Register No. 135

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON

FURTHER APPLICATIONS OF THE PRINCIPLES OF INDIRECT SYMMETRY OF POSITION IN SECONDARY ALPHABETS

30 April 1959

This document is declassified by authority of the Director, National Security Agency.

Paul S. Willard
Colonel, AGC
Adjutant General

Classification changed to RESTRICTED
By Authority of
HAROLD G. HAYES, Col., Signal Corps
Acting Chief, Army Security Agency

by MASON G. CAMPBELL, 1st Lt. SigC
1 April 1946

NO ACCOUNTING NECESSARY

REGISTRATION CANCELED
by
Authority Hqs. ASA ltr dated 27 Feb 46
2d Ind 11 Mar 46, signed:
HAROLD G. HAYES, Col., Signal Corps
Acting Chief, Army Security Agency

~~Confidential~~

Register No. 135

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

FURTHER APPLICATIONS OF THE PRINCIPLES OF INDIRECT SYMMETRY OF POSITION IN SECONDARY ALPHABETS

TECHNICAL PAPER

By

FRANK B. ROWLETT
Junior Cryptanalyst

SIGNAL INTELLIGENCE SECTION
WAR PLANS AND TRAINING DIVISION

UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON: 1935

CONTENTS

FURTHER APPLICATIONS OF THE PRINCIPLES OF INDIRECT SYMMETRY OF POSITION IN SECONDARY ALPHABETS

SECTION I

INTRODUCTORY REMARKS

1. **Purpose.**—This paper is intended as a supplement to the technical paper, *The Principles of Indirect Symmetry of Position in Secondary Alphabets and Their Application in the Solution of Polyalphabetic Substitution Ciphers*,[1] in which only one of the many applications of the principles of indirect symmetry is treated. In this paper other applications of this valuable tool will be presented, and the steps to be followed in the analysis of three types of cipher systems will be shown in detail.[2]

2. **General remarks.**—As a general rule, the principles of indirect symmetry can be applied in the solution of any cipher system based upon two sequences which are slid against each other. This includes polyalphabetic ciphers based upon a square table or cipher disk, the Wheatstone Cipher, autokey ciphers, and some others which are not so frequently met by the cryptanalyst.

[1] By William F. Friedman, Cryptanalyst, Chief of Signal Intelligence Section, Office of the Chief Signal Officer, 1935.

[2] The methods and principles described herein were developed in collaboration with other members of the staff of the Signal Intelligence Section and I desire to acknowledge my indebtedness for the important contributions made by them, especially by Drs. S. Kullback and A. Sinkov. In particular, it is necessary to indicate that credit for the original discovery of the principle of "conversion to monoalphabetic terms", described in par. 22, belongs to Mr. William F. Friedman, Chief of the Section, who first applied it in 1923 in the solution of a polyalphabetic cipher involving two sliding, mixed, primary components.

SECTION II

SOLUTION OF A PROGRESSIVE ALPHABET SYSTEM IN WHICH THE ALPHABETS ARE CHANGED AT THE END OF EACH WORD

3. **An actual example.**—A very frequently encountered type of cipher is one in which a key letter designates the alphabet to be used for enciphering a complete word. A great many users of this type of system commonly encipher an infrequently used letter, such as Q, J, or Z, at the end of each word to indicate to the decipherer that he is to proceed to the next alphabet in order to decipher the following letters. This practice usually facilitates the solution of such systems, and in order to bring out other ideas of cryptanalysis, as well as to present an application of the principles of indirect symmetry, the example herein treated will be of this nature. The cryptogram of figure 1 is known to have been enciphered by means of such a system, using two different keyword-mixed alphabets and the letter Q to indicate the end of a word:

CRYPTOGRAM

```
                5                  10                  15                  20                  25                  30
Q X R U B  Y A Y K F  D J V K K  C D R B Y  W D B Q Z  M Z K G I

               35                  40                  45                  50                  55                  60
N E T I S  X E J I R  D U Y D W  A D V X P  J B R X V  B G Z Y H

               65                  70                  75                  80                  85                  90
B Z R E K  G J U Z G  X F I Y S  U H C J G  M F G Y B  W I V B E

               95                 100                 105                 110                 115                 120
Z M Z P O  V G B T J  D T I G S  X M I P S  U K V X A  Y E R V T

              125                 130                 135                 140                 145                 150
D T S J V  A G Y C I  A I C S I  Z U T M M  T S P R E  G T U N X

              155                 160                 165                 170                 175                 180
Q P U X Y  E R V J K  Q F U P Y  H B Z K P  Y Z M G I  L G E E X

              185                 190                 195                 200                 205                 210
E Z Q U H  F Y D V J  G M B R R  Y K H A O  Z X R C O  G E B K L

              215                 220                 225
I X V S Y  S P U H F  Y D V J K  V A B
```

FIGURE 1

4. **Determination of word lengths.**—Only one repetition of more than four letters in length occurs in the foregoing message. Its first occurrence begins with the 184th letter of the message and ends with the 190th letter, while the second occurrence begins with the 218th letter and ends with the 224th letter. Since each word of the message is followed by Q, this repetition must represent a five-letter word with the Q's preceding and following it. Therefore, $U_c = Q_p$ in one and $J_c = Q_p$ in the other of the alphabets used in the encipherment of the plain text which causes this repetition. Wherever in the cipher text a sequence of letters occurs, produced by the alphabet which gives $Q_p = J_c$, this sequence will be preceded and followed in every case by the letters U and J respectively. Let us now search through the cipher text of the message for a U

followed by a J at a distance approximating the length of one word (not more than 15 letters), and tabulate the sequences thus found, for study.

```
4                  12
U B Y A Y K F D J

42                       51
U Y D W A D V X P J

76    79
U H C J

111                          124
U K V X A Y E R V T D T S J

153          159
U X Y E R V J

184          190
U H F Y D V J

218          224
U H F Y D V J
```

