CHAPTER 7

SOLUTION OF POLYGRAPHIC SUBSTITUTION SYSTEMS

Section I
Analysis of Four-Square and Two-Square Ciphers

7-1. Identification of Plaintext

Recovery of any digraphic system is largely dependent on the ability to correctly identify or assume plaintext. As with any system, isologs and stereotyped messages can help a great deal. Pattern words can also be of assistance. With unilateral systems, patterns of repeated letters provided an assist. With digraphic systems, patterns of repeated digraphs can do the same thing. Appendix D, beginning on page D-38, includes several types of word pattern tables. The first type, listed on pages D-38 and D-39 shows patterns applicable to any digraphic system. The means of representing digraphic patterns are simpler than those for unilateral patterns. The patterns identify the repeated digraph in a word or phrase by the letters AB in each case, and non-repeating digraphs are just represented by dashes. Here are a few examples that show how the patterns are formed.

```
DE CO DE
AB -- AB

PO ST PO NE
AB -- AB --

MA IN TA IN IN G-
-- AB -- AB AB --

-M AI NT AI N-
-- AB -- AB --
```

7-2. Solution of Regular Four-Squares

Regular four-square ciphers, in which the plaintext squares are in A through Z order, are slightly easier to solve than the type with all mixed squares.

a. With the known plaintext squares, an additional type of word pattern can be used. Since the plaintext locations are fixed, certain words will always produce single letter ciphertext repeats. The word MI LI TA RY, for example, will always produce a repeated ciphertext letter in the first and third cipher position. When MI LI TA RY is enciphered by the matrix shown in paragraph 6-3, it produces KL KO NS SW. Four-square word patterns are shown on pages D-43 through D-47. The patterns are represented by the repeated letters only, placing A, C, E, and soon in the first letter positions of digraphs, and B, D, F, and so on in the second letter positions. Repeats between different positions are ignored. Following these rules, a few examples of four-square word patterns appear below.

```
re qu es te d-
UR UM AU US OY
A- A- -- A- --

el em en ts
PK LK AK RQ
-B -B -B --

qu ar te rm as te r-
UM LM US QF AM US RW
AB -B AD -- -B AD --
```

b. Identifying the four-square from other digraphic systems is largely a matter of elimination. It will include double letters, unlike the Playfair. It will not include a high proportion of good plaintext digraphs or reversed plaintext digraphs like the two-squares. There is no ready clue to tell whether a four-square is a regular one or not, but it is often easiest to assume the simplest case for a start and only consider more complicated construction when the simple case fails to produce a solution.

c. To demonstrate the use of four-square word patterns and recovery of the system, consider the cryptogram shown below.

```
TATO UTOD HIDM FIPK ROFM  HRVH BMAH NHKM UNAN ZMRO
SKHH RQBX FSYF KQNS QFAT  KQUY SMQP SMNT MYRO RYDM
FIPK ROFM IQLT TYSQ RYRV  FEDC ATGR RHTO AOTD QP
```

d. The underlined repeats give a chance to try a four-square word pattern as an entry to the cryptogram.

```
DM FI PK RO FM
-B A- -- -- AB
```

The only word with this pattern in Appendix D is INFORMATION. Placing *INFORMATION* in the text, and beginning reconstruction of a regular matrix produces the next example.

```
            in form atio  n
TATO UTOD HIDM FIPK ROFM  HRVH BMAH NHKM UNAN ZMRO

                                                in
SKHH RQBX FSYF KQNS QFAT  KQUY SMQP SMNT MYRO RYDM

form atio n
FIPK ROFM IQLT TYSQ RYRV  FEDC ATGR RHTO AOTD QP
```

	a	b	c	d	e				R		
	f	g	h	i/j	k			D	F		
p1	l	m	n	o	p						HI c1
	q	r	s	t	u		P				
	v	w	x	y	z						
						a	b	c	d	e	
						f	g	h	i/j	k	
c2	I	K		M		l	m	n	o	p	p2
	O					q	r	s	t	u	
						v	w	x	y	z	
			R								
			Q								

