TRANSPOSITION SPECIAL SOLUTIONS

13-1. Special Exploitable Situations

Military forces are rarely equipped to change cryptosystem keys with every message transmitted. The logistics and management problems of providing enough different keys and controlling their use are difficult to handle. Normally, keys will be reused for a period before they are changed. With transposition systems, several special situations can arise when keys are reused that make a solution possible when the system might otherwise resist successful analysis. One of these situations arises in columnar transposition whenever similar beginnings and endings are used with the same width matrix. The keys do not have to be the same in this case as long as the width is the same. Another more general situation occurs whenever two or more different messages of the same length occur using exactly the same keys. Each of these situations is explained in the following paragraphs.

13-2. Similar Beginnings and Endings

With columnar transposition, repeated message beginnings or endings can cause an easily recognizable and exploitable situation. When the same width keys are used and the beginnings are the same, the tops of the columns in each message will consist of the same letters. When the length of the repeated beginning is several times as long as the width of the matrix, these repeated letters are easy to spot.

a. The next two messages demonstrate the techniques that can be used when similar beginnings are encountered. Repeated segments between the two messages are underlined.

Message 1:

```
ASOLI LBOAE WDLIR ACIEL NSAIR   IEDLS NDWND TQNIH UAOTL FMLIF
1             2               3               4             5
AMPES DBREU SCEPV NELOM YEODC   SHCAI TIELT MNAEE IDERA
           6             7               8
```

Message 2:

```
QNILB TSROI RRIEP LIHUE OZYAS   OLSUT ARZEO LTMUI MTQBR OAUSC
1             2               3             4              5
IEEHT RXOLI RSWBO DSERD EODPL   TIAFS EIFAE SDEEE ZT
          6             7              8
```

(1) There are eight repeated segments in each, which shows that the messages are each eight columns wide. The repeated segments are not in the same order, which shows that the two messages use different numerical keys.

(2) Message 1 has 95 letters. Dividing 8 into 95 gives 11 with a remainder of 7. This means that all but one column must have 12 letters. The distance between repeats shows that this is true. All segments have 12 letters except for the fifth segment, which has 11 letters. The fifth segment, beginning IFA, must be the right-hand column of the matrix.

(3) Message 2 has 92 letters. Four columns have 12 letters and four columns have 11 letters.

(4) All repeated segments contain three letters except for the ASOL segment. The column beginning ASOL is probably the left-hand column.

(5) As a result of these observations, we can place the first and last columns in each matrix, and we can separate the middle six columns into two groups of three, based on the length of the columns in message 2.

Message 1:

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

Message 2:

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

(6) Completion of the solution from here is straightforward. Anagram each group of three columns in each message, and the solution is complete. The similar beginning is *ALL REQUISITIONS FOR MEDICAL.*

b. Messages with similar endings, such as a repeated signature block, show repeated segments which represent the bottoms of columns instead of the top. The solution is approached the same way, except that the text will not necessarily appear in the same columns in both messages.

13-3. Messages With the Same Length and Keys

Whenever two or more messages have the same length and are transposed with the same keys, they can be solved together. The more messages you find that are the same length and use the same keys, the easier they are to solve. This technique can be used regardless of the type of transposition system.

a. Solving messages with the same length and keys is particularly effective with columnar transposition. The next example shows how the solution can be approached. The five messages all use the same keys. Their positions have been numbered for easy reference and to aid in key recovery.

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

(1) The Q in message 2 in position 1 must certainly be followed by the U in position 8.

(2) Position 1 must be at the top of a column in the original matrix, since columns are extracted beginning at the top. Position 8 is also probably at the top of a column. This applies not just to message 2, but to all five messages. The position 1 column can be written next to position 8.

1	8
L	L
Q	U
A	G
I	N
J	U

(3) Position 2 must be from the second row of the matrix. If position 8 is from the top row, then position 9 must be from the second row, also. Similarly, positions

3 and 10 are from the third row. Positions 4 and 11 are from the fourth row. Positions 5 and 12 are probably from the fifth row, although these are short messages and there might not be as many as five rows.

