REF ID:A57070

11-1

~~SECRET~~

Register No. 125

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON

GENERAL SOLUTION FOR THE DOUBLE TRANSPOSITION CIPHER

Declassified and approved for release by NSA on 05-19-2014 pursuant to E.O. 13526

Helen D. Siegl

~~SECRET~~

Register No. 125

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

GENERAL SOLUTION FOR THE DOUBLE TRANSPOSITION CIPHER

TECHNICAL PAPER

By

SOLOMON KULLBACK, Ph.D.
Junior Cryptanalyst

SIGNAL INTELLIGENCE SECTION
WAR PLANS AND TRAINING DIVISION

UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON: 1934

CONTENTS

Section		Page
I.	Introductory remarks	1
II.	Analysis of system and general procedure	2–4
III.	Reconstruction of key, solution known	5–8
IV.	Reconstruction of key, plain-text positions of several cipher letters known	9–13
V.	Reconstruction of key, relative positions in plain-text of several cipher letters being known	14–17
VI.	Solution of messages enciphered by double transposition cipher system	18
VII.	Double transposition with different keys	19–23
Appendix		25–27

GENERAL SOLUTION FOR THE DOUBLE TRANSPOSITION CIPHER

SECTION I

INTRODUCTORY REMARKS

	Paragraph		Paragraph
Nature of investigation	1	Summary of conclusions	3
Purpose of this paper	2		

1. **Nature of investigation.**—It is known that two or more messages of identical length, enciphered by means of a double transposition system, may be read by anagramming. It was conjectured that the very nature of the system is such that some pseudomathematical procedure could be devised for the solution of single messages or messages of different lengths enciphered by means of a double transposition system.

2. **Purpose of this paper.**—This paper was written for the purpose of setting forth in detail the results of a study for a general method of solution of the double transposition cipher system. The method herein described is novel in cryptography and presents a principle which may be of value for other types of transposition. A preliminary knowledge of the more important and fundamental principles of cryptanalysis, particularly with regard to transposition systems, is advisable, though not absolutely necessary, for a proper understanding of the details of this analysis. Reference is therefore made to Signal Corps Training Pamphlet No. 3, "Elements of Cryptanalysis", wherein will be found elucidated the basic principles of the science. The method of procedure, though mathematical in nature, makes no heavy demands on the mathematical knowledge and ability of the reader.

3. **Summary of conclusions.**—It is shown in this paper that it is possible to solve a single message, or several messages of different lengths enciphered by means of a double transposition cipher system. The ease and speed with which the solution may be attained will depend on the number of cryptanalysts, the general situation, etc., and no attempt has been made to estimate an average time of solution.

REF ID:A57071

SECTION II

ANALYSIS OF SYSTEM AND GENERAL PROCEDURE

	Paragraph		Paragraph
General considerations	4	Number of different cipher resultants possible with given key and message	7
Notation	5		
Plain-text cipher-text relationships	6		

4. **General considerations.**—The general method herein presented for the solution of a double transposition cipher involves some notions which may not be familiar and are therefore discussed in this section.

Consider the fundamental element of a transposition method. Transposition is a process which does not change the identity of the letters of a message but does change their relative positions. As a result of any transposition, the separate letters of the plain text are rearranged in some new order. It will be found of value to consider this process as one in which a letter of the plain text is replaced by some other letter of the plain text. Consider, for example, a columnar transposition with key 2–5–6–1–4–3 applied to a message of 50 letters. It will be found convenient in what follows to disregard the identity of the letters and represent them by numbers giving their position in the plain text. Thus, 1 will mean the first plain-text letter; 2, the second plain-text letter; etc.

2	5	6	1	4	3
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	45	46	47	48
49	50				

FIGURE 1

The cipher text, obtained by columnar transposition, in terms of these numbers is 04–10–16–22–28–34–40–46–01–07–13–19–25–31–37–43–49–06–12–18–24–30–36–42–48–05–11–17–23–29–35–41–47–02–08–14–20–26–32–38–44–50–03–09–15–21–27–33–39–45.

The above notation means that the first cipher letter is the fourth plain-text letter, the second cipher letter is the tenth plain-text letter, etc. This may be represented as follows:

C_0----	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
C_1----	04	10	16	22	28	34	40	46	01	07	13	19	25	31	37	43	49	06	12	18
C_0----	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
C_1----	24	30	36	42	48	05	11	17	23	29	35	41	47	02	08	14	20	26	32	38
C_0----	41	42	43	44	45	46	47	48	49	50										
C_1----	44	50	03	09	15	21	27	33	39	45										

FIGURE 2

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38
39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57
58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76
77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95
96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114
115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133
134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152
153 154

Here the number in line C_0 represents the position in the cipher text of the letter whose position in the plain text is given directly beneath it. (Notice that the sequence of numbers of C_1 are those of the columns of figure 1. The columns have been rearranged according to the key and written horizontally in sequence.)

5. **Notation.**—For convenience, the following notation will be used: C_0 will represent the plain text *and also* will be used to enumerate the positions in the cipher text; C_1 will represent the cipher text resulting from the first transposition and thus also the "plain text" for the second transposition; C_2 will represent the cipher text resulting from the second transposition.

It is seen from figure 2 that the transposition in question replaces the first plain-text letter by the fourth, the second plain-text letter by the tenth, the third plain-text letter by the sixteenth, etc.

To effect the second transposition the same operation must be performed on C_1 that was performed on C_0. The first letter of C_1 (4 of C_0) must be replaced by the fourth letter of C_1 (22 of C_0); the second letter of C_1 (10 of C_0) must be replaced by the tenth letter of C_1 (7 of C_0); the third letter of C_1 (16 of C_0) must be replaced by the sixteenth letter of C_1 (43 of C_0), etc.

The operations discussed above may be represented as in figure 3. In figure 4 is shown the result of the operations, where again C_0 is the plain text (and also used to enumerate the positions), C_1 the result of the first transposition and C_2 the result of the second transposition.

This scheme can now be used to effect a double transposition with the same key.

T_1

C_0	C_1
01	04
02	10
03	16
04	22
05	28
06	34
07	40
08	46
09	01
10	07
11	13
12	19
13	25
14	31
15	37
16	43
etc.	

$T_1 \times T_1 = T_2$

C_0	C_1	C_1	C_2	C_0	C_2
01	04	04	22	01	22
02	10	10	07	02	07
03	16	16	43	03	43
04	22				
		etc.			