e. The recovered values have been placed in the matrix, and the alphabetic construction is apparent. Additionally, four values have been placed outside the matrix for the moment as suggested by the plaintext Ns at the end of *INFORMATION.* H and I must be in the same row as plaintext N. R and Q must be in the same column. Several additions can now be made from the alphabetic construction. L and N fit in the third row of the c2 matrix. Further, if H and I are in the third row of the cl matrix, then they must be the first two letters on that row and G is the last letter of the second row. Placing all of these in the matrix and using the partially recovered matrix to decipher as much plaintext as possible produces the next example.

```
          llin form atio  n                     at
TATO UTOD HIDM FIPK ROFM  HRVH BMAH NHKM UNAN ZMRO

     c                                     at   in
SKHH RQBX FSYF KQNS QFAT  KQUY SMQP SMNT MYRO RYDM

form atio n                      h
FIPK ROFM IQLT TYSQ RYRV  FEDC ATGR RHTO AOTD QP
```

	a	b	c	d	e				R		
	f	g	h	i/j	k			D	F	G	
p1	l	m	n	o	p	H	I				c1
	q	r	s	t	u		P				
	v	w	x	y	z						
						a	b	c	d	e	
						f	g	h	i/j	k	
c2	I	K	L	M	N	l	m	n	o	p	p2
	O					q	r	s	t	u	
						v	w	x	y	z	
			R								
			Q								

f. Next, suppose that Q in the c1 matrix is in the keyword. If so, the U would normally be with it. There are not enough letters left in the alphabet after the P in the cl matrix to put both Q and U at the beginning, so Q is almost certainly right after the P.

g. We can be fairly confident of the recoveries up to this point. A number of possibilities present themselves, but as they are only possibilities, the work should be done lightly in pencil. We can next try placing the Q and R in the c2 matrix. The Q is more likely to be in the sequence than the keyword, so we will tentatively place it in the fourth row and R in the first row. We can place P in the fourth row, also, before Q. Another possibility is to place plaintext A on line one of the message, forming the word *ALL* before *INFORMATION.*

```
        a llin form atio  na                    at
TATO UTOD HIDM FIPK ROFM  HRVH BMAH NHKM UNAN ZMRO

     ct                          rs        at   in
SKHH RQBX FSYF KQNS QFAT  KQUY SMQP SMNT MYRO RYDM

form atio nr                     he           rs
FIPK ROFM IQLT TYSQ RYRV  FEDC ATGR RHTO AOTD QP
```

						O					
	a	b	c	d	e				R		
	f	g	h	i/j	k			D	F	G	
p1	l	m	n	o	p	H	I				c1
	q	r	s	t	u		P	Q			
	v	w	x	y	z						
			R			a	b	c	d	e	
						f	g	h	i/j	k	
c2	I	K	L	M	N	l	m	n	o	p	p2
	O	P	Q			q	r	s	t	u	
						v	w	x	y	z	

h. Next consider the plaintext RS on line two. It must certainly be preceded by a vowel, therefore, the ciphertext digraph SM must produce a vowel in the p2 position. The only vowel in the same row in the p2 matrix as the ciphertext M in the c2 matrix is plaintext O. S must be in the fourth column of the c1 matrix above the plaintext O. The only logical place for the S is on the fourth row. Adding the S and entering the values increases our solution as shown in the next example.

```
        a llin form atio  na                    at
TATO UTOD HIDM FIPK ROFM  HRVH BMAH NHKM UNAN ZMRO

     ct                        tors to     at   in
SKHH RQBX FSYF KQNS QFAT  KQUY SMQP SMNT MYRO RYDM

form atio nr     st              he           rs
FIPK ROFM IQLT TYSQ RYRV  FEDC ATGR RHTO AOTD QP
```

						O					
	a	b	c	d	e				R		
	f	g	h	i/j	k			D	F	G	
p1	l	m	n	o	p	H	I				c1
	q	r	s	t	u		P	Q	S		
	v	w	x	y	z						
			R			a	b	c	d	e	
						f	g	h	i/j	k	
c2	I	K	L	M	N	l	m	n	o	p	p2
	O	P	Q			q	r	s	t	u	
						v	w	x	y	z	