FIGURE 2

The letters falling between each U and J above are in the same monoalphabet, and if this monoalphabet can be solved, a great deal will have been accomplished toward complete solution of this message. With such a small amount of data, however, it will be a very difficult matter to make correct assumptions as to the plain text represented by the foregoing cipher text. However, if we can determine the cipher letters which represent Q in each alphabet as we have those above, solution of the message will be facilitated. Let the foregoing portions, with the cipher text following them, be superimposed as shown in figure 8, and let us search for cipher letters which may represent Q_p in each alphabet used in this message.

```
4                                                                   41
U B Y A Y K F D J V K K C D R B Y W D B O Z M Z K G I N E T I S X E J I R D
Q               Q

42                                59  62                          75
U Y D W A D V X P J B R X V B G Z Y H B Z R E K G J U Z G X F I Y S
Q                 Q

76                                                            110
U H C J G M F G Y B W I V B E Z M Z P O V G B T J D T I G S X M I P S
Q    Q

111                                                                 152
U K V X A Y E R V T D T S J V A G Y C I A I C S I Z U T M M T S P R E G T U N X Q P
Q                       Q

153                   165  168                          183
U X Y E R V J K Q F U P Y H B Z K P Y Z M G I L G E E X E Z Q
Q           Q

184                                                         217
U H F Y D V J G M B R R Y K H A O Z X R C O G E B K L I X V S Y S P
Q           Q

218                  228
U H F Y D V J K V A B
Q           Q
```

FIGURE 3

Note the repetition of Y H B Z of 59–62 and 165–168. This is probably a two-letter word with its associated word stops, and we should find a Y and Z in each of the first six sections of superimposed text separated by intervals which correspond to reasonable word lengths. This condition is met with in all the first six sections; and, in the fourth section of the foregoing, Y is separated from J by only three cipher letters. This, when coupled with the fact that the first word stop, $Q_p=U_c$, occurs as the fourth letter of the message, leads to the conclusion that the cipher equivalents for Q_p in the first four alphabets have been determined.

An examination of the remaining cipher text discloses that only two letters, G and X, occur in each of the first six sections of cipher text, and we can assume first, that only six cipher alphabets are involved, and second, that these two letters (G and X) represent Q_p in the fifth and sixth alphabets, respectively. The following six values have now been obtained:

Alphabet 1_____ $Q_p=U_c$
Alphabet 2_____ $Q_p=J_c$
Alphabet 3_____ $Q_p=Y_c$
Alphabet 4_____ $Q_p=Z_c$
Alphabet 5_____ $Q_p=G_c$
Alphabet 6_____ $Q_p=X_c$

FIGURE 4

Since the equivalents for Q_p in six alphabets are known, the message can be broken into word lengths as shown in figure 5.

```
  1           2           3           4           5
Q X R U  B Y A Y K F D J  V K K C D R B Y  W D B O Z  M Z K G
      Q           Q           Q           Q           Q

  6           1           2           3           4
I N E T I S X  E J I R D U  Y D W A D V X P J  B R X V B G Z Y  H B Z
          Q           Q           Q           Q           Q  Q

  5           6           1           2           3           4
R E K G  J U Z G X  F I Y S U  H C J  G M F G Y  B W I V B E Z
      Q           Q           Q     Q           Q           Q

  5           6           1           2
M Z P O V G  B T J D T I G S X  M I P S U  K V X A Y E R V T D T S J
        Q           Q           Q                       Q

  3           4           5           6           1
V A G Y  C I A I C S I Z  U T M M T S P R E G  T U N X  Q P U
      Q           Q           Q     Q     Q

  2           3           4           5           6           1
X Y E R V J  K Q F U P Y  H B Z  K P Y Z M G  I L G E E X  E Z Q U
          Q           Q     Q           Q           Q     Q

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

  2           3
H F Y D V J  K V A B
          Q
```

FIGURE 5

5. **Solution of two alphabets.**—Note the sequence U T M M T S P R E in alphabet 5. The T M M T suggests the A T T A of the word B A T T A L I O N, and when the equivalents obtained from assuming this to be the correct decipherment are substituted in the other portions enciphered by this alphabet, the following solution for alphabet 5 is obtained without difficulty.

```
  1           2           3           4           5
Q X R U  B Y A Y K F D J  V K K C D R B Y  W D B O Z  M Z K G
    Q           Q           Q           Q  T H E Q

  6           1           2           3           4
I N E T I S X  E J I R D U  Y D W A D V X P J  B R X V B G Z Y  H B Z
      Q           Q           Q           Q           Q

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

    5           6           1           2
M Z P O V G  B T J D T I G S X  M I P S U  K V X A Y E R V T D T S J
T H I R D Q              Q           Q                       Q

  3           4           5           6           1
V A G Y  C I A I C S I Z  U T M M T S P R E G  T U N X  Q P U
    Q           Q  B A T T A L I O N Q        Q     Q

  2           3           4           5           6           1
X Y E R V J  K Q F U P Y  H B Z  K P Y Z M G  I L G E E X  E Z Q U
      Q           Q     Q  E I G H T Q              Q        Q

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

  2           3
H F Y D V J  K V A B
      Q
```

FIGURE 6

An enciphering table is now drawn up in which all the equivalents obtained are tabulated. This table is shown in figure 7.

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Plain		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	1																	U									
	2																	J									
	3																	Y									
	4																	Z									
	5	T	U		V	K	X	Y	Z	P			S		E	R		G	O		M	C					
	6																	X									

FIGURE 7

If the same sequence served as both the plain and cipher components, the principles of indirect symmetry of position could be applied in the foregoing diagram between the plain and cipher alphabets to obtain new values in other alphabets. However, since the plain and cipher

components of this example are known to be different, equivalents in some other alphabet must be determined before the principles of indirect symmetry of position can be applied. This can best be done by solving another portion of the cipher text.

Solution of alphabet 6 is obtained by assuming a plain-text word. The cipher text following the plain-text word E I G H T of alphabet 5 suggests the word T H R E E. Insertion of the values obtained from this assumption throughout alphabet 6 yields the following:

```
 1           2           3           4        5
Q X R U  B Y A Y K F D J  V K K C D R B Y  W D B O Z  M Z K G
   Q           Q           Q           Q  T H E Q

 6        1        2           3           4
I N E T I S X  E J I R D U  Y D W A D V X P J  B R X V B G Z Y  H B Z
T W E N T Y Q     Q           Q           Q     Q

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

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

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

    2           3           4           5           6        1
X Y E R V J  K Q F U P Y  H B Z  K P Y Z M G  I L G E E X  E Z Q U
      Q           Q     Q  E I G H T Q  T H R E E Q        Q

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

 2        3
H F Y D V J  K V A B
      Q
```

FIGURE 8

The equivalents which have been obtained in alphabet 6 when inserted in figure 7 give figure 9.