FIGURE 3

REF ID:A57071

C_0	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
C_1	04	10	16	22	28	34	40	46	01	07	13	19	25	31	37	43	49	06	12	18
C_2	22	07	43	30	17	02	38	21	04	40	25	12	48	35	20	03	39	34	19	06

C_0	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
C_1	24	30	36	42	48	05	11	17	23	29	35	41	47	02	08	14	20	26	32	38
C_2	42	29	14	50	33	28	13	49	36	23	08	44	27	10	46	31	18	05	41	26

C_0	41	42	43	44	45	46	47	48	49	50
C_1	44	50	03	09	15	21	27	33	39	45
C_2	09	45	16	01	37	24	11	47	32	15

FIGURE 4

6. **Plain-text cipher-text relationships.**—Since the same operation has been effected twice, there ought to exist a "plain-text cipher-text" relationship between (C_0C_1) and (C_1C_2) which remains invariant. Such a relationship does exist. Notice that the pairs in (C_0C_1) are the same as those in (C_1C_2); their relative positions have been changed. For example, under 1 in C_0, we find 4 in C_1; under 1 in C_1, we find 4 in C_2; under 2 in C_0, we find 10 in C_1; under 2 in C_1, we find 10 in C_2, etc.

If a third, fourth, . . . *n*th transposition is effected with the same key, the same phenomenon will occur and can be used to find C_3, C_4, . . . C_n readily. The pairs in (C_0C_1), (C_1C_2), (C_2C_3), (C_3C_4) . . . will all be the same so that C_3 can be found by writing under C_2 the numbers to form the pairs already determined by (C_0C_1).

7. **Number of different cipher resultants possible with given key and message.**—It is possible to determine the number of transpositions which may be effected with a given key on a message before the original message is obtained. Using the scheme of figure 4 and the message already discussed, the numbers of C_1, C_2, C_3, . . . C_n appearing under the 1 of C_0 will be limited to a particular set. The number of elements in this set depends on the number of steps in the chain 1→4, 4→22, 22→30, . . . , 44→9, 9→1, i.e., 38. Similarly, the set of numbers corresponding to any element in this chain will be of the same length. The last number in any one of these 38 sets is always the same as the corresponding number in C_0 so that any number of transpositions which is a multiple of 38 will always make the first cipher letter the first plain-text letter, the fourth cipher letter the fourth plain-text letter, etc.

The message being 50 letters long, there are still 12 unaccounted for, the smallest of which is 3. We can form a chain for this number in the same way as for 1, viz, 3→16, 16→43, 43→3 whose length is 3. Any number of transpositions which is a multiple of 3 will make the third, sixteenth, and forty-third plain-text letters become the third, sixteenth, and forty-third cipher letters, respectively.

Continuing this process all 50 letters may be accounted for. In this particular case four chains were needed of lengths 38, 7, 3, and 2. In order that the plain and cipher texts be identical, the number of transpositions used must involve each of these numbers as a factor. The smallest number possible is therefore the least common multiple of them, 3×7×38, or 798.

This same notion is applicable to any type of transposition and will determine how many steps are needed to regain the original text as a cipher message.

(7) 11-13-25-48-33-47-27-11

(2) 12-19-12

REF ID:A57071

SECTION III

RECONSTRUCTION OF THE KEY, THE SOLUTION BEING KNOWN

	Paragraph
Application of paired relationships	8
Test of assumptions	9

8. **Application of paired relationships.**—The notions set forth in section II may be used to great advantage for the solution of messages enciphered by means of a double transposition. The method will be illustrated by several examples, increasing in difficulty.

Suppose several messages, enciphered by means of a double transposition, have been read by anagramming messages of identical length. In order to read other messages in this same key, but of different length, it is necessary to know the key, which can be recovered by applying some of the ideas set forth in section II.

Let us refer for a minute to figure 4. The knowledge of line C_1 is sufficient to recover the key since $\begin{Bmatrix} C_0 & 1 \\ C_1 & 4 \end{Bmatrix}$ indicates that the fourth column was read first, $\begin{Bmatrix} C_0 & 9 \\ C_1 & 1 \end{Bmatrix}$ shows that the first column was next transcribed, $\begin{Bmatrix} C_0 & 18 \\ C_1 & 06 \end{Bmatrix}$ shows that the sixth column was the third one transcribed, etc.

The complete key is thus found to be:

$$\text{Key} \begin{Bmatrix} 2 & 5 & 6 & 1 & 4 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{Bmatrix}$$

If the message has been read by anagramming, lines C_0 and C_2 are both known, but C_1 must be reconstructed before the key can be obtained. The method for reconstructing C_1 is, in general terms, to assume a width which will enable one to arrange the sequence of numbers of C_1 to insure proper pairing of (C_0C_1) and (C_1C_2). The procedure will be illustrated by using the message of figure 4, assuming C_1 unknown. Let us write the numbers of C_0 and C_2, leaving space for C_1.

C_0----	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
C_1----																				
C_2----	22	07	43	30	17	02	38	21	04	40	25	12	48	35	20	03	39	34	19	06
C_0----	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
C_1----																				
C_2----	42	29	14	50	33	28	13	49	36	23	08	44	27	10	46	31	18	05	41	26
C_0----	41	42	43	44	45	46	47	48	49	50										
C_1----																				
C_2----	09	45	16	01	37	24	11	47	32	15										

Figure 5

9. **Test of assumptions.**—Let us assume that the keyword is not less than five letters in length. As a first case then, suppose the width of the rectangle to be five. The first number of C_1 must then be 1, 2, 3, 4, or 5.

If it is 1, then the next several are 1, 6, 11, 16, 21, 26, 31, 36, 41, 46; we stop with 46 since 51 is not possible, there being but 50 letters in the message. Writing these numbers in their positions, we have

C_0---- 01 02 03 04 05 06 07 08 09 10, etc.
C_1---- 01 06 11 16 21 26 31 36 41 46, etc.
C_2---- 22 07 43 30 17 02 38 21 04 40, etc.

FIGURE 6

This is impossible since 1→1 in (C_0C_1) contradicts 1→22 in (C_1C_2).
The remaining possibilities for width 5 yield similar contradictions, as shown below:

Assumption	Contradiction
C_0---- 01 02 03 04 05 06 . . .	C_0 02 C_1 02
C_1---- 02 07 12 17 22 27 . . .	C_1 07 C_2 22
C_2---- 22 07 43 30 17 02 . . .	
C_0---- 01 02 03 04 05 06 . . .	C_0 03 C_1 03
C_1---- 03 08 13 18 23 28 . . .	C_1 13 C_2 22
C_2---- 22 07 43 30 17 02 . . .	
C_0---- 01 02 03 04 05 06 . . .	C_0 04 C_1 04
C_1---- 04 09 14 19 24 29 . . .	C_1 19 C_2 22
C_2---- 22 07 43 30 17 02 . . .	
C_0---- 01 02 03 04 05 06 . . .	C_0 05 C_1 05
C_1---- 05 10 15 20 25 30 . . .	C_1 25 C_2 22
C_2---- 22 07 43 30 17 02 . . .	

