-4. Since O_p (the 1st O in TROOP) $= X_1R_2$ and it is known that $O_p = 3$-1, therefore X must be in position 3-3. The checkerboard is now as shown in Fig. 88. From Fig. 86, $X_1 = E_2$. Now $X_1 = 3$, and

	1	2	3	4	5	
1	R				S	G
2	C					
3	O		X	L		
4	M					ADE
5	W		T			
			H	I		

FIGURE 88.

	1	2	3	4	5	
1	R				S	G
2	C					
3	O		X	L		
4	M		E			AD
5	W		T			
			H	I		

FIGURE 89.

since the E must be in row 4, it is evident that E must occupy cell 4-3, as seen in Fig. 89. There are now only 2 possible rows for H, either 1 or 2. It is deemed unnecessary to give further details of the process. Suffice it to say that in a few minutes the entire checkerboard is found to be as shown in Fig. 90. It will decipher the entire cryptogram as it stands, but speculating upon the presence of W U T V Z in the last row, and assuming a key-word mixed sequence has brought this about, a rearrangement of the columns of the checkerboard is made to give T U V W Z, as shown in Fig. 91. The arrangement of the rows now becomes quite evident and the original checkerboard is found to be as shown in Fig. 92. It seems to be based upon the key phrase XYLOPHONIC BEDLAM.

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

FIGURE 90.

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

FIGURE 91.

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

FIGURE 92.

k. The completely deciphered cryptogram is as follows:

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

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

9	10	11	12
B A T T A L I	O N F O R T Y	S E V E N T H	I N F A N T R
2 3 5 5 3 1 2	1 2 3 1 4 5 1	4 3 5 3 2 5 2	2 2 3 3 2 5 4
5 3 1 1 3 3 3	4 2 5 4 4 1 2	5 1 3 1 2 1 1	3 2 5 3 2 1 4
I Z E B E L A	Y E S O B R Y	Q V B B L N X	N A B Q B D O

13	14	15	16
Y H A S R E A	C H E D C R O	S S R O A D S	E V E N F I V
1 2 3 4 4 3 3	2 2 3 3 2 4 1	4 4 4 1 3 3 4	3 5 3 2 3 2 5
2 1 3 5 4 1 3	4 1 1 2 4 4 4	5 5 4 4 3 2 5	1 3 1 2 5 3 3
Y M Q D L W L	N A C O X C R	R G A S W Q B	F D D T E B A

17	18	19	20
E S E V E N D	D A S H R O A	D J U N C T I	O N F I V E T
3 4 3 5 3 2 3	3 3 4 2 4 1 3	3 2 5 2 2 5 2	1 2 3 2 5 3 5
1 5 1 3 1 2 2	2 3 5 1 4 4 3	2 3 2 2 4 1 3	4 2 5 3 3 1 1
M F D E T E N	A K G D F O Q	D U B N D C L	Y D V W B A X

21	22	23	24
H R E E T H R	E E G S T O P	E N E M Y H O	L D S W O O D
2 4 3 3 5 2 4	3 3 4 4 5 1 1	3 2 3 3 1 2 1	1 3 4 5 1 1 3
1 4 1 1 1 1 4	1 1 1 5 1 4 5	1 2 1 4 2 1 4	3 2 5 4 4 4 2
C A U G G X O	A R T X X T S	D A Y X H K O	L S X A B R K

25	26	27	28
S S O U T H W	E S T O F C H	A R L E S T O	W N I N C O N
4 4 1 5 5 2 5	3 4 5 1 3 2 2	3 4 1 3 4 5 1	5 2 2 2 2 1 2
5 5 4 2 1 1 4	1 5 1 4 5 4 1	3 4 3 1 5 1 4	4 2 3 2 4 4 2
R P U Z W H O	M T D H T S G	M L S L Q P O	U N H C I C K

29	30	31	32
S I D E R A B	L E F O R C E	S T O P W I L	L M A K E E V
4 2 3 3 4 3 2	1 3 3 1 4 2 3	4 5 1 1 5 2 1	1 3 3 4 3 3 5
5 3 2 1 4 3 5	3 1 5 4 4 4 1	5 1 4 5 4 3 3	3 4 3 2 1 1 3
K A Q B D O F	L E K A P R G	S X U P O W A	L M A V Q H L