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

FIGURE 9

6. **Application of principles of indirect symmetry.**—By applying the principles of indirect symmetry between alphabets 5 and 6 of figure 9, the following pairs of letters separated by the same interval in the original primary component are obtained.[1]

T(5—1)	D(6—1)	E(5—14)	T(6—14)
K(5—5)	E(6—5)	R(5—15)	U(6—15)
X(5—6)	J(6—6)	G(5—17)	X(6—17)
Y(5—7)	K(6—7)	O(5—18)	G(6—18)
Z(5—8)	L(6—8)	M(5—20)	I(6—20)
P(5—9)	B(6—9)	C(5—21)	Z(6—21)

FIGURE 10

The letters X and J both occur in column 17, giving the pair

X(6—17) J(2—17)

From alphabets 5 and 6 we have

X(5—6) J(6—6)

This means that the equivalent primary component formed from alphabets 5 and 6 is the same as that which can be obtained from alphabets 6 and 2, and that wherever in figure 9 a first letter of one of the pairs obtained from alphabets 5 and 6 occurs in alphabet 6, its associated letter can be written in the corresponding column in alphabet 2. For instance, from T(5—1) D(6—1), we can write T(6—14) D(2—14), which means that the letter D must occupy the cell in figure 9 designated by the coordinates (2—14).

All the values which can be entered are given in figure 11.

X(5— 6)	J(6— 6)	X(6—17)	J(2—17)
T(5— 1)	D(6— 1)	T(6—14)	D(2—14)
K(5— 5)	E(6— 5)	K(6— 7)	E(2— 7)
Z(5— 8)	L(6— 8)	Z(6—21)	L(2—21)
E(5—14)	T(6—14)	E(6— 5)	T(2— 5)
G(5—17)	X(6—17)	G(6—18)	X(2—18)

FIGURE 11

These equivalents are now inserted in figure 9 to give figure 12.

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

FIGURE 12

[1] The system of notation used here is the same as in Friedman, W. F., loc. cit. For instance, T(5—1) refers to the letter T in line 5 and column 1.

Five values have been obtained in alphabet 2 without making any assumptions as to a plain-text word enciphered by this alphabet. These values can be tested by inserting them in the cipher text of alphabet 2 as shown in figure 13.

```
B Y A Y K F D J
          N Q

Y D W A D V X P J
  N     N   R   Q

H C J
    Q

K V X A Y E R V T D T S J
    R     G     E N E   Q

X Y E R V J
R   G     Q

H F Y D V J
      N   Q

H F Y D V J
      N   Q
```

FIGURE 13

Solution of this monoalphabet checks the values obtained by application of the principles of indirect symmetry of position and gives the partial solution of the message shown in figure 14.

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

    6           1                   2                 3           4
I N E T I S X  E J I R D U  Y D W A D V X P J  B R X V B G Z Y  H B Z
T W E N T Y Q        Q  I N F A N T R Y Q              Q     Q

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

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

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

    2           3           4           5           6       1
X Y E R V J  K Q F U P Y  H B Z  K P Y Z M G  I L G E E X  E Z Q U
R I G H T Q        Q     Q  E I G H T Q  T H R E E Q       Q

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

    2         3
H F Y D V J  K V A B
P O I N T Q
```

FIGURE 14

The new equivalents obtained in alphabet 2 are inserted in figure 12 to give figure 15.

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

FIGURE 15

7. **Reconstruction of the cipher component.**—From the three partially recovered secondary sequences of figure 15, portions of three equivalent primary sequences can be reconstructed by the application of the principles of indirect symmetry of position between the three pairs of alphabets which can be formed from alphabets 2, 5, and 6. The tabulation of the pairs obtained from alphabets 5 and 6, 6 and 2, and 5 and 2 is given in figure 16.[1]

5—6	6—2	5—2
T D	D A	T A
K E	E T	V S
X J	J W	K T
Y K	K E	X W
Z L	L R	Y E
P B	B Y	Z R
E T	T D	P Y
R U	U F	S B
G X	X J	E D
O G	G X	R F
M I	I V	G J
C Z	Z L	O X
	S P	M V
		C L

FIGURE 16

Since some of the pairs from 5—6 and from 6—2 are the same, these two sets can be combined, and all pairs of both 5—6 and 6—2 having common letters can be united to give the following sequences:

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

[1] Hereafter, when reference is made to two alphabets, the numbers corresponding to them will be used. For instance, alphabets 5 and 6 will be replaced by 5—6.

The pairs of 5—2 can also be united in a similar manner.

K T A
M V S B
O X W
P Y E D
Z R F
C L

If the letters of the sequence K T A of 5—2 are separated by one space, the interval between them will be the same as in S P B Y K E T D A. All the sequences of 5—2 can be so treated to give:

K . T . A
M . V . S . B
O . X . W
P . Y . E . D
Z . R . F
C . L

Unfortunately, only one of the foregoing sequences can be used to combine any of the sequences of 5—6, viz, the sequence M . V . S . B which permits the union of M I V and S P B Y K E T D A to give M I V . S P B Y K E T D A. All the pairs formed from the three pairs of alphabets have now been combined to give the following sequences based on the interval of 5—6:

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

At this point it is impossible to insert other letters in this equivalent primary component unless some other equivalent primary component is made available. Now it usually happens in a keyword-mixed sequence that the low-frequency letters J K, X Y Z, P Q, and B C D retain their original alphabetical order. If this is true of the original primary component with which we are working, we can assume that X Y Z are sequent letters in it and bring the sequences of 5—6 in juxtaposition as shown below:

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

The sequence X Y Z appears in the foregoing superimposition in a column, and since the assumption has been made that these three letters are a part of the original primary component, the other columns of this arrangement must also be portions of the original primary component. This assumption is corroborated by the fact that O P, B C, J K L, T U, and D F fall in their proper alphabetical order. Since B C and D F are sequent letters in the columns of the foregoing arrangement, it is reasonable to assume that they can be united to form B C D F. If this is true, the B of M I V . S P B Y K E T D A and the C of C Z L R U F may be placed over the D of M I V . S P B Y K E T D A to give the following arrangement:

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

This arrangement permits the combination of O G X J W and C Z L R U F, and also gives the following columnar sequences:

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

From a consideration of their alphabetical order, the sequences J K L and M O P . T U can be combined to give J K L M O P . T U. This arrangement, however, gives two appearances of the letter M in the sequence M I V . S P B Y K E T D A M, separated by an interval of 13. This means that the equivalent primary component thus recovered for 5—6 consists of two sets of 13 letters each. We can now revise the arrangement which we have been using to give the one shown herewith.

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

The fact that A follows Z in the columnar sequence of the foregoing diagram leads to the conclusion that it is the first letter of the keyword upon which the sequence is based. All the columnar sequences can now be united to give:

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

Only three letters, H, N, and Q, are missing from this sequence. The H and Q can be inserted in their proper alphabetical positions leaving N to follow A, which gives the sequence

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

8. **Reconstruction of the plain component.**—The plain component can now be obtained by using the three secondary sequences of figure 15 to prepare the deciphering table shown in figure 17 in which the principles of *direct symmetry* of position may be used.

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

FIGURE 17

The sequence obtained by application of the principles of *direct symmetry* of position from figure 17 is

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

The missing letters, C, J, K, V, X, and Z, can be easily inserted to give

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

9. **Solution completed.**—Now that both plain and cipher components have been recovered, it is possible to prepare sliding strips to complete the decipherment of the message. The correct relative positions of these two strips for alphabets 1, 3, and 4 are determined by the values of Q_p in these alphabets. The complete decipherment of the cryptogram is given in figure 18.

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

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

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

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

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

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

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

H F Y D V J  K V A B
P O I N T Q  F O U R
```