FIGURE 7

The transposition rectangle therefore cannot be five columns wide.

On the assumption of width 6, the initial number of C_1 may be any one of the numbers 1 to 6. The first three yield immediate contradictions.

Assumption	Contradiction
C_0---- 01 02 03 04 05 06 . . .	C_0 01 C_1 01
C_1---- 01 07 13 19 25 31 . . .	C_1 01 C_2 22
C_2---- 22 07 43 30 17 02 . . .	
C_0---- 01 02 03 04 05 06 . . .	C_0 02 C_1 02
C_1---- 02 08 14 20 26 32 . . .	C_1 08 C_2 22
C_2---- 22 07 43 30 17 02 . . .	
C_0---- 01 02 03 04 05 06 . . .	C_0 03 C_1 03
C_1---- 03 09 15 21 27 33 . . .	C_1 15 C_2 22
C_2---- 22 07 43 30 17 02 . . .	

FIGURE 8

REF ID:A57071

For the assumption $\begin{Bmatrix} C_0 & 1 \\ C_1 & 4 \end{Bmatrix}$ there is found

C_0---- 01 02 03 04 05 06 07 08 . . .
C_1---- 04 10 16 22 28 34 40 46 . . .
C_2---- 22 07 43 30 17 02 38 21 . . .

FIGURE 9

This is possible since we have 4→22 in both (C_0C_1) and (C_1C_2). Since (C_1C_2) yields 10→7, (C_0C_1) should also yield 10→7. Inserting 7 in C_1 under 10 of C_0, no contradiction is obtained, since there is room in C_1 for the number 1 which must precede 7 and we find that both (C_0C_1) and (C_1C_2) yield 1→4. We now have—

C_0---- 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20
C_1---- 04 10 16 22 28 34 40 46 01 07 13 19 25 31 37 43 49
C_2---- 22 07 43 30 17 02 38 21 04 40 25 12 48 35 20 03 39 34 19 06
C_0---- 21 22 23 . . .
C_1----
C_2---- 42 29 14 . . .

FIGURE 10

Notice the further checks: 16→43; 13→25 in both (C_0C_1) and (C_1C_2).

Since in (C_1C_2) we find 22→30, we insert in C_1 the number 30 under the 22 of C_0. There is no contradiction, as there are just enough places for the numbers 06, 12, 18, 24, which must precede 30. We now have—

C_0---- 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
C_1---- 04 10 16 22 28 34 40 46 01 07 13 19 25 31 37 43 49 06 12 18 24
C_2---- 22 07 43 30 17 02 38 21 04 40 25 12 48 35 20 03 39 34 19 06 42

C_0---- 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 . . .
C_1---- 30 36 42 48
C_2---- 29 14 50 33 28 13 49 36 23 08 44 27 10 46 31 18 05 41 26 09 . . .

FIGURE 11

The further checks can leave no doubt in our minds of the fact that we are on the right track. Since in (C_1C_2) we find 30→29, we insert 29 in C_1 under the 30 of C_0. We now have—

C_0---- 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
C_1---- 04 10 16 22 28 34 40 46 01 07 13 19 25 31 37 43 49 06 12 18 24
C_2---- 22 07 43 30 17 02 38 21 04 40 25 12 48 35 20 03 39 34 19 06 42

C_0---- 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 . . .
C_1---- 30 36 42 48 05 11 17 23 29 35 41 47
C_2---- 29 14 50 33 28 13 49 36 23 08 44 27 10 46 31 18 05 41 26 09 . . .

FIGURE 12

Since in (C_1C_2) we find 35→8 and 47→27, we insert 8 in C_1, under the 35 of C_0, and 27 in C_1 under the 47 in C_0. We now have—

C_0----	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
C_1----	04	10	16	22	28	34	40	46	01	07	13	19	25	31	37	43	49	06	12	18
C_2----	22	07	43	30	17	02	38	21	04	40	25	12	48	35	20	03	39	34	19	06

C_0----	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
C_1----	24	30	36	42	48	05	11	17	23	29	35	41	47	02	08	14	20	26	32	38
C_2----	42	29	14	50	33	28	13	49	36	23	08	44	27	10	46	31	18	05	41	26

C_0----	41	42	43	44	45	46	47	48	49	50
C_1----	44	50	03	09	15	21	27	33	39	45
C_2----	09	45	16	01	37	24	11	47	32	15

FIGURE 13

Having reconstructed C_1, it is a very simple matter to find the key.

REF ID:A57071

SECTION IV

RECONSTRUCTION OF THE KEY, THE PLAIN-TEXT POSITIONS OF SEVERAL OF THE CIPHER LETTERS BEING KNOWN

	Paragraph		Paragraph
The problem presented	10	Testing assumptions	12
Preliminary considerations	11		

10. **The problem presented.**—Suppose the following message is intercepted (the enemy is known to be using double transposition).

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

Later a C. P. is captured and the following plain text found without the work sheets.

IN CASE OF GENERAL ATTACK THE MAIN LINE OF DEFENSE WILL BE HELD.

In order to read other messages, we must reconstruct the key. A frequency table (fig. 14) shows the message to have but one B, G, K, M, R, W.

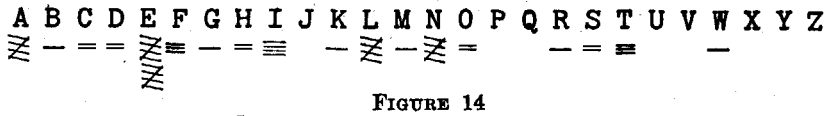

FIGURE 14

We can definitely correlate these letters in the cipher text with the same letters in the plain text.

11. **Preliminary considerations.**—Let us assign the numerical positions to those letters which are definitely known. (The numbers in C_2 are the positions in the plain text of the corresponding letters in the cipher text, e.g., R is the thirteenth letter in the plain text, etc.)

