PART FIVE

Transposition Systems

CHAPTER 11

TYPES OF TRANSPOSITION SYSTEMS

11-1. Nature of Transposition

Transposition systems are fundamentally different from substitution systems. In substitution systems, plaintext values are replaced with other values. In transposition systems, plaintext values are rearranged without otherwise changing them. All the plaintext characters that were present before encipherment are still present after encipherment. Only the order of the text changes.

a. Most transposition systems rearrange text by single letters. It is possible to rearrange complete words or groups of letters rather than single letters, but these approaches are not very secure and have little practical value. Larger groups than single letters preserve too much recognizable plaintext.

b. Some transposition systems go through a single transposition process. These are called single transposition. Others go through two distinctly separate transposition processes. These are called double transposition.

c. Most transposition systems use a geometric process. Plaintext is written into a geometric figure, most commonly a rectangle or square, and extracted from the geometric figure by a different path than the way it was entered. When the geometric figure is a rectangle or square, and the plaintext is entered by rows and extracted by columns, it is called columnar transposition. When some route other than rows and columns is used, it is called route transposition.

d. Another category of transposition is grille transposition. There are several types of grilles, but each type uses a mask with cut out holes that is placed over the worksheet. The mask may in turn be rotated or turned over to provide different patterns when placed in different orientations. At each position, the holes lineup with different spaces on the worksheet. After writing plaintext into the holes, the mask is removed and the ciphertext extracted by rows or columns. In some variations, the plaintext may be written in rows or columns and the ciphertext extracted using the grille. These systems may be difficult to identify initially when first encountered, but once the process is recognized, the systems are generally solvable.

e. Transposition systems are easy to identify. Their frequency counts will necessarily look just like plaintext, since the same letters are still present. There should be no repeats longer than two or three letters, except for the rare longer accidental repeat. The monographic phi will be within plaintext limits, but a digraphic phi should be lower, since repeated digraphs are broken up by transposition. Identifying which type of transposition is used is much more difficult initially, and you may have to try different possibilities until you find the particular method used or take advantage of special situations which can occur.

f. Columnar transposition systems can be exploited when keys are reused with messages of the same length. As will be explained in Chapter 13, the plaintext to messages with reused keys can often be recovered without regard to the actual method of encipherment. Once the plaintext is recovered, the method can be reconstructed.

11-1. Examples of Columnar Transposition

The most common type of transposition is columnar transposition. It is the easiest to train and use consistently.

a. Simple Columnar Transposition. At its simplest, columnar transposition enters the plaintext into a rectangle of a predetermined width and extracts ciphertext by columns from left to right. For example, a simple columnar transposition with a width of seven is shown below.

Plaintext: ENEMY TANKS APPROACHING HILL EIGHT SIX THREE STOP

E	N	E	M	Y	T	A
N	K	S	A	P	P	R
O	A	C	H	I	N	G
H	I	L	L	E	I	G
H	T	S	I	X	T	H
R	E	E	S	T	O	P

Ciphertext:

ENOHH RNKAI TEESC LSEMA HLISY PIEXT TPNIT OARGG HPXXX

(1) The cryptographer receiving the above message knows only that a width of 7 was originally used. The cryptographer rebuilds the matrix by determining the length of each column and writing the ciphertext back into the columns. With a width of 7 and a length of 42, each column must have 6 letters. Inscribing the ciphertext into columns from left to right recreates the original matrix, and the plaintext can be read by rows.

(2) Not all messages will come out even on the bottom row. Here is the same message with *STOP* omitted. The columns are not all the same length. In this case, the matrix is called an incompletely filled matrix.

E	N	E	M	Y	T	A
N	K	S	A	P	P	R
O	A	C	H	I	N	G
H	I	L	L	E	I	G
H	T	S	I	X	T	H
R	E	E				

Ciphertext:

ENOHH RNKAI TEESC LSEMA HLIYP IEXTP NITAR GGHXX

(3) The deciphering cryptographer must now perform the additional step of determining which columns will be longer than the others. With 38 letters and a given width of 7, dividing 38 by 7 produces 5 with a remainder of 3. This means that the basic column length is 5, but the first 3 columns are 1 letter longer. Sometimes, cryptographers will avoid this additional step by padding message texts so that the bottom row is always completely filled.

(4) The solution of these systems is extremely easy. The security depends on just one number, the matrix width. All you have to do to solve a message enciphered by simple columnar transposition is to try different matrix widths until you find the right one. To try each width, you just do exactly what the deciphering cryptographer does. Divide the total length by the trial width and the result and remainder will tell you the basic column length and how many longer columns there are.