33	34	35	36
E R Y E F F O	R T T O D R I	V E H O S T I	L E T R O O P
3 4 1 3 3 3 1	4 5 5 1 3 4 2	5 3 2 1 4 5 2	1 3 5 4 1 1 1
1 4 2 1 5 5 4	4 1 1 4 2 4 3	3 1 1 4 5 1 3	3 1 1 4 4 4 5
M L A X K P W	S T M C X K Q	V H S I X S L	L W X L X R S

37	38	39	40
S O U T A N D	O C C U P Y D	E F E N S I V	E P O S I T I
4 1 5 5 3 2 3	1 2 2 5 1 1 3	3 3 3 2 4 2 5	3 1 1 4 2 5 2
5 4 2 1 3 2 2	4 4 4 2 5 2 2	1 5 1 2 5 3 3	1 5 4 5 3 1 3
G Z D F K L N	Y B X M R B N	A D K T T B A	E O B H W V L

41	42	43	44
O N S T O P M	Y T R O O P S	H A V I N G D	I F F I C U L
1 2 4 5 1 1 3	1 5 4 1 1 1 4	2 3 5 2 2 4 3	2 3 3 2 2 5 1
4 2 5 1 4 5 4	2 1 4 4 4 5 5	1 3 3 3 2 1 2	3 5 5 3 4 2 3
Y S X M B O W	P G X K O R Z	I U C E A D Y	I D B L Z M I

45	46	47	48
T Y M A I N T	A I N I N G C	O N N E C T I	O N W I T H F
5 1 3 3 2 2 2	3 2 2 2 2 4 2	1 2 2 3 2 5 2	1 2 5 2 5 2 3
1 2 4 3 3 2 3	3 3 2 3 2 1 4	4 2 2 1 4 1 3	4 2 4 3 1 1 5
T A N H C A I	D N C I D D O	Y I B C N O L	Y U U M C E P

49	50	51	52
O R T Y F I F	T H I N F A N	T R Y O N N O	R T H S T O P
1 4 5 1 3 2 3	5 2 2 2 3 3 2	5 4 1 1 2 2 1	4 5 2 4 5 1 1
4 4 1 2 5 3 5	1 1 3 2 5 3 2	1 4 2 4 2 2 4	4 1 1 5 1 4 5
O T D M G B F	U N A H L B D	W X N X K K C	S C T O X T S

53	54	55	56
E N E M Y N O	N C O M M I S	S I O N E D O	F F I C E R C
3 2 3 3 1 2 1	2 2 1 3 3 2 4	4 2 1 2 3 3 1	3 3 2 2 3 4 2
1 2 1 4 2 2 4	2 4 4 4 4 3 5	5 3 4 2 1 2 4	5 5 3 4 1 4 4
D A Y X H K C	N L D K R R F	K Y A P M H C	A N M B V G R

57	58	59	60
A P T U R E D	N E A R C H A	R L E S T O W	N S T A T E S
3 1 5 5 4 3 3	2 3 3 4 2 2 3	4 1 3 4 5 1 5	2 4 5 3 5 3 4
3 5 1 2 4 1 2	2 1 3 4 4 1 3	4 3 1 5 1 4 4	2 5 1 3 1 1 5
E Z Q A T C Y	I M N D L R L	G M T W E T R	C V V K T E P

61	62	63	64
T H A T E N E	M Y S E V E N	T H D I V I S	I O N I S M O
5 2 3 5 3 2 3	3 1 4 3 5 3 2	5 2 3 2 5 2 4	2 1 2 2 4 3 1
1 1 3 1 1 2 1	4 2 5 1 3 1 2	1 1 2 3 3 3 5	3 4 2 3 5 4 4
U F D E L X H	E Q V C B L Y	U D U G Y A F	H N Q L K F R

65	66	67	68
V I N G I N T	O A T T A C K	P O S I T I O	N S T O N I G
5 2 2 4 2 2 5	1 3 5 5 3 2 4	1 1 4 2 5 2 1	2 4 5 1 2 2 4
3 3 2 1 3 2 1	4 3 1 1 3 4 2	5 4 5 3 1 3 4	2 5 1 4 2 3 1
U C N V D L H	L Z D R E L K	X K U P S E M	C T N K T K E

69	70	71	72
H T P R E P A	R A T O R Y T	O A T T A C K	A T D A Y L I
2 5 1 4 3 1 3	4 3 5 1 4 1 5	1 3 5 5 3 2 4	3 5 3 3 1 1 2
1 1 5 4 1 5 3	4 3 1 4 4 2 1	4 3 1 1 3 4 2	3 1 2 3 2 3 3
B O E E P G V	Q T G W E R H	L Z D R E L K	F A X I Y D A