	1	8	2	9	3	10	4	11	5	12
Message 1:	L	L	P	P	Q	U	R	A	Y	R
Message 2:	Q	U	S	H	N	B	E	H	T	R
Message 3:	A	G	O	U	E	C	E	M	W	T
Message 4:	I	N	O	R	O	N	O	N	E	N
Message 5:	J	U	N	F	U	R	O	R	T	C

(4) Now the task is to find additional columns to add to the fragments already started. For example, the QU in message 2 should be followed by a vowel, and the most likely letter after JU in message 5 is N. There are three columns with an N in message 5, and only one of these, position 19, has a vowel in message 2. Therefore, we will add columns 19, 20, 21, 22, and 23 to our fragments.

	1	8	19	2	9	20	3	10	21	4	11	22	5	12	23
Message 1:	L	L	E	P	P	O	Q	U	E	R	A	T	Y	R	S
Message 2:	Q	U	A	S	H	A	N	B	O	E	H	A	T	R	E
Message 3:	A	G	E	O	U	R	E	C	E	E	M	S	W	T	O
Message 4:	I	N	G	O	R	E	O	N	T	O	N	T	E	N	W
Message 5:	J	U	N	N	F	I	U	R	T	O	R	A	T	C	I

(5) All of the fragments produce good plaintext except, possibly, the last one. QUA will usually be followed by an R. Of the two columns with an R in message 2, column 12 provides the best combinations.

	1	8	19	12	2	9	20	13	3	10	21	14	4	11	22	15	5	12	23	16
Message 1:	L	L	E	R	P	P	O	R	Q	U	E	S	R	A	T	I	Y	R	S	U
Message 2:	Q	U	A	R	S	H	A	S	N	B	O	M	E	H	A	D	T	R	E	R
Message 3:	A	G	E	T	O	U	R	N	E	C	E	I	E	M	S	S	W	T	O	F
Message 4:	I	N	G	N	O	R	E	P	O	N	T	O	O	N	T	H	E	N	W	T
Message 5:	J	U	N	C	N	F	I	V	U	R	T	A	O	R	A	D	T	C	I	O

(6) All of the matches give good plaintext, except the fifth set, which clearly does not belong now. It is easy now to see words to build on, such as *ARTILLERY*, *QUARTERS* or *HEADQUARTERS*, *JUNCTION*, *SUPPORT*, *FIVE*, and others. All of these leads are added to the completely anagrammed messages.

	1		2	1			1	1		2	1			2	1		2	1		1	2	1		2	1
	1	4	2	5	1	8	9	2	5	3	6	2	9	0	3	6	4	7	3	0	1	4	7	5	8
Message 1:	A	R	T	I	L	L	E	R	Y	S	U	P	P	O	R	T	R	E	Q	U	E	S	T	E	D
Message 2:	H	E	A	D	Q	U	A	R	T	E	R	S	H	A	S	B	E	E	N	B	O	M	B	E	D
Message 3:	M	E	S	S	A	G	E	T	W	O	F	O	U	R	N	O	T	R	E	C	E	I	V	E	D
Message 4:	N	O	T	H	I	N	G	N	E	W	T	O	R	E	P	O	R	T	O	N	T	O	D	A	Y
Message 5:	R	O	A	D	J	U	N	C	T	I	O	N	F	I	V	E	F	O	U	R	T	A	K	E	N

(7) The final step in the solution is to recover the numerical keys. Looking at the beginning, the pattern starts to repeat after seven letters, so the original matrix was seven letters wide. The numerical key, derivable by observing the order in which the columns were extracted, was 4275136.

b. The technique of solving messages of the same length and keys can be used with any transposition system. It can be used as the basis for recovery of more difficult transposition systems such as large grilles and double transposition. The cyclic pattern of columnar transposition aided the solution of the example above. Given four or more messages of the same length and keys, however, the complete messages can often be anagrammed without the help of the cyclic pattern.