CONFIDENTIAL

~~RESTRICTED~~

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON

MILITARY CRYPTANALYSIS

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~~

1939

CONFIDENTIAL

30 April 1959

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

Paul S. Willard
Colonel, AGC
Adjutant General

REF ID:A56913

~~CONFIDENTIAL~~

MILITARY CRYPTANALYSIS, PART IV

TRANSPOSITION AND FRACTIONATING SYSTEMS

CONTENTS

SECTION I.

GENERAL

Paragraph

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 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	D	5	D	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 I 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 <u>B N T S E</u> A R K C and the 1st column of No. 2 will contain the letters <u>B N T S E</u> I N D O T; the 2d column of No. 1 will contain the letters <u>L C E T</u> T N B I T and the 2d column of No. 2 will contain the letters <u>L C E T</u> 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	2
B L E N T	B L E N T
N C R N O	N C R N O
T E R O K	T E R O K
S T O N M	S T O N M
E T T N S	E S M S F
A N A E Z	I A O T E
R B E N T	N F I I Y
K I L O G	D P S I K
C T T O N	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.

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

```
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
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
S R B E N   1 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.

```
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
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
C I A A I   N S C W N   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

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

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

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

No. 2

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

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

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

STOP
Jump to 114

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

SECTION VIII

SOLUTION OF THE ADFGVX SYSTEM

Paragraph

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.

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. 1.

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						

No. 2.

FIGURE 48.

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. 1.

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						

No. 2.

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, <u>viz</u>, in columns 5 and 12.

<u>c</u>. Now comes the attempt to place the columns in proper sequence in the respective transposition rectangles. Since No. 6 has only 2 long columns, <u>viz</u>, 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 even, 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 this distribution, if it is at all normal, will afford a basis for matching other columns which will produce similar distributions, 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.

STOP

f. But now consider a plain-text rectangle in the ADFGVX system, in which the number of columns is odd, 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 e apply equally to this case where the width of the rectangle is odd.