FIGURE 18

10. **Concluding remarks.**—In the solution of the foregoing example, the principles of *indirect symmetry* of position were applied to an *enciphering table* (figure 15) to recover the cipher component, while the plain component was obtained by applying the principles of *direct symmetry* of position to a *deciphering table* (figure 17) based upon the recovered cipher component. However, the same result could have been obtained by first recovering the plain component by the application of the principles of indirect symmetry of position to the *deciphering table* based on the normal alphabet, resulting from figure 15. In this case the cipher component could have been recovered from an *enciphering table* based on the recovered plain component, by the use of the principles of *direct symmetry* of position.

SECTION III

SOLUTION OF A PROGRESSIVE ALPHABET SYSTEM IN WHICH THE ALPHABETS ARE CHANGED FOR EACH LETTER

11. **Nature of the system.**—A very important application of the principles of indirect symmetry of position in the analysis of a cipher system based upon a square table will be brought out in the solution of another type of progressive-alphabet cipher system. The method of encipherment is such that the first letter of the plain text is enciphered by a prearranged alphabet of a square table, the second letter by the alphabet immediately following that used for the first letter, and so on until 26 letters have been enciphered, after which the cycle of alphabets is repeated for each set of 26 letters until the entire message is enciphered. The same effect can be obtained with a cipher disk such as the obsolete United States Army Cipher Disk, by moving the inner disk one space clockwise after the encipherment of each letter of the plain text.

12. **Preliminary analysis.**—In order to develop the fundamental idea upon which solution of the following example is based, the beginnings of two messages enciphered by means of the square table shown in figure 19 will be examined. The sequence upon which the table is based is keyword-mixed, derived from the word QUESTIONABLY.

71833—35——3

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

FIGURE 19

1ST MESSAGE

Plain_____ F I R S T B A T T A L I O N W I L L S U P P O R T
Cipher____ F O W O A F F Y C J P H K P Y P Q U R P F G E K E

Plain_____ S E C O N D . . .
Cipher____ E E D A L J

2D MESSAGE

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

Plain_____ T H I R D . . .
Cipher____ O M B Q M

FIGURE 20

The cipher text produced by the two encipherments of the words FIRST BATTALION WILL SUPPORT is different in each case, but when the two encipherments for these words are superimposed, as shown in figure 21, certain phenomena are exhibited by the cipher text.

Plain text	F I R S T B A T T A L I O N W I L L S U P P O R T
1st encipherment	F O W O A F F Y C J P H K P Y P Q U R P F G E K E
2d encipherment	J B Q B Y J J F G P W M R W F W S T X W J K I R I

FIGURE 21

These phenomena deal with characteristics here designated by the term *isomorphism*. If two sequences occur in a cryptogram, one of which can be obtained by applying a monoalphabetic substitution upon the other, the two sequences are said to be *isomorphic*. For instance, the sequences L R S R U L M V L R M and Q S F S B Q N J Q S N are isomorphic because the second can be derived by applying a monoalphabetic substitution to the first using the following substitution:

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

Note that the two encipherments of figure 21 are isomorphic, and that if the interval in the original primary component between corresponding cipher letters of this superimposition is determined, it will be seen that in each case the letter of the second encipherment is three letters removed from the corresponding letter of the first encipherment in the sequence

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

If the letters of the first encipherment are paired off with the letters of the second encipherment, so that they are separated by the proper interval, portions of the original primary component will result. The pairs which can be formed from these two encipherments are tabulated in figure 22.

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

FIGURE 22

By uniting the pairs which have common letters, the following sequences are formed:

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

FIGURE 23

A comparison of these sequences with the original primary component shows that both are identical in interval. This can be seen from the following superimposition.

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

FIGURE 24

13. **An actual example.**—It is obvious from the foregoing discussion that if at least two differently enciphered versions of a plain-text repetition of fifteen or more letters should occur in a cryptogram enciphered by this system, and if the isomorphisms resulting from this repetition could be detected by the cryptanalyst, partial or complete reconstruction of the original or an equivalent primary component could be effected. These isomorphisms can best be detected by superimposing and comparing all portions of cipher text containing like letters which are adjacent or separated by one, two, three, or four letters. An illustration of this method of finding isomorphisms in the cipher text is given in the solution of the following example which is enciphered by means of the system referred to above.