C----	L	D	E	C	S	E	N	R	E	O	T	N	E	H	E	B	N	G	L	I
C_0----	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
C_1----	3	9	15	21	27	33	39	45	51	6	12	18	24	30	36	42	48	2	8	14
C_2----	15	51	36	10				13								46		09		

C----	A	L	D	T	O	I	I	E	H	E	T	A	S	M	K	E	W	A	N	E
C_0----	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
C_1----	20	26	32	38	44	50	5	11	17	23	29	35	41	47	4	10	16	22	28	34
C_2----														25	21		42			

C----	F	A	C	N	E	F	L	L	A	I	F
C_0----	41	42	43	44	45	46	47	48	49	50	51
C_1----	45	46	1	7	13	19	25	31	37	43	49
C_2----			3	39							

FIGURE 15

We will find it convenient to write down the numbers corresponding to columns of different widths for a message of 51 letters, since the numbers of C_1 are these columns rearranged, each column being kept as a unit. We thus have, for example, for widths 5–7:

1__	01	02	03	04	05
2__	06	07	08	09	10
3__	11	12	13	14	15
4__	16	17	18	19	20
5__	21	22	23	24	25
6__	26	27	28	29	30
7__	31	32	33	34	35
8__	36	37	38	39	40
9__	41	42	43	44	45
10__	46	47	48	49	50
11__	51				

(*a*)

1__	01	02	03	04	05	06
2__	07	08	09	10	11	12
3__	13	14	15	16	17	18
4__	19	20	21	22	23	24
5__	25	26	27	28	29	30
6__	31	32	33	34	35	36
7__	37	38	39	40	41	42
8__	43	44	45	46	47	48
9__	49	50	51			

(*b*)

1__	01	02	03	04	05	06	07
2__	08	09	10	11	12	13	14
3__	15	16	17	18	19	20	21
4__	22	23	24	25	26	27	28
5__	29	30	31	32	33	34	35
6__	36	37	38	39	40	41	42
7__	43	44	45	46	47	48	49
8__	50	51					

(*c*)

FIGURE 16

For a width 5 there is 1 column of 11 and 4 columns of 10 letters; for a width 6 there are 3 columns of 9 and 3 columns of 8 letters, etc. It will be found convenient to prepare a list showing the number of letters corresponding to various combinations of short and long columns; for example, for width 5 we have

$$1\times10=10,\ 1\times11=11,\ 2\times10=20,\ 1\times10+1\times11=21,\ 3\times10=30,$$
$$2\times10+1\times11=31,\ 4\times10=40,\ 3\times10+1\times11=41,\ 4\times10+1\times11=51$$

12. **Testing assumptions.**—Let us suppose the transposition rectangle was 5 columns wide. The number of C_1 under 8 of C_0 must be either 36, 37, 38, 39, or 40, since the first number of C_1 must be either 1, 2, 3, 4, or 5. (See fig. 16*a*.)

If it were 36, then under the 36 of C_0, we must place 13 of C_1. This is impossible, since this would place the beginning of a column[1] under 34 $\begin{cases} C_0: & 34\ 35\ 36 \\ C_1: & 03\ 08\ 13 \end{cases}$ and no combination of short and long columns will yield such a result. (No combination of 10's and one 11 is equal to 33.)

The remaining possibilities yield similar contradictions as shown below.

[1] By a column of C_1, we shall understand a sequence of numbers which come from a column of the transposition rectangle.

REF ID:A57071

Assumption	Contradiction	
C_0 08	C_0 35 36 37	$(n\times 10+11\neq 34)_1$
C_1 37	C_1 03 08 13	
C_2 13		
C_0 08	C_0 36 37 38	$(n\times 10+11\neq 35)$
C_1 38	C_1 03 08 13	
C_2 13		
C_0 08	C_0 37 38 39	$(n\times 10+11\neq 36)$
C_1 39	C_1 03 08 13	
C_2 13		
C_0 08	C_0 38 39 40	$(n\times 10+11\neq 37)$
C_1 40	C_1 03 08 13	
C_2 13		

FIGURE 17

The transposition rectangle is therefore not 5 columns wide.

Suppose the width to be 6. This means 3 columns of 9 and 3 columns of 8 letters. (See fig. 16*b*.)

$1\times 8=8$, $1\times 9=9$, $2\times 8=16$, $1\times 8+1\times 9=17$, $2\times 9=18$, $3\times 8=24$, $2\times 8+1\times 9=25$, $1\times 8+2\times 9=26$, $3\times 9=27$, $3\times 8+1\times 9=33$, $2\times 8+2\times 9=34$, $1\times 8+3\times 9=35$, $3\times 8+2\times 9=42$, $2\times 8+3\times 9=43$, $3\times 8+3\times 9=51$

The number of C_1 under the 8 of C_0 must be either 43, 44, 45, 46, 47, or 48. (See fig. 16*b*.)

If it were 43, then under the 43 of C_0, we must place 13 of C_1. This is impossible, since it would place the beginning of a column under 41.

If it were 44, then under the 44 of C_0, we must place 13 of C_1. This is impossible, since it would place the beginning of a column under 42.

If it were 45, then under the 45 of C_0, we must place 13 of C_1. This is possible, since it would place the beginning of a column under 43 and 3 short and 2 long columns make this possible. ($3\times 8+2\times 9=42$.) This information added to figure 15 gives the following:

	L	D	E	C	S	E	N	R	E	O	T	N	E	H	E	B	N	G	L	I
C_0----	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
C_1----	03	09	15	21	27	33	39	45	51											
C_2----								13								46		09		

	A	L	D	T	O	I	I	E	H	E	T	A	S	M	K	E	W	A	N	E
C_0----	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
C_1----																				
C_2----														25	21		42			

	F	A	C	N	E	F	L	L	A	I	F
C_0----	41	42	43	44	45	46	47	48	49	50	51
C_1----			01	07	13	19	25	31	37	43	49
C_2----											

FIGURE 18

[1] No combination of 10's and one 11 can equal 34.

There are several checks which seem to indicate that this is the correct arrangement. From (C_0C_1) we find 43→1 also 1→3. This means that under the 1 of C_1 must go 3 of C_2, indicating that the corresponding letter, C, is the third letter of the plain text. There is no contradiction, as the third plain-text letter is a C. Similarly, from 1→3, 3→15, we place 15 of C_2 under 3 of C_1. (See fig. 19.) This indicates that the corresponding letter, L, is the fifteenth letter of the plain text. There is no contradiction, as the fifteenth plain-text letter is an L, etc.