i. These additions suggest several possibilities. *STOP* may appear in the middle of line 2. *REQUEST* may be the word after *INFORMATION* on line 3. Placing these values produces good alphabetical progression in the matrix and many more plaintext possibilities.

```
  qu    a llin form atio na          on        at
TATO UTOD HIDM FIPK ROFM HRVH BMAH NHKM UNAN ZMRO

ro   ct   it   nsou      ns   tors topu pdat edin
SKHH RQBX FSYF KQNS QFAT KQUY SMQP SMNT MYRO RYDM

form atio nreq uest edby        he   qu    e rs
FIPK ROFM IQLT TYSQ RYRV FEDC ATGR RHTO AOTD QP
```

	a	b	c	d	e	L			R		
	f	g	h	i/j	k			D	F	G	
p1	l	m	n	o	p	H	I	K	M	N	c1
	q	r	s	t	u	O	P	Q	S	T	
	v	w	x	y	z						
			R		Y	a	b	c	d	e	
						f	g	h	i/j	k	
c2	I	K	L	M	N	l	m	n	o	p	p2
	O	P	Q	S	T	q	r	s	t	u	
	U	V	W	X	Z	v	w	x	y	z	

j. From here, the solution is routine. *REQUEST* is the first word. *HEADQUARTERS* is the last word. These values in turn fill in enough blanks in the matrix to recognize the keywords and complete the solution. The keywords are LAUREL and HARDY.

7-3. Solution of Mixed Four-Squares

Slightly different techniques must be used when standard sequences are not used in the p1 and p2 squares. The specific four-square word patterns of Appendix D, pages D-43 through D-47 no longer apply, although the general digraphic patterns that precede them on pages D-38 and D-39 are still applicable. Generally, because the matrix construction is less orderly, more text must be known or assumed to successfully complete the solution. The problem that follows shows how the solution can be approached with mixed squares.

```
FMFE FMPX ZPYX IYYP GGME  TXGS YGGB YLFI HAGB YLMK
MRGH YRFM BYYP MMBQ YMHD  MHLN MNOS YPVI DMXH RPGL
MNSO QLMP GBYL VGQI QLYX  KTZG HEEM GBKM FLYK PHMA
SREE GDMK DEBG TTEB IXCN  VINI SOSC HHIG THHM OQPO
TGKI VGQI PMXR CPGH YRSE  PLMN LNMN ACVC OCCO KPWC

PKIP PCSU GHYR FKSC YGXX
```

a. The above cryptogram has been identified as a four-square. Previous messages from the same headquarters have been signed by ADAMS or MILLER. The repeated segments in the text suggest several possibilities for plaintext.

(1) The AB -- AB pattern at the beginning fits the common stereotype *REFERENCE.*

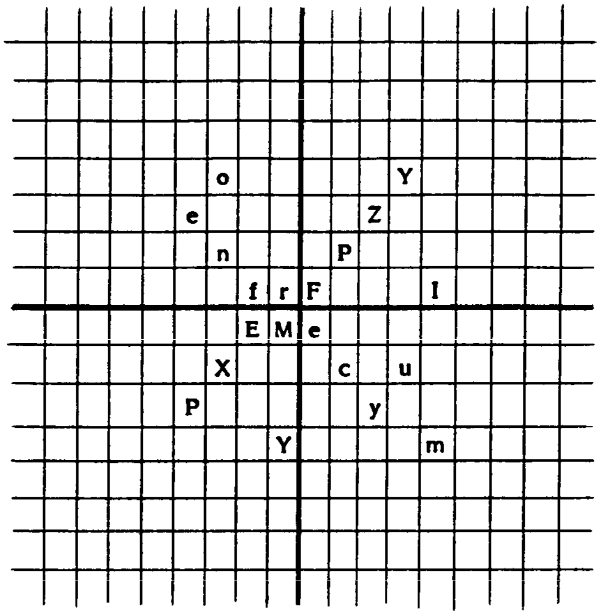
(2) The repeated GBYL segments appear to be numbers, and the number of characters is exactly right to fit in the expanded stereotype *REFERENCE YOUR MESSAGE NUMBER,* before the numbers. To add to this, recent messages from the addressee have been numbered in the mid 4500s. *FOUR FIVE FOUR* is probably the text of the first three numbers.