CRYPTOGRAM

```
                5                  10                  15                  20                  25
A R N U X  X V M P Y  O P M F Y  K Z T I W  E H C D M
               30                  35                  40                  45                  50
H D S M M  D W N G J  Z O K U V  B R Q D X  T F T C I
               55                  60                  65                  70                  75
R B T I B  R U Y Y A  U P P K O  H H E O F  S N F O A
               80                  85                  90                  94
S Z G D L  T B J R X  O J X K O  O X T P
```

FIGURE 25

The first step in the solution of this cipher is to rewrite it in superimposed cycles of 26 letters, so that letters enciphered by the same alphabet occur in the same column.

```
 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
A  R  N  U  X  X  V  M  P  Y  O  P  M  F  Y  K  Z  T  I  W  E  H  C  D  M  H
          30                   35                   40                   45                   50
D  S  M  M  D  W  N  G  J  Z  O  K  U  V  B  R  Q  D  X  T  F  T  C  I  R  B
       55                   60                   65                   70                   75
T  I  B  R  U  Y  Y  A  U  P  P  K  O  H  H  E  O  F  S  N  F  O  A  S  Z  G
    80                   85                   90                   94
D  L  T  B  J  R  X  O  J  X  K  O  O  X  T  P
```

FIGURE 26

14. **Detection of isomorphisms.**—The next step is to search through the cipher text of the message for isomorphisms. This is done by first superimposing portions of the cipher text with like letters occupying adjacent positions. Only six such pairs of letters occur in the message and they are given in figure 27 with the 8 letters preceding and following them.

```
                1         5        10        15
(1)   - - - - A R N U X X V M P Y O P M F Y
                   25        30        35
(2)   E H C D M H D S M M D W N G J Z O K U
          50        55        60        65
(3)   C R B T I B R U Y Y A U P P K O H H E
             55        60        65        70
(4)   I B R U Y Y A U P P K O H H E O F S N
                60        65        70        75
(5)   Y Y A U P P K O H H E O F S N F O A S
                   85        90        94
(6)   B J R X O J X K O O X T P - - - - - -
```

FIGURE 27

Note that in lines (1) and (5) of figure 27 an isomorphism occurs which begins with the doubled letter and extends throughout the remainder of these two lines.

```
 5  66   6  67    8  69   13  74    9  70   12  73   10  71   15  76
(X→H; X→H) (M→O; M→O) (P→F; P→F) (Y→S; Y→S)
```

However, the isomorphism does not extend to the left any further than $\overset{5}{X}\overset{66}{\rightarrow}H$, because $\overset{4}{U}\overset{65}{\rightarrow}O$ conflicts with $\overset{8}{M}\overset{69}{\rightarrow}O$ and $\overset{13}{M}\overset{74}{\rightarrow}O$. Let us now superimpose all the cipher text between $\overset{66}{H}$ and the end of the message, with the corresponding portion following $\overset{5}{X}$.

```
 5        10        15        20        25        30
X X V M P Y O P M F Y K Z T I W E H C D M H D S M M D W N
66        70        75        80        85        90        94
H H E O F S N F O A S Z G D L T B J R X O J X K O O X T P
```

FIGURE 28

$\overset{20}{W}\overset{81}{\rightarrow}T$ and $\overset{32}{W}\overset{93}{\rightarrow}T$, and $\overset{8}{M}\overset{69}{\rightarrow}O$, $\overset{13}{M}\overset{74}{\rightarrow}O$, $\overset{25}{M}\overset{86}{\rightarrow}O$, $\overset{29}{M}\overset{90}{\rightarrow}O$ and $\overset{30}{M}\overset{91}{\rightarrow}O$ indicate that the above two portions of cipher text represent the same plain text and that this repetition begins in one case with the 5th letter of the message and in the other with the 66th letter. Since the isomorphism extends through the next to last letter of the message, it is safe to include the 33d and 94th letters in the repetition.

15. **Reconstruction of the cipher component.**—Reference to figure 28 above shows that the first letter of the first occurrence of the repetition is represented by X_5 in alphabet 5 and the first letter of its second occurrence is represented by H_{14} in alphabet 14 (66−52=14). Now since X_5 in alphabet 5 and H_{14} in alphabet 14 represent the same plain-text letter, these two letters must

be separated by an interval of 14 minus 5, or 9, in the original primary component. This is also true for all the other pairs of the above superimposition, and they can be written as shown in figure 29.

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

FIGURE 29

By uniting pairs having common letters the following sequences can be formed:

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

These sequences are portions of the original primary component with which the square table was formed and if this component is keyword mixed, V W X Y Z, B C D, and J K are very likely sequent letters. Let us make the assumption that V W X Y Z are sequent letters and combine sequences (1), (2), and (4) on this basis:

(7) X Y Z . . . . E T H S G . . . . B D J K . . . . V W

The sequence B D J K corroborates this assumption, because all are low frequency letters and not likely to occur in the keyword, and it is very reasonable now to assume that the keyword occupies the portion of the foregoing sequence falling between Z and B.

If the letter L does not occur in the keyword, then from alphabetical considerations it must follow the K of B D J K in (7), which will permit the union of (6) and (7). This is impossible because the I of (6) would have to occupy the position of G of (7). Therefore, L must be in the keyword. Since the letter L occurs in the keyword, then from alphabetical considerations the M P of (3) should fall immediately after the K of (7) to give

(8) X Y Z O F . . E T H S G N A . . B D J K M P . . V W

16. **Result of completing the plain component.**—There is now a total of 20 letters in (8) and it may be possible at this point to obtain plain text from some part of the message by correcting for the movement of this sequence against itself and completing the plain component. If this sequence is correct, plain text may result on one generatrix.

The last 10 letters of the message, X O J X K O O X T P, seems a likely portion to use, because all of these letters occur in (8). However, there are letters missing from this sequence, but since the portion of text to be deciphered contains none of the missing letters, the only difficulty which may arise is in the case where a letter in the cipher component may correspond to a blank in the plain component. This difficulty can be surmounted by inserting arbitrary symbols in the blank spaces of (8) to give (9).

(9) X Y Z O F 2 3 E T H S G N A 4 5 B D J K M P 6 7 V W.

The text can now be converted by assuming an initial relative position of the sequence with respect to itself, and proceeding as in deciphering. In order to illustrate this clearly, (9) will be used to convert the first three letters of X 0 J X K 0 0 X T P.

Let the initial relative position of the sequence be that shown herewith:

Plain_____ X Y Z 0 F 2 3 E T H S G N A 4 5 B D J K M P 6 7 V W
Cipher____ X Y Z 0 F 2 3 E T H S G N A 4 5 B D J K M P 6 7 V W

In this position $X_c = X_p$.

The cipher component is moved one space to the left for deciphering the next letter.

Plain_____ X Y Z 0 F 2 3 E T H S G N A 4 5 B D J K M P 6 7 V W
Cipher____ Y Z 0 F 2 3 E T H S G N A 4 5 B D J K M P 6 7 V W X

This gives $0_c = Z_p$.