73	74	75
G H T T O M O	R R O W M O R	N I N G
4 2 5 5 1 3 1	4 4 1 5 3 1 4	2 2 2 4
1 1 1 1 4 4 4	4 4 4 4 4 4 4	2 3 3 1
K Z L X X O R	R P E R R R R	N C I E

1. The steps taken in recovering the original substitution checkerboard demonstrate that cyclic permutations of a correct checkerboard will serve to decipher such a cryptogram just as well as the original checkerboard. In other words, a cryptogram prepared according to this method is decipherable by factorial 5 (5 x 4 x 3 x 2 x 1 = 120) checkerboards, all of which are cyclically equivalent. Even though the identities of the components will be different if the same message is enciphered by two different cyclically-equivalent checkerboards, when these components are

recombined, they will yield identical cipher texts, and therefore so far as external appearances are concerned different checkerboards yield identical cryptograms. The reason that there are only factorial 5 cyclically-equivalent checkerboards and not factorial 10, is that whatever permutation is applied to the row coordinates must be the same as that applied to the column coordinates in order that the aforesaid relationship hold true. If two checkerboards have identical row coordinates but different column coordinates certain portions of the cryptographic text will decipher correctly, others incorrectly. For this reason, in working with cryptograms of this type the cryptanalyst may successfully use a checkerboard which is incorrect in part and correct it as he progresses with the solution. It may also be added that the actual permutation of digits applied to the side and top of the checkerboard is of no consequence, so long as the permutations are identical. In other words, the permutation 5-2-1-3-4 will work just as well as 3-2-4-1-5, or 1-2-3-4-5, etc., so long as the same permutation is used for both row and column coordinates. It is the order of the rows and columns in the checkerboard which is the determining element in this system. Any arrangement (of the letters within the checkerboard) which retains the original order as regards the letters within rows and columns will work just as well as the original checkerboard.

m. A final remark may be worth adding. After all, the security of cryptograms enciphered by the bifid fractionating method rests upon the secrecy inherent in a single mixed alphabet. In ordinary substitution, a single mixed alphabet hardly provides any security at all. Why does the bifid system, which also uses only a single mixed alphabet, yield so much higher a degree of security? Is it because of the transpositional features involved? Thinking about this point gives a negative answer, for after all, finding the length of the periods and replacing the cryptographic text by components based upon the cipher letters is a relatively easy matter. The transpositional features are really insignificant. No, the answer to the question lies in a different direction and may be summed up about as follows. In solving a simple mixed-alphabet substitution cipher one can attack a few cipher letters (the ones of greatest frequency) and find their equivalents, yielding fragments of good plain text here and there in the cipher text. Once a few values have been established in this manner, say 6 values, the remaining 20 values can be found almost from the context alone. And in establishing these 6 values, the letters involved are not so interrelated that all 6 have to be ascertained simultaneously. <u>The cryptanalyst may establish the values one at a time</u>. But in the case of the bifid system the equivalents of the plain-text letters are so interrelated that the cryptanalyst is forced to establish the positions of several letters in the checkerboard simultaneously, not one by one. In other words, to use an analogy which may be only partially justified, the solution of a simple monoalphabetic substitution cipher is somewhat like forcing one's way into an inner chamber which has a number of doors each having a single lock; the solution of a bifid fractionated cipher is somewhat like getting into a vault--there is only one door which is provided with a complex 5-combination lock and all the tumblers of the lock must be positioned correctly <u>simultaneously</u> before the releasing lever can drop into the slot and the door opened. Fundamentally, this principle is responsible for the very much greater security of the bifid system as compared with that afforded by the simple monoalphabetic system. It is a principle well worth remembering and speculating upon.

48. Special solutions for bifid systems. - a. The security of the bifid system is very considerably reduced if the situation in which it is employed happens to be such that two or more messages with identical beginnings, endings, or internal portions can often be expected to occur. For in this case it is possible to establish equivalencies between components and quickly reconstruct the substitution checkerboard. An example will be given to illustrate the steps in a specific case.

b. Here are two cryptograms transmitted by two coordinate units to a superior headquarters at about the same time. They show certain identities, which have been underlined.