(3) GHYR occurs at good sentence length intervals and is probably *STOP.*

(4) These possibilities give enough values to begin reconstructing the matrix.

b. If you assume that standard p1 and p2 squares were used, entering the values in the matrix produces conflicts. The squares must be mixed. To recover a mixed four-square, divide a sheet of cross-section paper into four areas, representing the four squares. The areas cannot initially be limited to 5 by 5 squares, although eventually the recovered values will condense into that size. Proceed by entering each plaintext and ciphertext pair of digraphs into the appropriate areas, maintaining the rectangular relationship. Start new rows and columns for each pair entered unless there are one or more values in common with previous entries. The entries for the first seven pairs are shown in the next diagram.

```
refe renc eyou rmes sage  numb erfo urfi vefo ur
FMFE FMPX ZPYX IYYP GGME  TXGS YGGB YLFI HAGB YLMK

 st  op
MRGH YRFM BYYP MMBQ YMHD  MHLN MNOS YPVI DMXH RPGL

          four
MNSO QLMP GBYL VGQI QLYX  KTZG HEEM GBKM FLYK PHMA

SREE GDMK DEBG TTEB IXCN  VINI SOSC HHIG THHM OQPO

                 st   op
TGKI VGQI PMXR CPGH YRSE  PLMN LNMN ACVC OCOO KPWC

          stop
PKIP PCSU GHYR FKSC YGXX
```



c. The first digraph pair entered was plaintext re equalling ciphertext FM, appearing in the inner corners of the four areas. We will use the notation re=FM to represent such pairs from here on with the plaintext in lower case. The next pair, fe=FE was placed on the same row as the first pair because of the common letters with the first pair. The entries continue, placing the letters on new rows and columns except when previously used values occur. The eighth pair, es=YP, presents a new situation. Plaintext e and ciphertext Y are already on different rows. The new pair shows that these two rows should be combined. The diagram below shows the entry before combining the rows. The rows are combined by writing the plaintext o of the first row in the same position on the second row.

					o						Y				
				e						Z	Y				
					n				P						
						f	r	F				I			
						E	M	e							
					X				c		u				
				P						y	s				
							Y					m			

d. When all entries have been made and all rows and columns combined wherever possible, the diagram appears as shown below. All plaintext that can be deciphered from the partially recovered matrix is also filled in.

```
refe renc eyou rmes sage   numb erfo urfi vefo ur
FMFE FMPX ZPYX IYYP GGME   TXGS YGGB YLFI HAGB YLMK

  st opre   es  e                    es            a
MRGH YRFM BYYP MMBQ YMHD   MHLN MNOS YPVI DMXH RPGL

          four        ou     e       fo
MNSO QLMP GBYL VGQI QLYX   KTZG HEEM GBKM FLYK PHMA

SREE GDMK DEBG TTEB IXCN   VINI SOSC HHIG THHM OQPO

 r                st  op
TGKI VGQI PMXR CPGH YRSE   PLMN LNMN ACVC OCOO KPWC

          stop      er
PKIP PCSU GHYR FKSC YGXX
```

						g		M							
	f	m		s									G	F	
			u	e	o					Z	Y				
					n				P		T				
						f	r	F				I			
						E	M	e							
					X				c		u				
				P						y	s				
							Y					m			
			L	G							r		a		
		S											b		
	B												o		
	I													i	
				H									t		
					R						p				

e. More plaintext can be added at this point. The four-letter number after *FOUR FIVE FOUR* must be *NINE,* because ZERO will not fit properly in the matrix. The word beginning at the end of the first line is probably *REQUEST*, and the sender is *MILLER*, not ADAMS. When these recoveries are added to the matrix, there are enough recoveries to see the basic structure of the four-square.

	l												S
						q				B			
		u	e	o					Z	Y			
				n	g	t	M	P		T			
			s	m	f	r	F				I	G	
				R	E	M	e			p			
				X		Y		c		u	m		
			P						y	s			
		L	G							r		a	
				S								b	
					B							o	
				K	I								
			H									t	
	C												l

f. Each area shows signs of alphabetic progression. The upper right area shows partial rows with the letters FGI, MPT, and YZ. The lower left has rows with IK and XY. The upper left has columns with fg, mno, and qrt. The lower right has a column with prsu in it. These patterns suggest that the plaintext squares (upper left and lower right) use sequences entered by columns and the ciphertext squares use sequences entered by rows. With this in mind, the rows and columns can be rearranged. The most obvious place to start is to rearrange the rows so that the partial sequences FGI, MPT, and YZ are the last three rows in the upper squares.