(5) If you suspect that only completely filled matrices are being used, the solution is easier. You only need to test widths that evenly divide into the message length in that case. For example, with a length of 56, you would try widths of 7 and 8. If neither of these worked, you would also try 4, 14, 2, and 28 to cover all possibilities. It is better to try the possibilities closest to a perfect square before you try very tall and very wide matrices.

b. Numerically-Keyed Columnar Transposition. Numerically-keyed transposition systems are considerably more secure than simple columnar transposition. You cannot exhaust all possibilities with just a few tries as you can with the simple systems. The transposition process is similar to that used to produce transposition mixed sequences.

(1) The numerical key is commonly based on a keyword or key phrase. Unlike keywords used to produce mixed sequences, the keyword may have repeated letters in it. To produce a numerical key from a keyword with repeated letters, the repeated letters are numbered from left to right.

1	2	6	4	8	3	7	5
A	A	R	D	V	A	R	K

12	9	1	4	10	8	6	11	2	13	3	7	5
T	R	A	N	S	P	O	S	I	T	I	O	N

(2) As with simple columnar transposition, matrices may be completely filled or incompletely filled. In either case, the plaintext is written horizontally and the ciphertext is extracted by column in the order determined by the numerical key. The following example shows an incompletely filled matrix.

5	6	1	4	3	2
O	R	A	N	G	E
R	E	Q	U	E	S
T	R	E	I	N	F
O	R	C	E	M	E
N	T	S	I	M	M
E	D	I	A	T	E
L	Y				

Ciphertext:

QECSI SFEME ENMMT UIEIA RTONE LERRT DYXXX

(3) The decipherment process for the receiving cryptographer is more complicated than with simple columnar transposition. The cryptographer must decide the column lengths, as before. With the above message, the cryptographer divides the length of the message by the length of the numerical key. In this case, 32 divided by 6 is 5 with a remainder of 2. The basic column length is 5 with two longer columns at the left. The cryptographer then sets up a matrix with the key at the top and marks the column lengths.

5	6	1	4	3	2
O	R	A	N	G	E
•	•	•	•	•	•
•	•	•	•	•	•
•	•	•	•	•	•
•	•	•	•	•	•
•	•	•	•	•	•
•	•				

(4) The ciphertext is now entered by columns according to the numerical key to produce the plaintext.

(5) The solution of numerically-keyed systems is more complex than for simple columnar transposition. It is more than just trying all possibilities. The solution of numerically-keyed columnar transposition is explained in Chapter 12.

11-3. Route Transposition

There are many other ways to transpose messages than columnar transposition using squares and rectangles. The shape of the geometric figure used can be varied, and the method of inscribing and extracting text can be varied. Columnar methods are the most common in military usage, because they are the easiest to learn and use reliably, but other methods may be encountered. Some of these common methods are shown below.

a. Route transposition using other geometric figures.

(1) The rail-fence cipher is inscribed by zigzag pattern and extracted by rows.

			N						M						R						G			
		I		F				E		E				A		R				N		N		
	E				O		C				N		S				I		I				O	
R						R						T						V						W

Ciphertext: **NMRGI FEEAR NNEOC NSIIO RRTVW**

(2) The triangular pattern is inscribed by rows and extracted by columns.

				R				
			E	I	N			
		F	O	R	C	E		
	M	E	N	T	S	A	R	
R	I	V	I	N	G	N	O	W

Ciphertext:

RMIFE VEONI RIRTN NCSGE ANROW

b. The next examples show just some of the possibilities for route transposition using squares or rectangles. Each example is based on *REINFORCEMENTS ARRIVING NOW* to help you see how the route was entered. The route can be:

(1) Inscribed by spiral, out by columns.

R	E	I	N	F
R	R	I	V	O
A	O	W	I	R
S	N	G	N	C
T	N	E	M	E

Ciphertext:

RRAST ERONN IIWGE NVINM FORCE

(2) Inscribed by diagonals, out by alternating rows.

R	I	O	M	A
E	F	E	S	V
N	C	T	I	G
R	N	R	N	O
E	R	I	N	W

Ciphertext:

RIOMA VSEFE NCTIG ONRNR ERINW

(3) In by outward spiral, out by alternating diagonals.

N	G	N	O	W
I	R	C	E	M
V	O	R	E	E
I	F	N	I	N
R	R	A	S	T

Ciphertext:

NIGNR VIOCO WERFR RNEME IASNT

(4) In by L-pattern, out by spiral from lower right.

R	R	R	O	W
E	A	I	N	G
I	S	V	I	N
N	T	N	E	M
F	O	R	C	E

Ciphertext:

ECROF NIERR ROWGN MENTS AINIV

c. Completely filled squares or rectangles are more common with route transposition than with columnar transposition. The reason is that it is often difficult for the cryptographers to figure out how to handle an incompletely filled matrix. It is simpler in practice to completely fill each matrix than to provide rules to cover every incompletely filled situation.

d. The solution of route transposition is largely a matter of trial and error. When you suspect route transposition, see if the message length is a perfect square or if the matrix can be set up as a completely filled rectangle. Then try entering the ciphertext by different routes, and look for visible plaintext by another route.