From (C_0C_1) we find 2→9; we must therefore place 2 of C_1 over the 9 of C_2. This involves no contradiction, as a column may begin under 18 of C_0 ($1\times8+1\times9=17$). From (C_0C_1) we find 4→21; we must therefore place 4 of C_1 over 21 of C_2. This involves no contradiction, as a column may begin under 35 of C_0 ($2\times9+2\times8=34$). Adding this new information, we have—

	L	D	E	C	S	E	N	R	E	O	T	N	E	H	E	B	N	G	L	I
C_0----	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
C_1----	03	09	15	21	27	33	39	45	51									02	08	14
C_2----	15							13								46		09		

	A	L	D	T	O	I	I	E	H	E	T	A	S	M	K	E	W	A	N	E
C_0----	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
C_1----	20	26	32	38	44	50									04	10	16	22	28	34
C_2----														25	21		42			

	F	A	C	N	E	F	L	L	A	I	F
C_0----	41	42	43	44	45	46	47	48	49	50	51
C_1----	40	46	01	07	13	19	25	31	37	43	49
C_2----			03								

FIGURE 19

From (C_1C_2) we can now obtain 16→42, so that 42 of C_1 goes under 16 of C_0. Inserting this, we have—

	L	D	E	C	S	E	N	R	E	O	T	N	E	H	E	B	N	G	L	I
C_0----	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
C_1----	03	09	15	21	27	33	39	45	51	06	12	18	24	30	36	42	48	02	08	14
C_2----	15							13										09		

	A	L	D	T	O	I	I	E	H	E	T	A	S	M	K	E	W	A	N	E
C_0----	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
C_1----	20	26	32	38	44	50									04	10	16	22	28	34
C_2----														25	21		42			

	F	A	C	N	E	F	L	L	A	I	F
C_0----	41	42	43	44	45	46	47	48	49	50	51
C_1----	40	46	01	07	13	19	25	31	37	43	49
C_2----			03								

FIGURE 20

REF ID:A57071

Obviously, the column headed by 5 must go into the blank spaces. From C_1 the key is found to be $\begin{Bmatrix} 6 & 3 & 1 & 5 & 4 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{Bmatrix}$. That this is correct may be verified by using the rectangle.

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

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

FIGURE 21

SECTION V

RECONSTRUCTION OF THE KEY, THE RELATIVE POSITION IN THE PLAIN TEXT OF SEVERAL LETTERS BEING KNOWN

	Paragraph		Paragraph
The problem presented	13	Testing assumptions	15
Preliminary considerations	14		

13. **The problem presented.**—Consider the following two messages of identical length.

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

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

Anagramming yields $\begin{Bmatrix} E & A & D & Q & U & A & R \\ C & A & V & A & L & R & Y \end{Bmatrix}$. It may be possible to read the messages completely by anagramming, but the following procedure is believed to be simpler.

14. **Preliminary consideration.**—Consider [1] the second message, assuming the width of the rectangle to be 8.

1----	01	02	03	04	05	06	07	08
2----	09	10	11	12	13	14	15	16
3----	17	18	19	20	21	22	23	24
4----	25	26	27	28	29	30	31	32
5----	33	34	35	36	37	38	39	40
6----	41	42	43	44	45	46	47	48
7----	49	50	51	52	53	54	55	56
8----	57	58	59					

FIGURE 22

[1] It is advisable that the reader himself carry out the steps outlined, writing the cipher message and C_0 in ink and C_1 and C_2 in pencil, to allow erasures.

REF ID:A57071

	S	A	U	T	L	A	N	I	F	N	L	A	N	H	T	R	A	E	U	V
C_0----	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
C_1----																				
C_2----																				
	N	H	M	T	E	S	S	S	H	E	O	T	Y	A	R	Y	T	T	W	E
C_0----	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
C_1----																				
C_2----																				
	R	C	N	V	C	I	G	I	R	N	O	I	A	D	A	R	O	A	H	
C_0----	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	
C_1----																				
C_2----																				

FIGURE 23

The underlined letters are those underlined in C A V A L R Y, viz, those which could be determined uniquely; there are two possibilities each for $\begin{Bmatrix} A \\ A \end{Bmatrix}$ and $\begin{Bmatrix} A \\ R \end{Bmatrix}$. If p represents the position of C in the plain text, the positions of V, A, L, Y are respectively $(p+2), (p+3), (p+4), (p+6)$.

15. **Testing assumptions.**—If the last three columns in C_1 were long, the numbers of C_1 corresponding to Y and V, letters number 36 and 44 of the cipher text, respectively, would be 1, 2, or 3, the initial numbers of the long columns. (See fig. 22.) This would make it impossible for the plain-text positions of V and Y (i.e., the corresponding numbers in C_2) to differ by 4, as the number of C_1 under 1, 2, 3 of C_0 are x, $x + 8$, $x + 16$, . . . and differ by at least 8. At least one of the last three columns is a short one.

Suppose the last two columns to be long. Since a long column has 8 letters, the number of C_1 under 44 of C_0 is 1, 2, or 3, and the number of C_1 under 42 of C_0 must be the next-to-last one of a short column, i.e., either 44, 45, 46, 47, or 48. (See fig. 22.)

Suppose 1 of C_1 is under 44 of C_0. With this assumption we must test 44, 45, . . . 48 in C_1 under 42 of C_0 in turn. $\begin{Bmatrix} C_0\ 42 \\ C_1\ 44 \end{Bmatrix}$ and $\begin{Bmatrix} C_1\ 44 \\ C_2\ 01 \end{Bmatrix}$ make C the first letter of the plain text[1]. Since V would then have to be the third letter of the plan text, 3 of C_2 must go under 1 of C_1 or 44 of C_0. Since (C_1C_2) yields $1 \rightarrow 3$, 3 of C_1 must go under 1 of C_0. Inserted in figure 23, this would be as follows:

	S	A	U	T	L	A	N	I	F	N	L	A	N	H	T	R	A	E	U	V
C_0----	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
C_1----	03	11	19	27	35	43	51	59												
C_2----																				
	N	H	M	T	E	S	S	S	H	E	O	T	Y	A	R	Y	T	T	W	E
C_0----	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
C_1----																	04	12	20	28
C_2----																07				
	R	C	N	V	C	I	G	I	R	N	O	I	A	D	A	R	O	A	H	
C_0----	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	
C_1----	36	44	52	01	09	17	25	33	41	49	57									
C_2----		01		03																

FIGURE 24

[1] Because of the assumption that $44 \rightarrow 1$ in (C_0C_1).

The number of C_1 under 36 of C_0 is either 52, 53, 54, 55, 56, 57, 58, or 59 (the last number of a column). Since the corresponding Y has to be the seventh of the plain text (we saw that C is to be the first of the plain text) then 7 of C_1 would have to go under either 52, 53, 54, 55, 56, 57, 58, or 59 of C_0. This is impossible, as the last column has been assumed to be long and 7 is in a short column. Therefore $\begin{Bmatrix} C_0\ 42, C_0\ 44 \\ C_1\ 44, C_1\ 01 \end{Bmatrix}$ is impossible.