	I												S	
						q				B				
			s	m	f	r	F				I	G		
				n	g	t	M	P		T				
		u	e	o					Z	Y				
				R	E	M	e			p				
				X		Y		c		u	m			
			P						y	s				
		L	G							r		a		
				S								b		
					B							o		
				K	I		i							
			H									t		
	C												!	

g. Moving these three rows put the letters mno and fg in the correct order in the upper left area. The row before these. three rows also appears to be correctly placed. Now examine the column arrangement. In the upper right area, the Y and Z are probably in the last two columns in the original matrix. With the T placed directly above the Y, there are just enough spaces to fill in UVWX between the T and the YZ on the bottom two rows. Then, with the U appearing in the alphabetical progression, the Q is probably the missing letter on the fourth row. The complete fourth row can be placed in MPQTU order. Similarly, in the upper left area, the fg, mno, and qrt columns are probably the second, third, and fourth columns of that matrix. We can now rearrange the columns so the first five columns on each side of the center line reflect the original order.

		I													S
						q					B				
	s			f	m	r	F					G	I		
				g	n	t	M	P	Q	T	U				
u	e				o		V	W	X	Y	Z				
				E	R	M	e			p					
					X	Y		c		u			m		
	P									s	y				
L	G									r		a			
					S							b			
				B								o			
				I	K		i								
	H											t			
		C												!	

h. The rearranged matrix suggests many more possibilities. In the upper left area, uvwxyz can be filled in as was done with the upper right. In the upper right, the G can be moved next to the F, combining two columns. Rows can be rearranged in the lower areas. Examining the lower right area, the fourth column must include the q by the same logic as was used in the upper right area. The correct order is pqrsu.

		l													S
							v								
						q	w				B				
	s			f	m	r	x	F	G					I	
				g	n	t	y	M	P	Q	T	U			
	e				o	u	z	V	W	X	Y	Z			
				E	R	M		e			p				
											q				
	G					L			a		r				
	P										s	y			
					X	Y			c		u			m	
					S				b						
				B					o						
				I	K			i							
	H								t						
		C												l	

i. All the rows and columns outside the 5 by 5 squares can be systematically placed in the squares by following the alphabetical order. Fully combined, the four-square appears below.

			p	v					
		l	q	w	S			B	
s	f	m	r	x	F	G	I	K	L
	g	n	t	y	M	P	Q	T	U
e		o	u	z	V	W	X	Y	Z
H	E	R	M		e	t		p	v
	B	C	D	F	l	o		q	w
G	I	K	L		i	a		r	x
P	Q	S	T	U		b		s	y
V	W	X	Y	Z		c	m	u	z

j. The remaining values are easily recovered by using this matrix to fill in more plaintext in the cryptogram. The additional plaintext will suggest still more plaintext, which can be used to complete the four-square.

7-4. Solution of Two-Square Ciphers

The solution of two-square ciphers, either horizontal or vertical, is similar to the solution of a mixed four-square, only much simpler. The worksheet is divided into two areas by a vertical or horizontal line, as appropriate, instead of four. Plaintext is much easier to recognize because of the transparencies that occur. Matrix reconstruction proceeds, like the four-square, by entering digraph pairs in their rectangular relationship, except for transparencies, which are plotted in the same row or column. New values are plotted in new rows and columns, unless one or more values are in common with previous plots, as with the four-square. As recovery proceeds, working back and forth between the matrix and the text, the two-squares can be combined and condensed to the original form, like the four-square.

Section II
Analysis of Playfair Ciphers

7-5. Security of Playfair Ciphers

Breaking into Playfair ciphers is similar to the solution of mixed four-squares in some respects and very different in others.

a. The Playfair shares the rectangular principle of encipherment with four-squares and two-squares, but it is complicated further by the EBDA and ERDL rules. When recoveries are plotted, every possible rule must be considered, not just the rectangular rule.

b. Recognition of plaintext is aided by another type of word pattern that occurs with Playfair only. Whenever a plaintext digraph is repeated in reverse order, the ciphertext appears in reverse order, too. This does not happen with four-squares and two-squares. It occurs whichever rule of decipherment is used. The word DEFENDED, for example, has a Playfair word pattern of AB -- -BA, the same as DEPARTED, RECEIVER, and a number of others. Playfair word patterns are listed in Appendix D, pages D-40 through D-42. The general digraphic word patterns of pages D-38 and D-39 can also be used.