For the next letter the cipher component is again moved one space to the left giving $J_c = B_p$. This procedure is followed until all 10 letters are converted, giving

X 0 J X K 0 0 X T P
X Z B 7 5 V 7 K X N

The result of completing the plain component for this decipherment is shown in figure 30.

X	Z	B	7	5	V	7	K	X	N
Y	0	D	V	B	W	V	M	Y	A
Z	F	J	W	D	X	W	P	Z	4
0	2	K	X	J	Y	X	6	0	5
F	3	M	Y	K	Z	Y	7	F	B
2	E	P	Z	M	0	Z	V	2	D
3	T	6	0	P	F	0	W	3	J
E	H	7	F	6	2	F	X	E	K
T	S	V	2	7	3	2	Y	T	M
H	G	W	3	V	E	3	Z	H	P
S	N	X	E	W	T	E	0	S	6
G	A	Y	T	X	H	T	F	G	7
N	4	Z	H	Y	S	H	2	N	V
A	5	0	S	Z	G	S	3	A	W
4	B	F	G	0	N	G	E	4	X
5	D	2	N	F	A	N	T	5	Y
B	J	3	A	2	4	A	H	B	Z
D	K	E	4	3	5	4	S	D	0
J	M	T	5	E	B	5	G	J	F
K	P	H	B	T	D	B	N	K	2
M	6	S	D	H	J	D	A	M	3
P	7	G	J	S	K	J	4	P	E
6	V	N	K	G	M	K	5	6	T
7	W	A	M	N	P	M	B	7	H
V	X	4	P	A	6	P	D	V	S
W	Y	5	6	4	7	6	J	W	G

FIGURE 30

The underlined generatrix obviously contains the word INFANTRY. This permits us to replace the 2 and 5 which were arbitrarily written in (9) by the letters I and R, respectively to obtain

X Y Z O F I 3 E T H S G N A 4 R B D J K M P 6 7 V W.

17. **Solution completed.**—Since the correctness of (9) has now been established and a word of the plain text determined, it is an easy matter to recover the letters missing in the sequence and consequently obtain the complete decipherment of the message as shown in figure 31.

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

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

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

FIGURE 31

18. **Concluding remarks.**—If, in the encipherment of this cryptogram, the encipherer had used different mixed sequences for the plain and cipher components, plain text would not have been obtained by completing the plain component with the cipher sequence. However, the analysis of the cipher would have been identical up to the point of completing the plain component, but, instead of converting only a few letters of the cipher text and completing the plain component, it would have been necessary to convert the entire message insofar as the partially reconstructed sequence (9) would permit, and then solve the converted text as a monoalphabet. This procedure will be illustrated in the part of this paper which treats of the solution of the Wheatstone Cipher.

SECTION IV

SOLUTION OF THE MODIFIED WHEATSTONE CIPHER[1]

19. **Preliminary analysis.**—The application of the principles of indirect symmetry of position in the solution of the modified Wheatstone Cipher is without doubt the easiest known method of solution for this cipher.[2] This solution depends upon the presence of a repetition or repetitions in the plain text of a message and their detection and identification as such in the cipher text by the cryptanalyst. The repetition or repetitions must be of sufficient length to permit the reconstruction of an equivalent primary component by the application of the principles of indirect symmetry of position. As in paragraph 14, repetitions can be detected by comparing portions of the cipher text until one or more isomorphisms are found which may be utilized to reconstruct an equivalent primary component of the cipher sequence.

Why isomorphisms appear in the cipher text resulting from two different encipherments of the same plain text can be seen from a study of the following plain text and its corresponding cipher text. Both sequences used in the preparation of this encipherment are given herewith,

Outer sequence:

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

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

Inner sequence:

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

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

[1] For a description of the modified Wheatstone Cipher device and a method for using it see Special Text No. 166, Advanced Military Cryptography 1931 Ed., Paragraph 60.

[2] For another method of solution see Friedman, W. F., *Several Machine Ciphers and Methods for their Solution*, Riverbank Publication No. 20, 1918.

Initial setting of sequences $A_p = A_c$

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

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

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

FIGURE 32

It will be noted that the plain-text repetition underlined in figure 32 does not give a repetition of the cipher text. However, when the cipher text corresponding to the repeated plain text is superimposed their isomorphic character is evident.

Plain..... * B A T Q A L I O N * T W E N T Y * T H I R D *
First encipherment... I Q Y M L H T M B R X T X K V A N J I R C Y S R
Second encipherment. K X C L Q I W L H B Y W Y M Z D P N K B U C R B

Plain..... I N F A N T R Y * W I
First encipherment... I U K V D N X Z V V H
Second encipherment. K S M Z G P Y O Z Z I

FIGURE 33

By pairing off the letters of the first encipherment with the letters of the second encipherment in the above superimposition, the following pairs are obtained:

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

FIGURE 34

In the cipher component, the interval between the first and second letters of each of these pairs is 22; that is, for the pair IK, K is the twenty-second letter beyond I. It follows, therefore, that pairs having common letters can be united to form portions of an equivalent primary component consisting of two sets of 13 letters each, which will be identical with the equivalent primary component derived by decimating the original primary component, using the interval 22.

The reason the interval between I and K is 22 is that the long hand of the device made 22 complete revolutions between the two encipherments of the character beginning each occurrence of the repeated plain text. Since each revolution effects a shift of one space between the plain and cipher sequences the 22 revolutions will effect a relative shift of 22 spaces. Also the reason the interval between the other corresponding letters of the cipher text remains constant at 22 is that the motion of the long hand is governed by the nature of the plain text enciphered, and since the plain text is the same in both cases, the movement of the long hand for both encipherments must be identical. From this it follows that if the nature of the text between the beginnings of the repetitions had been such that the relative shift of the cipher sequence

would have been 8 instead of 22, the interval between the corresponding letters of the two encipherments would have been 8, and instead of the pair I K, the pair I B would have resulted.

20. **An actual example.**—In order to show how the foregoing principles can be applied in the solution of a message, an actual example will be worked out in detail. The cryptogram given herewith is known to have been enciphered by means of a modified Wheatstone Cipher, using two different mixed alphabets.