1. QVBBL YXNAB QBDOY HONDW VUYTE MHQZD QTLKE EWAFK QSLIP QDWC

2. VBNHY XDABG DOIHO BNWVL YTFWH QXDQV LKEWW AXDQS ABCAN XGX

c. Apparently these two cryptograms contain almost identical texts. In order to bring the identities into the form of superimposed components, it is necessary to transcribe the texts into periods of 7 and to superimpose the two messages as shown in Fig. 93.

d. The shifting of the 2d cryptogram 2 intervals to the right brings about the superimposition of the majority of θ_1 and θ_2 components and it may be assumed that for the most part the texts are identical. Allowing for slight differences at the beginnings and ends of the two messages, suppose a table of equivalencies is drawn up, beginning with the 8th superimposed pairs. Thus, $\overset{N_1}{Q_2} = \overset{N_2}{D_1}$; hence $Q_2 = D_1$. $\overset{N_2}{B_1} = \overset{H_1}{D_2}$; hence $N_2 = H_1$ and $B_1 = D_2$. Going through the text in this manner and terminating with the 42d superimposed pairs, the results are tabulated as shown in Fig. 94.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Q_1	Q_2	V_1	V_2	B_1	B_2	B_1	N_1	W_2	A_1	A_2	B_1	B_2	Q_1	Y_1	Y_2	E_1	H_2	O_1	O_2	N_1	U_1	U_2	Y_1	Y_2	T_1	T_2	E_1
B_2	L_1	L_2	Y_1	Y_2	X_1	X_2	Q_2	B_1	B_2	D_1	D_2	O_1	O_2	N_2	D_1	D_2	W_1	W_2	V_1	V_2	E_2	M_1	M_2	H_1	H_2	Q_1	Q_2
Q	V	B	B	L	Y	X	N	A	B	Q	B	D	O	Y	H	O	N	D	W	V	U	Y	T	E	M	H	Q
		V_1	V_2	B_1	B_2	N_1	N_2	H_1	A_1	A_2	B_1	B_2	G_1	G_2	B_1	H_1	H_2	O_1	O_2	B_1	B_2	N_1	Y_1	Y_2	T_1	T_2	F_1
		H_2	Y_1	Y_2	X_1	X_2	D_1	D_2	B_2	D_1	D_2	O_1	O_2	I_1	I_2	N_2	W_1	W_2	V_1	V_2	L_1	L_2	W_2	H_1	H_2	Q_1	Q_2
		V	B	N	H	Y	X	D	A	B	G	B	D	O	I	H	O	B	N	W	V	L	Y	T	F	W	H

29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49		
Z_1	Z_2	D_1	D_2	Q_1	Q_2	T_1	E_1	E_2	W_1	W_2	A_1	A_2	P_1	L_1	L_2	I_1	I_2	P_1	P_2	Q_1		
T_2	L_1	L_2	K_1	K_2	E_1	E_2	P_2	K_1	K_2	Q_1	Q_2	S_1	S_2	Q_2	D_1	D_2	W_1	W_2	C_1	C_2		
Z	D	Q	T	L	K	E	E	W	A	P	K	Q	S	L	I	F	Q	D	W	C		
F_2	W_1	D_1	D_2	Q_1	Q_2	V_1	V_2	L_1	W_1	W_2	A_1	A_2	X_1	X_2	D_1	B_1	B_2	C_1	C_2	A_1	A_2	N_1
X_1	X_2	L_2	K_1	K_2	E_1	E_2	W_1	W_2	D_2	Q_1	Q_2	S_1	S_2	A_1	A_2	N_2	X_1	X_2	G_1	G_2	X_1	X_2
Q	X	D	Q	V	L	K	E	W	W	A	X	D	Q	S	A	B	C	A	N	X	G	X

FIGURE 93.

$\theta_1\theta_2$ .. =	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
		D_2		Q_2	F_1	E_1		N_2	N_2	W_2	E_2	L_2	N_2		X_1				V_1	B_2	T_1	Z_2	T_2	G_2	F_2
		Y_2		I_2	V_2						X_2		B_1								P_1				
		N_1											U_2												

$\theta_2\theta_1$ .. =	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
		U_1		B_1	L_1	Z_1	Y_1		D_1	D_2	M_1	W_2	N_1			D_1			X_1	N_1	E_1	M_2	L_1	B_1	W_1
				N_2									H_1									K_1			
				K_2									I_1												
													D_2												

FIGURE 94.

e. From these equivalencies it is possible to reconstruct, if not the entirely, then at least a portion of the substitution checkerboard. For example, the data show that N, H, and I belong in the same row, E and F belong in the same row, N and K belong in the same column, and so on. Experimentation to make all the data fit one checkerboard would sooner or later result in reconstructing the checkerboard shown in Fig. 92, and the two messages read as follows:

1. SEVENTH INFANTRY IN POSITION TO ATTACK AT FOUR AM PLAN FOUR.

2. TENTH INFANTRY IN POSITION TO ATTACK AT FOUR AM PLAN THREEX.

f. The foregoing gives a clue to what would happen in the case of an extensive traffic in which long phrases or entire sentences may be expected to occur repeatedly. By a proper indexing of all the material, identical sequences would be uncovered and these, attacked along the lines indicated, would soon result in reconstructing the checkerboard, whereupon all the messages may be read with ease.