7-6. Reconstruction of Playfair Ciphers

To illustrate the analysis of Playfair ciphers and the reconstruction of the Playfair matrix, consider the following message. This message was sent from a brigade headquarters to three subordinate battalions.

```
DT BV VF GO OG MV CQ IH NS MN VI FC IK FK NX KH UB GK AV LH
CA CF WC YC IA VM PB CI FK CA GV UH NC BX OV LY NU CQ ED GO
OG MV CQ VW OV UB QH CM CM QM UO BX OV YG DH HB KR CY OG MV
CQ IH NS NS QR EX IU GO OG OE GO XK AV DT CB XK AV XK AV YV
TQ RH OC NS NB GS LG FN RH GO CV MX VM SL FU CM GO XK AV KT
GH KT GH DT CB YV TQ
```

a. Initial plaintext recoveries are fairly easy with this message.

(1) The XK AV repeats on line four strongly suggest *ZE RO* with another four digit letter group in between them. The numbers are most likely to be a spelled out time.

(2) YV TQ, appearing after the time and at the end of the message, is probably *ST OP.*

(3) The series of four letter repeats beginning with *ZE RO* at the end of line five and continuing on line six before the final *ST OP* is probably another time.

(4) The repeat GO OG MV CQ has a number of possibilities in Appendix D, but in the context in which the message was sent, it is most likely to be *B AT TA LI ON.*

(5) If BATTALION is correct, then the partial repeat beginning at the end of line three represents the plaintext *TA LI ON.* This is again part of the word BATTALION, but the word started out as an even letter division with the digraph *BA.* TT, the next digraph, is impossible with the Playfair system, so a null must have been inserted, probably *TX.* With the addition of the null, the remainder of the word is divided into digraphs, as before, to produce the partial repeat.

(6) The ciphertext in the middle of line four, GO OG OE GO, which deciphers as *AT TA -- AT* using the common values from *B AT TA LI ON,* is probably *AT TA CK AT.*

b. These plaintext recoveries give more than enough information to reconstruct the original Playfair matrix. The trickiest step in matrix reconstruction is to pick the best starting point. As every possibility for the matrix is plotted, it can get very complicated. Careful selection of what values to place first can reduce the complexity a great deal. The cryptogram is repeated below with all recovered values filled in to assist in finding the best starting point.

```
       b at ta li on
DT BV VF GO OG MV CQ IH NS MN VI FC IK FK NX KH UB GK AV LH

               il                                  on  b at
CA CF WC YC IA VM PB CI FK CA GV UH NC BX OV LY NU CQ ED GO

ta li on                                        ba tx ta li
OG MV CQ VW OV UB QH CM CM QM UO BX OV YG DH HB KR CY OG MV

on                   at ta ck at ze ro        ze ro ze ro st
CQ IH NS NS QR EX IU GO OG OE GO XK AV DT CB XK AV XK AV YV

op                                  il           at ze ro
TQ RH OC NS NB GS LG FN RH GO CV MX VM SL FU CM GO XK AV KT

               st op
GH KT GH DT CB YV TQ
```

(1) Usually the best starting point, if available, is to select a digraph pair where there is a letter in common between the plaintext and ciphertext digraphs. These only occur when adjacent rows or columns are involved, using the ERDL or EBDA rules respectively. This problem does not have any recovered digraph pairs with a common letter, so another starting point must be found.

(2) The next best starting point is to find two digraph pairs with at least two letters in common between the two pairs. The ro=AV and at=GO pairs share the As and Os in common. Other pairs are also possible.

(3) The reconstruction begins by taking one of the selected pairs and plotting each possibility for it. All three rules must be considered. The three separate plots that follow show the result of plotting ro=AV for the rectangular rule, ERDL, and EBDA in turn.

```
Rectangular rule:          ERDL:              EBDA:

   R    A              R A    O V               R
                                                A

   V    O                                       O
                                                V
```

(4) The positioning of the letters is arbitrary. In the rectangular plot, we do not know that R is to the left of A or above V. We do not know how many rows and columns occur between the characters. We only know that the four letters form

a rectangle if that is the correct rule. In the ERDL plot, we do not know that RA is to the left of OV or if there is a column in between the pairs or not. Similarly, in the EBDA plot, we do not know that RA comes above OV or if there is a row in between. The spaces and placements are unknown until the reconstruction has proceeded further.