If 45 of C_1 were under 42 of C_0, 9 of C_2 would have to go under 45 of C_1 or 42 of C_0, because 42→45 and 45→9. This would make C of CAVALRY the ninth letter of the plain text and V the eleventh. This is impossible, since this would place 11 of C_2 under 1 of C_1 and therefore 11 of C_1 under 1 of C_0, whereas the number of C_1 under 1 of C_0 must be 01, 02, . . . 08. For similar reasons, we find that 46, 47, or 48 of C_1 cannot go under 42 of C_0. Therefore 1 of C_1 is not under 44 of C_0.[1]

Suppose 2 of C_1 is under 44 of C_0. If 44 of C_1 is under 42 of C_0, then 2 of C_2 is under 44 of C_1. This would make the Y of CAVALRY the thirty-sixth cipher letter, the eighth of the plain text. This is impossible, since as before the number of C_1 under 36 of C_0 is 51, 52, . . . 59, and these numbers of C_0 cannot be over 8 of C_1, as this would make the last column short.[1]

If 45 of C_1 is under 42 of C_0, then 10 of C_2 is under 45 of C_1, since 42→45 and 45→10. Since the C of CAVALRY must be the tenth plain-text letter, V must be the twelfth, so that 12 of C_2 must go under 2 of C_1 or 44 of C_0. This makes the Y of CAVALRY the sixteenth plain-text letter. This is impossible, since as before either 52, 53, . . . or 59 of C_1 would be over 16 of C_2, necessitating either 52, 53, . . . or 59 of C_0 to be over 16 of C_1; and 16 is in a short column.[1]

If 46 of C_1 were under 42 of C_0, then 18 of C_2 would have to go under 46 of C_1, since 42→46 and 46→18. This would make V of CAVALRY the twentieth plain-text letter, placing 2 of C_1 over 20 of C_2. This is impossible, since 2 of C_0 can be over only 9, 10, 11, . . . or 16 of C_1. (See fig. 22.) For similar reasons 47 and 48 of C_1 cannot be under 42 of C_0. Therefore 2 of C_1 is not under 44 of C_0.[1]

Suppose 3 of C_1 is under 44 of C_0. If 44 of C_1 is under 42 of C_0, then 3 of C_2 must be under 44 of C_1, since 42→44, 44→3. This will make V of CAVALRY the fifth letter of the plain text. This is impossible, since 3 of C_1 over 5 of C_2 implies 3 of C_0 over 5 of C_1, whereas 3 of C_0 must be over 17, 18, 19, . . . or 24 of C_1. (See fig. 22.) For a similar reason 45 of C_1 cannot be under 42 of C_0.[1]

If 46 of C_1 is under 42 of C_0, then 19 of C_2 is under 46 of C_1, since 42→46 and 46→19. This means that 21 of C_2 must be under 3 of C_1 and therefore 21 of C_1 under 3 of C_0, which is possible. The fact that Y will be the twenty-fifth plain-text letter, placing 25 of C_2 under 36 of C_0 and either 52, 53, . . . or 59 of C_1, involves no contradiction as yet, since 25 is in a long column and 52, 53, . . . 59 of C_0 must be over a number of C_1 coming from a long column.[1]

The number of C_1 which goes under 36 of C_0 must be 55 to enable 25 which is the fourth number of the first column to fit in properly in C_1. Inserting this information, we obtain—

[1] It is advisable that the reader himself carry out the steps outlined, writing the cipher message and C_0 in ink and C_1 and C_2 in pencil, to allow erasures.

REF ID:A57071

	S	A	U	T	L	A	N	I	F	N	L	A	N	H	T	R	A	E	U	V
C_0----	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
C_1----	05	13	21	29	37	45	53	08	16	24	32	40	48	56						
C_2----											23									

	N	H	M	T	E	S	S	S	H	E	O	T	Y	A	R	Y	T	T	W	E
C_0----	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
C_1----											07	15	23	31	39	47	55	06	14	22	30
C_2----															22		25			

	R	C	N	V	C	I	G	I	R	N	O	I	A	D	A	R	O	A	H
C_0----	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	
C_1----	38	46	54	03	11	19	27	35	43	51	59	01	09	17	25	33	41	49	57	
C_2----		19		21																

FIGURE 25

We find a further check. (C_0C_1) gives 39→22 and (C_1C_2) also gives 39→22. We canl ocate one more column, since (C_0C_1) gives 32→23, so that 32 of C_1 goes over 23 of C_2 or under 11 of C_0. The portion of C_1, now filled in, gives as part of the key, $\begin{Bmatrix} 8 & . & 7 & . & 1 & 6 & 5 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{Bmatrix}$. Let us now use the transposition rectangle to verify and complete the solution.

8 . 7 . 1 6 5 2	8 . 7 . 1 6 5 2
I . V . S T E I	. . . . I L E I
A . C . A T O F	N . A . . R Y A
D . I . U W T N	N . C . V A L .
A . G . T E Y L	Y . R . . A R C
R . I . L R A A	H . N . S O . .
O . R . A C R N	H . A . T . I A
A . N . N N Y H	. . . . E R . T
H . A	O . N

FIGURE 26

There is now no doubt that we are on the right track. To fit in INFANTRY as the second word, the complete key is 8–3–7–4–1–6–5–2.

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

FIGURE 27

SECTION VI

SOLUTION OF MESSAGES ENCIPHERED BY A DOUBLE TRANSPOSITION CIPHER SYSTEM

	Paragraph
The general problem	16
Summary	17

16. **The general problem.**—In the previous sections we have reconstructed the key to a double transposition cipher, starting with a great deal of information and progressively decreasing the amount of known information. Given a series of messages our problem is not any different. If one or more of the messages [1] contains a Q then we can definitely say that the Q must be followed by a U. By proceeding as in the previous sections, we can eliminate various lengths of keys and arrangements of columns and eventually read the message. If there is no Q, then the assumption of probable digraphs, trigraphs, or words will enable one to reach a solution. The actual manipulation is easier than it appears to be and provides a straightforward procedure which will *eventually* yield the solution.

17. **Summary.**—To summarize, the essential features of the method and its application are the following:

(1) The invariance of (C_0C_1), (C_1C_2) pairs.
(2) The assumption of probable widths.
(3) The assumption of plain-text position of certain cipher letters (if necessary).
(4) The elimination of incorrect widths by contradictions of—
    (*a*) Known cipher-text plain-text relationships (relative position of letters, final X's, etc.).
    (*b*) Improbable arrangement of plain text (unlikely digraphs, trigraphs, etc.).

It is interesting to note that the method was applied to read intercepted messages of a well-organized group of smugglers. It was discovered that these persons were using a single columnar transposition method with keys from 10 to 20 letters long. Soon a double transposition was introduced, but the messages were read.