CRYPTOGRAM

```
                5                  10                  15                  20                  25
G R C S L  J J M Y M  P E J G G  W E N N M  R V M N G

               30                  35                  40                  45                  50
C T I N U  R A N Y S  S X Q G R  M J V T G  X Y D J M

               55                  60                  65                  70                  75
L I F L J  E R U X Z  G P Y P O  N I G G M  L C I W V

               80                  85                  90                  95                 100
F X R U J  U K E B B  F R Q W U  T N R Z I  M I Z F O

              105                 110                 115                 120                 125
M C K J A  S O S Y W  K U A E P  G E P P Q  M N I E F

              130                 135                 140                 145                 150
J M G V C  V F U D L  K Y A V U  N S C T H  T O X X I

              155                 160                 165                 170                 175
D A S N Z  X B A C J  U J C D R  U E Q P H  W R W F N

              180                 185                 190                 195
Q Z H G N  X V V S U  B J G D P  U L O E O
```

FIGURE 35

21. **Reconstruction of the cipher component.**—The first step in the solution of this cryptogram is to pick out portions of the cipher text which are isomorphic. The most thorough and straightforward way of doing this is to follow the procedure given in paragraph 14; that is, to superimpose portions of the cipher text falling on each side of like letters which are adjacent or separated by one, two, three, or four letters. However, this procedure is rather laborious, and it may be eliminated by scanning the cipher text and picking out peculiar patterns of cipher letters which are isomorphic, somewhat in the same manner as a search would be made for repetitions in a monoalphabetic cipher. Such distinctive patterns as A B B A, A B A C A, A A B B A, A B C B A, etc., are easy to pick up with the eye and in a majority of the cases where they do occur in the different encipherments of the same plain text, the cipher text corresponding thereto can be easily discovered.

In the foregoing message two groupings of the type A B C B A are found, beginning with the 94th and 159th letters of the cipher text, respectively. The portions of text including them are superimposed in order to determine whether the isomorphism extends further in either direction.

```
83 85                90                  95                 100                 105                 110                 115
E B B F R Q W U T N R Z I M I Z F O M C K J A S O S Y W K U A E P

       150                 155                 160                 165                 170                 175                 180
X X I D A S N Z X B A C J U J C D R U E Q P H W R W F N Q Z H G N
```

FIGURE 36

In this superimposition, the similarity which can be verified begins with $\overset{86}{F}\rightarrow\overset{151}{D}$ and ends with $\overset{113}{A}\rightarrow\overset{178}{H}$ and it is possible that the plain-text repetition extends on each side of these limits, because neither corroborations nor contradictions can be found for $\overset{85}{B}\rightarrow\overset{105}{I}$, and $\overset{114}{E}\rightarrow\overset{179}{G}$. However, it can be said that the repetition does not extend further than one letter on each side of these limits, because $\overset{84}{B}\rightarrow\overset{149}{X}$ conflicts with $\overset{85}{B}\rightarrow\overset{150}{I}$, and $\overset{115}{P}\rightarrow\overset{180}{N}$ conflicts with $\overset{110}{W}\rightarrow\overset{175}{N}$. In order to preclude the possibility of introducing error, only those portions which show positive evidence of similarity will be used in reconstructing an equivalent primary component.

By pairing off the letters of the foregoing isomorphism and uniting those pairs having common letters, the following sequences can be formed:

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

Unfortunately, since no complete equivalent primary component can be recovered from the available data, it will be necessary to obtain portions of some other equivalent primary component which will permit the consolidation of the above sequences. These portions may be obtained either by assuming sequent letters in the original primary component as was done in the two preceding examples, or by finding other isomorphisms in the message and using the sequences formed from them to combine the sequences already obtained. Of these two courses, the latter is the easier to apply in the analysis of this cipher, because the sequences used are known to be systematically mixed, and to make correct assumptions of sequent letters in such cases is difficult.

In order to find other isomorphisms, repeated letters of the cipher text which are adjacent are superimposed as shown in figure 37.

```
                                    5                 10                15
(1)____ - - - G R C S L J J M Y M P E J G G

                          10                15                20
(2)____ J J M Y M P E J G G W E N N M R V M

                10                15                20                25
(3)____ M P E J G G W E N N M R V M N G C T

                      30                35                40
(4)____ T I N U R A N Y S S X Q G R M J V T

                60                65                70                75
(5)____ Z G P Y P O N I G G M L C I W V F X

                          80                85                90
(6)____ F X R U J U K E B B F R Q W U T N R

               110               115               120               125
(7)____ W K U A E P G E P P Q M N I E F J M

               140               145               150               155
(8)____ U N S C T H T O X X I D A S N Z X B

                    175               180               185               190
(9)____ F N Q Z H G N X V V S U B J G D P U
```

FIGURE 37

In lines 6 and 9 of the superimposition the repetitions $^{81}_{U}\rightarrow{}^{179}_{G}$ and $^{90}_{U}\rightarrow{}^{188}_{G}$, $^{84}_{B}\rightarrow{}^{182}_{V}$ and $^{85}_{B}\rightarrow{}^{193}_{V}$, and $^{87}_{R}\rightarrow{}^{185}_{U}$ and $^{93}_{R}\rightarrow{}^{191}_{U}$ indicate that portions of these two lines are isomorphic. The isomorphism begins with $^{81}_{U}\rightarrow{}^{179}_{G}$ and extends to the end of each of the two lines. A superimposition of the text occurring beyond these two points is made in order to determine where the isomorphism ends.

		80				85				90				95					
U	J	U	K	E	B	B	F	R	Q	W	U	T	N	R	Z	I	M	I	Z	F
			180				185				190				195					
Z	H	G	N	X	V	V	S	U	B	J	G	D	P	U	L	O	E	O	–	–

FIGURE 38

A check at the end of the message is found, viz., $^{95}_{I}\rightarrow{}^{193}_{O}$ and $^{97}_{I}\rightarrow{}^{195}_{O}$, which indicates that the isomorphism includes these letters. However, there is no corroboration for $^{80}_{J}\rightarrow{}^{178}_{H}$, and although it may be possible to include this pair of letters, it is not used in forming the following sequences:

Q B V
M E X
F S
I O
K N P
R U G
W J
Z L

A reference to the first set of partial sequences found shows two, M U Z C E and K Q S W N B, which have letters in common with three of the foregoing sequences. These three are Q B C, M E X, and K N P. In the first set the interval between M and E is 4; in this set it is 1. The new set can therefore be reduced to the interval of the first by rewriting each of its sequences so that the letters are separated by an interval of 4 instead of 1.