49. Solution of trifid systems. - a. In the trifid fractionating system the cipher alphabet is tripartite in nature, that is, the plain-text letters are represented by permutations of 3 components taken in groups of 3's, thus forming a set of 27 equivalents, such as that shown below:

A = 111	J = 211	S = 311
B = 112	K = 212	T = 312
C = 113	L = 213	U = 313
D = 121	M = 221	V = 321
E = 122	N = 222	W = 322
F = 123	O = 223	X = 323
G = 131	P = 231	Y = 331
H = 132	Q = 232	Z = 332
I = 133	R = 233	? = 333

b. The equivalents may, of course, be arranged in a mixed order, and it is possible to use one tripartite alphabet for decomposition and a wholly different one for recomposition. One disadvantage of such an alphabet is that it is a 27-element alphabet and therefore some subterfuge must be adopted as regards the 27th element, such as that illustrated in the footnote to Par. 57 of Special Text No. 166, Advanced Military Cryptography, wherein ZA stands for Z and ZB for the 27th character.

c. The various types of fractionation possible in bifid systems are also adaptable in trifid systems. For example, using the alphabet shown above for recomposition as well as decomposition the encipherment of a message in periods of 5 is as follows:

R E L I E F O	F Y O U R R E	G I M E N T T	O M O R R O W
2 1 2.1 1 1.2	1 3 2.3 2 2.1	1 1 2.1 2 3.3	2 2 2.2 2 2.3
3 2.1 3 2.2 2	2 3.2 1 3.3 2	3 3.2 2 2.1 1	2 2.2 3 3.2 2
3.2 3 3.2 3 3	3.1 3 3.3 3 2	1.3 1 2.2 2 2	3.1 3 3.3 3 2
K A Q H O R R	H W F L X I Z	B F ? N A T N	N N W R O I Z

Cryptogram ... K A Q H O R R H W F L X I Z A B F Z B N A T N N N W R O I Z

d. The solution of a single cryptogram of this nature would be a quite difficult matter, especially if there were nothing upon which to make assumptions for probable words. But a whole series of cryptograms could be solved, following in general the procedure outlined in the case of the bifid system, although the solution is, admittedly, much more complicated. The first step is to ascertain the length of the period, and when this has been done, transcribe the cipher text into components, which in their vertical combinations then represent monoalphabetic equivalents, with of course many variants for each letter of the plain text. Then a study is made to establish component equivalents, just as in the bifid system. If the text is replete with repetitions, or if a long word or a short phrase may be assumed to be present, a start may be made and once this sort of entering wedge has been forced into the structure, its further disintegration and ultimate complete demolition is only a matter of time and patience.

50. Concluding remarks on fractionating systems. - a. It goes without saying that the basic principles of fractionation in the bifid and trifid systems are susceptible to a great deal of variation and complication. For example, instead of having periods of fixed length through the message, it is possible to vary the length of the periods according to some simple or complex key suitable for this purpose. Or, the bifid and trifid systems may be combined into a single scheme, enciphering a text by the bifid method and then reenciphering the cipher text by the trifid method.

and so on. Systems of this sort may become so complex as to defy analysis, especially if the keys are constantly and frequently varied so that no great amount of traffic accumulates in any single key. Fortunately for the cryptanalyst, however, such complex systems as these, if introduced into actual usage, are attended by so many difficulties in practice that the enemy cryptographic service would certainly break down and it would not be long before requests for repetition, the transmission of the same cryptogram in different keys, and so on would afford clues to solution. Could such systems be employed successfully in field service there is no doubt that from the standpoint of security, the cryptograms would be theoretically secure. But the danger of error and the slowness with which they could be operated by the usual cryptographic clerks are such that systems of this complexity can hardly be employed in the field, and therefore the cryptanalyst may not expect to encounter them.

b. However, the simple bifid system, the ADFGVX system and the like are indeed practicable for field use, have been used with success in the past, and may be expected to be in use in the future. It is therefore advisable that the student become thoroughly familiar with the basic principles of their solution and practice the application of these principles as frequently as possible. In this connection, the attention of the student is directed to the fact that there is theoretically no reason why the bipartite components of the ADFGVX system cannot be recombined by means of the same or a different checkerboard, thus reducing the cryptographic text to a form wherein it consists of 25 different letters, and at the same time cutting the length of the messages in half. The matter is purely one of practicability: it adds one more step to the process.