A series of messages including some actual intercepts is appended hereto and will serve the reader as an interesting set of problems.

[1] More than one message can be employed, since an assumption as to position of numbers and length of columns in one message, imposes a definite position in the others.

REF ID:A57071

SECTION VII

DOUBLE TRANSPOSITION WITH DIFFERENT KEYS

	Paragraph
Analysis of the system	18
Example of procedure	19

18. **Analysis of the system.**—In the preceding sections we limited ourselves to a study of double transposition with the same key. It happens that a very similar procedure is applicable to the case in which a message undergoes columnar transposition twice, using different keys.

For the sake of convenience, suppose we consider a 19-letter message transposed with the key 5–4–2–1–3 and then 1–2–6–3–5–4.

```
5  4  2  1  3
-----------
01 02 03 04 05
06 07 08 09 10
11 12 13 14 15
16 17 18 19

C1: 04 09 14 19 03 08 13 18 05 10 15 02 07 12 17 01 06 11 16

1  2  6  3  5  4
-----------
04 09 14 19 03 08
13 18 05 10 15 02
07 12 17 01 06 11
16

C2: 04 13 07 16 09 18 12 19 10 01 08 02 11 03 15 06 14 05 17
```

FIGURE 28

In figure 28 C_1 is the text after the first transposition and C_2 the final text.

Let us analyze this case as we did the previous cases.

```
C0---- 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19
C1---- 04 09 14 19 03 08 13 18 05 10 15 02 07 12 17 01 06 11 16
```

FIGURE 29

Figure 29 represents the first transposition.

Let us use a similar representation for the operation of the second key on a 19-letter message.

```
C0---- 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19
C1---- 01 07 13 19 02 08 14 04 10 16 06 12 18 05 11 17 03 09 15
```

FIGURE 30

According to figure 30, the first plain-text letter is replaced by the first, the second plain-text letter by the seventh, etc.

If the second key were the only one applied to the message, then figure 30 would be sufficient. However, the correct plain text for the second key is C_1 of figure 29. If we combine figures 29 and 30 and apply the operations of the second key to C_1 of figure 29, we shall obtain the proper cipher message.

C_0---- 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19
C_1---- 04 09 14 19 03 08 13 18 05 10 15 02 07 12 17 01 06 11 16
C_1'---- 01 07 13 19 02 08 14 04 10 16 06 12 18 05 11 17 03 09 15
C_2---- 04 13 07 16 09 18 12 19 10 01 08 02 11 03 15 06 14 05 17

FIGURE 31

Let us study figure 31 with respect to the operations of figures 29 and 30. C_0 is the plain text and is also used to enumerate the positions. C_1 indicates the result of the first transposition. The pairs of C_0C_1' indicate the operations of the second transposition, the plain text for which is C_1. Thus, the second transposition replaces the first plain-text letter of C_1 (4 of C_0) by the first letter of C_1 (4 of C_0); therefore the first letter of C_2 is 4. The second transposition replaces the second letter of C_1 (9 of C_0) by the seventh letter of C_1 (13 of C_0); therefore the second letter of C_2 is 13, etc.

The invariance of pairs is maintained in this case also, but now the relationship is (C_0C_1), $(C_1'C_2)$. (In the previous case where the two keys were the same, C_1 and C_1' coincided.) Thus, notice the pairs 1→4; 7→13; 13→7; etc., in (C_0C_1) and $(C_1'C_2)$.

The method for recovery of the key or solution of a message is similar to the procedure already outlined. In this case, the assumption as to the length of key may be made for C_1 or C_1', the length of the other key will be determined therefrom.

19. **Example of procedure.**—A simple example will make this clear. Suppose that by anagramming, the following message has been determined:

23–16–07–37–30–20–15–29–22–13–06–36–26–21–17–10–01–31–24–14–09–
05–35–28–19–12–02–32–27–11–04–34–25–18–08–03–33

Let us write out C_0 and C_2, leaving room for C_1 and C_1'.

C_0---- 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20
C_1----
C_1'----
C_2---- 23 16 07 37 30 20 15 29 22 13 06 36 26 21 17 10 01 31 24 14
C_0---- 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37
C_1----
C_1'----
C_2---- 09 05 35 28 19 12 02 32 27 11 04 34 25 18 08 03 33

FIGURE 32

Suppose the second key were 5 wide. Then C_1' would begin with one of the sequences 1, 6, 11, . . .; 2, 7, 12 . . .; 3, 8, 13, . . .; 4, 9, 14, . . .; or 5, 10, 15, . . . Let us try each in turn. The first possibility

C_1'---- 01–06–11–16–21–26–31–36
C_2---- 23–16–07–37–30–20–15–29

involves the following set-up for C_0, C_1, C_1', and C_2:

REF ID:A57071

C_0----	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
C_1----	23					16					07					37				
C_1'----	01	06	11	16	21	26	31	36												
C_2----	23	16	07	37	30	20	15	29	22	13	06	36	26	21	17	10	01	31	24	14

C_0----	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37			
C_1----	30					20					15					29				
C_1'----																				
C_2----	09	05	35	28	19	12	02	32	27	11	04	34	25	18	08	03	33			

FIGURE 33

It is doubtful that C_1 begins with 23. Let us test the second possibility.

C_0----	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
C_1----		23					16					07					37			
C_1'----	02	07	12	17	22	27	32	37												
C_2----	23	16	07	37	30	20	15	29	22	13	06	36	26	21	17	10	01	31	24	14

C_0----	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37			
C_1----		30					20					15					29			
C_1'----																				
C_2----	09	05	35	28	19	12	02	32	27	11	04	34	25	18	08	03	33			

FIGURE 34

In order for 23 in C_1 to be the second of a column, the key for C_1 must be at least 12 letters wide. Let us draw up a table showing the number of long and short columns for different widths and immediately eliminate those which do not fit in properly with 7 of C_1 under 12 of C_0.

Width of key	Long and short columns
12	1–4, 11–3
13	11–3, 2–2
14	9–3, 5–2
15	7–3, 8–2
16	5–3, 11–2
17	3–3, 14–2
18	1–3, 17–2

We stop with 18 because it is doubtful that the key for C_1 is much longer.

Width 12 is immediately impossible since $4+n\times3\neq11$. Widths 13–18 are apparently possible since $3\times3+2=11$ or $3+4\times2=11$. For width 13, the 7 of C_1 is to be followed by 20. But $13\rightarrow20$ in (C_0C_1) and $27\rightarrow20$ in $(C_1'C_2)$ contradict so that width 13 is impossible. For width 14 the 7 of C_1 is to be followed by 21. The pair $13\rightarrow21$ in (C_0C_1) implies $13\rightarrow21$ in $(C_1'C_2)$. This is impossible since 13 in C_1' cannot be placed over 21 of C_2 or under 14 of C_0 and still allow for a proper arrangement of C_1'; therefore width 14 is impossible. Similar results will be found for the remaining widths.[1]

The third possibility for C_1' yields the following set-up:

[1] It is suggested that the reader carry out the details omitted.