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

All these sequences can now be combined to give the following equivalent primary component:

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

22. **Conversion of the cipher text to monoalphabetic terms.**—At this point it is necessary to explain an important characteristic of the cipher text produced by the Wheatstone device. The fundamental cryptographic idea underlying this instrument is to provide two sequences, each of which is composed of a different number of elements, connected by a mechanism in such a manner that intervals between elements of one can be measured in terms of intervals between elements of the other. For instance, in the encipherment of the word FIRST of the example given in paragraph 19 of this section, the interval between the F and I in the plain sequence is equal to the interval between the Q and R of the cipher sequence. Likewise, the interval between the I and R in the plain sequence corresponds to the interval between R and S in the cipher sequence, and so on for the other letters of the message. From this it can be seen that the cipher text of a message merely indicates to the decipherer the number of spaces over which the long hand must be moved in order to pick up the next plain-text letter, and that the cipher sequence serves as a sort of "yardstick" on which these spaces are measured. It follows from this that unless *the exact order* of the letters of the cipher sequence is known, the correct interval between letters of the plain sequence cannot be determined and consequently solution of the message is still a difficult matter, *even if the plain sequence is known.* On the other hand, if the cipher sequence is known, the intervals between letters of the plain sequence can be determined, *and if an arbitrary sequence is inscribed on the outer circle of the device, the process of decipherment will result in a monoalphabetic substitution on the plain text.*[1]

Now the sequence of 26 letters which has been recovered may be either the original primary component or any one of the eleven equivalent primary components of 26 letters which can be derived by a decimation of the original primary component, using an odd interval other than 13. Since it is necessary to obtain the exact sequence of the inner circle in order to convert the cipher text to monoalphabetic terms, it will be necessary at this point to determine the original primary component of the cipher sequence. This component can be obtained by either of two methods. One is to derive the other eleven possible primary components of 26 letters from the sequence above, make the cipher-text conversions for each, and select that conversion which gives a monoalphabetic distribution. Another is to follow the procedure shown on pages 6–11 inclusive of *Methods for the Reconstruction of Primary Alphabets*, Publication No. 21, Riverbank Laboratories, by William F. Friedman, in which the reconstruction of systematically mixed alphabets is treated. The second of these two possibilities is easier to apply in this instance; the first method would have to be used if the sequences were random-mixed. It is found that the component derived by a decimation of the foregoing sequence, using interval 21, gives the best arrangement for a systematically mixed alphabet. This component is given herewith.

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

In this component it is found that the pairs YW, WV, VU, and ZX are each separated by three letters, while the pairs UZ and XY are separated by four letters. This gives a diagram with six columns, and if the letters U V W X Y Z are arranged so that they occur in their normal alphabetical order, the following diagram is obtained and the correctness of the sequence is established:

[1] This idea of conversion of the cipher text can be applied not only to the Wheatstone Cipher, but also to a great many other types of cipher systems based upon two sliding alphabets, if both the cipher sequence and the exact manner in which it is to be used are known.

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

If the sequence resulting from this diagram is inscribed on the inner circle of the device, any sequence whatsoever inscribed on the outer circle, and the process of deciphering applied to the cipher text, a monoalphabetic substitution on the plain text will result. For instance, if we write the normal alphabet, with the word stop(*) falling after Z, in the twenty-seven spaces provided on the outer circle, the sequence obtained from the foregoing diagram on the inner circle, set B of the inner circle opposite A of the outer circle, and convert the message as we would if we were deciphering it, the conversion shown in figure 39 is obtained.

```
Message------ G R C S L J J M Y M P E J G G W E N N M R V M N G C T I N U
Conversion---- S D H K W I H Q I P K H D L K H D L K H S H F H D T M P E H

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

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

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

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

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

              X V V S U B J G D P U L O E O
              W I H Y K M W D H * I G I W H
```

FIGURE 39

23. **Solution of the converted cipher text.**—Since the principles involved in the solution of a monoalphabetic cipher are elementary, it is not considered necessary to go into a detailed explanation of how the solution of this example is obtained. The plain text of the message is given in figure 40.

```
Conversion____ S D H K W I H Q I P K H D L K H D L K H S H F H D T M P E H
Plain text_____ A T * O N E * Z E R O * T W O * T W O * A * M * T H I R D *

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

M I E H R M W I H I M X T D H D T P I U H K W I H Y K M W D
I E D * L I N E * E I G H T * T H R E Q * O N E * P O I N T

H * I G I W H E S * T H * I G I W H I M X T D H J M G I H Y
* S E V E N * D A S H * S E V E N * E I G H T * F I V E * P

K M W D H * I G I W H D K H I M X T D H D T P I U H D L K H
O I N T * S E V E N * T O * E I G H T * T H R E Q * T W O *

Y K M W D H * I G I W H E S * T H * I G I W H I M X T D H K
P O I N T * S E V E N * D A S H * S E V E N * E I G H T * O

W I H Y K M W D H * I G I W H
N E * P O I N T * S E V E N *
```

FIGURE 40

24. **Reconstruction of the plain component.**—All the variable elements incorporated in the cryptogram have been obtained except the plain component. Probably the easiest method of recovering it is to prepare a deciphering alphabet from the above solution based on the arbitrary sequence used in converting the cipher text. The plain component of this deciphering alphabet will be the plain component used in the preparation of the message.

DECIPHERING ALPHABET

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

All 27 elements of the plain component cannot be obtained directly from the above deciphering alphabet, but it is possible to recover the missing letters by reconstructing the diagram from which it was obtained, using the method by which the original primary cipher component was recovered. Application of this method gives the arrangement shown herewith which can be completed without difficulty.

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

SECTION V

AUTOKEY CIPHER USING THE CIPHER TEXT AS A KEY

25. **General discussion.**—The application of the principles of indirect symmetry of position to isomorphisms in the cipher text of a message enciphered by means of an autokey cipher system using the cipher text as a key affords an easy method of solution.

The method of solution for this type of autokey cipher is identical with that used for the Wheatstone Cipher up to the point where the cipher component is reconstructed from isomorphisms. From this point on it differs in only one detail, viz, instead of it being necessary to use the original primary cipher component for converting the cipher text to a monoalphabet, either it, or any one of the eleven possible equivalent primary components consisting of a complete set of 26 letters, may be used. However, as in the aforementioned example, in converting the cipher text to a monoalphabet, it is necessary to duplicate the deciphering process, using an arbitrary sequence as the plain component.

○