CHAPTER 12

SOLUTION OF NUMERICALLY-KEYED COLUMNAR TRANSPOSITION CIPHERS

12-1. Completely Filled Matrices - Determining Matrix Size

When completely filled matrices are known or suspected, the first step in their solution is to determine the matrix size. As discussed in Chapter 11 for simple columnar transposition, the correct width must be an even divisor of the message length. With simple columnar transposition, the correct width could be confirmed easily, because plaintext will appear on the rows when the width is correctly selected. It is not as simple with numerically-keyed transposition. Although each row will contain the letters of plaintext for that row when the width is correctly selected, the letters will be out of order. The key to recognition is the vowel count on each row. Vowels should appear consistently with fairly even counts on each row when the correct width is tried. In plaintext, vowels appear about 40 percent of the time even in small samples of text. This is necessary for text to be pronounceable. If some of the rows have too many or too few vowels, you probably have the wrong width. Consider the next cryptogram.

ERESO RIERU GRFPT TEOAE OOSNN MNIEU SDEES MTSUR FYSBW TEARC

EUXRQ GXXXX

a. The cryptogram has 56 letters, assuming the final Xs are all nulls. If a completely filled matrix is suggested by past experience, then the matrix is probably either 7 or 8 letters wide. Write the cryptogram by columns into a trial matrix of each width and count the vowels in each row.

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

E	E	T	O	U	M	S	C	4
R	R	T	S	E	T	B	E	2
E	U	E	N	S	S	W	U	4
S	G	O	N	D	U	T	X	2
O	R	A	M	E	R	E	R	4
R	F	E	N	E	F	A	Q	3
I	P	O	I	S	Y	R	G	3

b. The first matrix, with a width of seven letters, has the more regular spacing of vowels. The letter Q in the first matrix also has a U on the same row, whereas the second matrix does not. The first matrix is clearly the better possibility.

12-2. Matrix Reconstruction by Anagramming

Continuing the same problem, the object now is to rearrange the columns into the original order. The rearrangement of letters to find the original plaintext order is called anagramming. You may be able to see possibilities for complete words on some of the rows, but the Q and the U on the seventh row provide the most obvious starting point. To recover the numerical key at the same time, number the columns in numerical order before starting reconstruction.

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

7	5			
R	E			
C	E			
E	S			
U	M			
X	T			
R	S			
Q	U			
G	R			

a. All the letter combinations produced by placing columns 7 and 5 together look reasonable for plaintext. At this point, you can see that the last two rows should both be followed by vowels. Both the 1 and 6 columns end with two vowels. Here is what each looks like when added to the initial two columns.

7	5	1
R	E	E
C	E	R
E	S	E
U	M	S
X	T	O
R	S	R
Q	U	I
G	R	E

7	5	6
R	E	F
C	E	Y
E	S	S
U	M	B
X	T	W
R	S	T
Q	U	E
G	R	A

b. Both possibilities give good plaintext letter combinations, but at this point, several words are suggested in the second match. REF.. ..CE could be part of *REFERENCE.* XTW could be part of *SIX TWO,* and the UMB in that case would suggest *NUMBER.* With these probable words, clearly column 3 follows 756. Column 7 is the left-hand column, because the letters needed for *REFERENCE, SIX,* and *NUMBER* are on the row above in column 4. Adding columns 3 and 4 produces the next matrix.

7	5	6	3			4
R	E	F	E	R	E	N
C	E	Y	O			M
E	S	S	A			N
U	M	B	E	R	S	I
X	T	W	O			U
R	S	T	O			E
Q	U	E	S			S
G	R	A	N			D

c. The remaining two columns are easily filled in to complete the solution.

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

12-3. Incompletely Filled Matrices - Hat Diagrams

Incompletely filled matrices are also solved by anagramming, but it is a more difficult process because you cannot initially tell which letters are on the same row with each other. If you know or can correctly assume the width of the matrix, you can limit the possibilities. Consider the next cryptogram, which is expected to have a matrix width of eight letters.

EARTR RGHRE TALOA OXUWA UETNE IOTAE ROCTT EROTE EAOSN GHNRD

SEDOO TELHT COEAI TONQR DIMSF EXXXX

a. With a length of 76 letters and a suspected width of 8, there must be four columns with 10 letters and four columns with 9 letters. We can show the range of letters that could be placed in each column by trying the first four columns as the longer columns and alternately, the last four columns as the long columns. The true arrangement is probably neither, but it will serve to show the possible range of first and last letters for each column.

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

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

b. These two extreme situations can be combined into a single diagram, called a hat diagram. It is constructed by using the first diagram. Next, combine the letters that the second diagram shows can precede the already listed letters by adding them to the top of the first diagram. Similarly, draw a line across the bottom of the first diagram to show the possible bottom letters. The altered first matrix is now the completed hat diagram.

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

c. The completed hat diagram can now be used as a guide to show how columns may be aligned together. Its value can be seen if you try to place the Q in the text before a U. There are two Us in the cryptogram. The Q is necessarily near the top of the matrix. The U in column 2 can only be at the bottom of the matrix. The U in column 3 can only be at or near the top of the matrix. The correct U to place with the Q is now obvious. Lining up the Q in column 8 with the U from column 3 produces an initial reconstruction.

8	3	
O	W	
N	A	
Q	U	
R	E	
D	T	
I	N	
M	E	
S	I	
F	O	
E	T	

d. Next, there is an X near the bottom of the matrix in column 2. It will combine well with the SI of the first two columns to produce *SIX.*

8	3	2
O	W	E
N	A	T
Q	U	A
R	E	L
D	T	O
I	N	A
M	E	O
S	**I**	**X**
F	O	U
E	T	W

e. *SIX* is not the only number near the bottom of the matrix. *FOUR* and *TWO* are likely on the last two rows, and column 4 is available with RO near the bottom.

8	3	2	4
O	W	E	A
N	A	T	E
Q	U	A	R
R	E	L	O
D	T	O	C
I	N	A	T
M	E	O	T
S	I	X	E
F	O	U	R
E	T	W	O

f. The E after *SIX* suggests *EIGHT.* The numbers themselves suggest the word *COORDINATES,* which appears in the middle of the matrix. With these words written in, the rest of the columns can be placed.

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

g. All letters are now used, but several letters appear at both the top and bottom of the matrix. The first word of the message is *ALTERNATE,* and the letters before it all appear correctly at the bottom of columns. The L at the bottom after *ONE* correctly appears as part of *ALTERNATE* at the top. Removing the duplicated letters and shifting *ALTERNATE* to begin at the left-hand column completes the solution.

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

h. This solution depended on correctly identifying the width of the matrix and the fortunate appearance of the Q and U. Without the Q and U and without any indication of the width, a great deal more trial and error would be required for a successful solution. Hat diagrams can be constructed for different possible widths, for example, and probable words searched for within the structure of the diagram. The solution is still possible in most cases, although it will often take longer than the example did. When the same keys are reused for a period, special situations can arise which make the solution much easier. The next chapter shows the techniques that can be used in these special situations.