C_0-----	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
C_1-----			23					16					07					37		
C_1'----	03	08	13	18	23	28	33													
C_2-----	23	16	07	37	30	20	15	29	22	13	06	36	26	21	17	10	01	31	24	14
C_0-----	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37			
C_1-----			30					20					15							
C_1'----																				
C_2-----	09	05	35	28	19	12	02	32	27	11	04	34	25	18	08	03	33			

FIGURE 35

In order for 23 in C_1 to be under 3 of C_0, the key for C_1 must be at least 8 letters wide. Let us again indicate the number of long and short columns pertaining to each possible width.

Width of key	Long and short columns
8	5–5, 3–4
9	1–5, 8–4
10	7–4, 3–3
11	4–4, 7–3
12	1–4, 11–3
13	11–3, 2–2
14	9–3, 5–2
15	7–3, 8–2
16	5–3, 11–2
17	3–3, 14–2
18	1–3, 17–2

Widths 8 and 9 are impossible since 16 of C_1 cannot be fitted in any arrangement of columns of length 5 and 4. Width 10 is impossible since for 7 of C_1 to be under 13 of C_0 the first four columns of C_1 must be long and 16 of C_1 cannot be the last of a column (under 8 of C_0). Similar contradictions will be found for the other possibilities.[3]

The fourth possibility for C_1' yields the following set-up:

C_0-----	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
C_1-----			23						16				07					37		
C_1'----	04	09	14	19	24	29	34													
C_2-----	23	16	07	37	30	20	15	29	22	13	06	36	26	21	17	10	01	31	24	14
C_0-----	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37			
C_1-----			30						20					15						
C_1'----																				
C_2-----	09	05	35	28	19	12	02	32	27	11	04	34	25	18	08	03	33			

FIGURE 36

[3] See note, p. 21.

REF ID:A57071

For 23 of C_1 to be under 4 of C_0, the key for C_1 must be at least 6 letters long. For a width 6 there are 5 columns of 6 letters and 1 column of 7 letters. It is possible to fit 7 of C_1 under 14 of C_0 since $2 \times 6 = 12$ (7 is the second of a column). If the key for C_1 is 6 letters long, then C_1 must begin with 5–11–17–23–29–35. This means that 29 of C_1 is under 05 of C_0 and therefore 05 of C_1' over 29 of C_2. For a key of width 6 for C_1, having the positions in C_1 of one of the numbers of each column, we can fit in all of C_1. If this is done we get the following:

C_0	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
C_1	05	11	17	23	29	35	04	10	16	22	28	34	01	07	13	19	25	31	37	06
C_1'	04	09	14	19	24	29	34	05	10	15	20	25	30	35						
C_2	23	16	07	37	30	20	15	29	22	13	06	36	26	21	17	10	01	31	24	14

C_0	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
C_1	12	18	24	30	36	02	08	14	20	26	32	03	09	15	21	27	33
C_1'																	
C_2	09	05	35	28	19	12	02	32	27	11	04	34	25	18	08	03	33

FIGURE 37

We find a check in that (C_0C_1) and ($C_1'C_2$) both show 10–22. Apparently, we are on the right track. The rest is, of course, simple, just a question of combining the proper pairs in $C_1'C_2$ according to those of C_0C_1.

The final result is as follows:

C_0	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
C_1	05	11	17	23	29	35	04	10	16	22	28	34	01	07	13	19	25	31	37	06
C_1'	04	09	14	19	24	29	34	05	10	15	20	25	30	35	03	08	13	18	23	28
C_2	23	16	07	37	30	20	15	29	22	13	06	36	26	21	17	10	01	31	24	14

C_0	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
C_1	12	18	24	30	36	02	08	14	20	26	32	03	09	15	21	27	33
C_1'	33	01	06	11	16	21	26	31	36	02	07	12	17	22	27	32	37
C_2	09	05	35	28	19	12	02	32	27	11	04	34	25	18	08	03	33

FIGURE 38

From C_1 we find the first key to be $\begin{Bmatrix} 3–5–6–2–1–4 \\ 1–2–3–4–5–6 \end{Bmatrix}$ and from C_1' the second key to be $\begin{Bmatrix} 4–5–3–1–2 \\ 1–2–3–4–5 \end{Bmatrix}$.

It is thus seen that there exists no radical difference in the procedure when the keys are different from that when the keys are the same.

No further illustrative examples will be given.

REF ID:A57071

APPENDIX

1. Given that the width of the transposition rectangle is 8 columns and that the phrase JAPANESE NEGOTIATIONS is in the cryptogram, solve the following and reconstruct the key:

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

2. Solve and reconstruct the key for the following cryptogram which is enciphered by a completely filled rectangle and contains the phrase NO DIVISIONS ARE:

N O I A N S B E K R O E I O D E I O E H T R R V T
N O I N N T I N A T R O S N W S N K N N N V O I E
I S R I O E A D S O S H L E R P O E A R W E

3. Solve and reconstruct the key for the following, enciphered with a rectangle of 9 columns:

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

4. Both the following messages were enciphered by completely filled rectangles and both are in the same key. Solve them and reconstruct the key:

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

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

5. The following rum-runner messages have been partly reconstructed by anagramming. The enciphering rectangle is incompletely filled. Complete the solution and reconstruct the key:

(1)

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

(2)

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

(1) W I L L B E O N P O S I T I O N W E D N E S D A Y A T F O U R P M
(2) C H A S E D O F F B Y C U T T E R I M P O S S I B L E R E T U R N

6. Given the width of rectangle as 7 columns, and the known text TOMORROW, solve the following:

T T O I R O T T E O A F N H P E O R L T G O J P R
E Y I E W I O E T N M C T T T M N R P C L E W O M
L H B E T R E I R E O S S N

7. Given the width of rectangle as 7 columns, solve the following:

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

8. The following three messages with different keys are intercepts of rum-runner traffic. Solve the messages and reconstruct the numerical and the literal keys. X's were used as nulls to make the total number of letters a multiple of four.

(1)

DEC 26, 1932 CHAS EDWARDS FROM BELIZE CK 10

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

(2)

MAR 20, 1933 BELIZE FROM NEW ORLEANS CK 28

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

(3)

APR 8, 1933 BELIZE AND NEW ORLEANS FROM CORAZEL CK 22

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

○