But it must not be overlooked that this additional step would add a good deal of strength to the system, for it would shorten, mask, distort, or entirely eliminate similar beginnings and similar endings--the two most fruitful sources of attack on this system.

51. Concluding remarks on transposition systems. - a. Simple transposition systems hardly afford any security at all, complex ones may in the case of individual or single messages afford a high degree of security. But just as soon as many cryptograms in the same key are transmitted the chances of finding two or more cryptograms of identical length become quite good and the general solution may be applied.

b. Contrary to the situation in the case of substitution, in that of transposition wherein the letters of the plain-text itself are transposed (not code) the shorter the cryptogram the greater the possibility of solution. For, in the case of a message of say only 25 or 30 letters, one might shift the letters about and actually reconstruct the plain text as one does in the case of the game called "anagrams." Of course, several different "solutions" may thus be obtained, but having such "solutions" it may be possible to reconstruct the system upon which the transposition was based and thus "prove" one of the solutions.

c. The text has confined itself almost entirely to cases of uniliteral transposition, in order to demonstrate basic principles. But there is inherently no reason why transposition may not be applied to digraphs, trigraphs, or tetragraphs. If longer sequences are used as the units of transposition the security decreases very sharply, as in the case of the ordinary route ciphers of the Civil War period.

d. Transposition designs, diagrams, or patterns are susceptible of yielding cryptograms of good security, if they are at all irregular or provide for nulls and blank spaces. Such devices are particularly difficult to solve if frequently changed.

e. Transpositions effected upon fixed-length sequences of plain text yield a low degree of security but when a transposition is applied to the cipher text resulting from a good substitution system or to the code text of cryptograms first encoded by means of an extensive codebook the increase in the cryptographic security of such cryptograms is quite notable. In fact, transposition methods and designs are frequently used to "superencipher" substitution text or code and play a very important role in this field. Their great disadvantage is that inherent in all transposition methods: the addition or deletion of a single letter or two often makes the entire cryptogram unreadable even with the correct key.

f. The clues afforded by messages with similar beginnings, endings, or internal portions, and by repetitions of incorrectly enciphered messages without paraphrasing the original text are often sufficient to make a solution possible or to facilitate a solution. For this reason the cryptanalyst should note all cases wherein clues of this sort may be applicable and be prepared to take full advantage of them.

g. Following out the scheme initiated in the first text, an analytical key applicable to the subject-matter in this text will be found on page 218.

Analytical Key for Military Cryptanalysis, IV
(Numbers in parenthesis refer to paragraph numbers in this text)

- 303-Pure Transposition (1-51)
  - 405-Monophase systems (3)
    - 507-Uniliteral systems
      - 617-Geometric designs and patterns (5, 30-34)
        - 719-Route systems (5)
        - 720-Grille systems (30-34)
          - 817-Fixed (30-33)
            - 905-One position (30)
            - 906-Multiple positions (31-33)
          - 818-Indefinite (34)
        - 721-Misc. (50)
      - 618-Columnar transposition methods (6-16)
        - 722-Incompletely filled rectangles (12-16)
        - 723-Completely filled rectangles (6-11)
      - 619-Other methods (4, 30) Miscellaneous methods such as reversed writing, rail-fence writing, etc. (4)
    - 508-Polyliteral systems
      - 620-Regular-length groupings (Digraphs, trigraphs, polygraphs) (5)
      - 621-Irregular-length groupings (Word lengths) (1d)
  - 406-Polyphase systems (3) (Double transposition) (26-29)
- 305-Combined substitution-transposition systems (35-51)
  - 407-Fractionating systems (37-50)
    - 509-Bifid, trifid, polyfid systems (44-50)
    - 510-Bipartite substitution with columnar transposition ADFGVX system (37-43)
  - 408-Other systems (35-36)
    - 511-Monoalphabetic with transposition (35)
    - 512-Polyalphabetic with transposition (36)

INDEX

Page