(5) The next step is to add our second pair to the first plots. Again, we have to consider all three rules as we add the second pair. With three possible rules for each pair, there could be as many as nine different possible plots after two pairs if we did not select some letters in common to limit the possibilities.

(6) Consider first, the addition of at=GO to the rectangular plot of the first pair.

```
R   A   G

V   O   T
```

(7) ERDL cannot be used with the second pair, since we have already placed A and O in separate rows. To use ERDL, they must be in the same row.

(8) When EBDA is applied to the at=GO pair and linked to the ro=AV rectangular plot, the plot looks like this.

```
R   A
    G

    T
V   O
```

(9) When we try to link at=GO to the ERDL plot for ro=AV, it cannot be done. With A and O in the same row, the rectangular plot and the EBDA plot cannot be applied properly. If we try to plot ERDL for at=GO, it results in six different letters on the same row, which is not possible in a normal Playfair. Therefore, we can cross out or erase the ERDL plot for ro=AV.

(10) We next plot all possible rules for at=GO with the EBDA plot for ro=AV. The rectangular rule is the only possibility. ERDL for at=GO is impossible, because we have already placed A and O in the same column. EBDA is impossible, because it would place six different letters in the same column.

```
R   A   G  |  R   A  |  R
           |      G  |  A   G
           |         |
V   O   T  |      T  |  O   T
           |  V   O  |  V
```

(11) The next step is to again pick a digraph pair with at least two letters in common with the letters already plotted. The most obvious possibility is the ba=KR on line three. Following the same approach as we did with the second pair, we find four possibilities this time.

```
R  A  G

V  O  T

B  K
```

```
R  A
   G

   T
V  O

B  K
```

```
BK AR  G

   OV  T
```

```
BK AR
   G

   T
   OV
```

(12) Both st=YV and op=TQ have two letters in common with the recovered diagrams. Checking all possibilities for each of these produces the next four diagrams.

```
R  A  G
V  O  T
B  K
S     Y
   Q  P
```

```
    A  GR
SY  O  TV
    K   B
    Q  P
```

```
BK AR G
   OV T
    S Y
   Q  P
```

```
R  AG
V  OT  PQ
B  K
S   Y
```

(13) Various approaches can be used to further build the possible diagrams. One approach is to try to recover more text. The repeated KT GH is certain to be a spelled out number. If we try to decipher KT using all of our trial diagrams, all

but the third one produce plaintext -O. The third diagram produces G-. From these results, we can rule out the third diagram, since no number has a G in the first position. The number *FO UR* is the only likely plaintext with O in the second position. We add fo=KT to the three remaining diagrams and then try to fit ur=GH. In each case, only the ERDL rule will apply. The last of the three remaining diagrams is also eliminated, since ur=GH cannot be plotted. We are left with these possibilities.

R	H	A	U	G
V		O		T
B		K		F
S				Y
		Q		P

		A	U	G	R	H
S	Y	O		T	V	
		K		F	B	
		Q		P		

(14) The second diagram above is impossible, since there is no way to fit the SY so that it aligns with the row above it. We are finally down to a single diagram, and with careful selection of digraph pairs to plot, we can keep it to a single diagram. Next we will plot on=CQ, tx=CY, and ze=XK.

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

(15) The X, Y, and Z on the fourth line clearly belong in sequence.

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

(16) The partially reconstructed matrix can now be used to add substantially more plaintext in the message.

```
      b at ta li on     x       et    ef     a re af ro
DT BV VF GO OG MV CQ IH NS MN VI FC IK FK NX KH UB GK AV LH

ou te    xt    il  f    ef ou rt hr    es to       on  b at
CA CF WC YC IA VM PB CI FK CA GV UH NC BX OV LY NU CQ ED GO

ta li on    to re a           ac es to       r  ba tx ta li
OG MV CQ VW OV UB QH CM CM QM UO BX OV YG DH HB KR CY OG MV

on     x  x  a       at ta ck at ze ro    ve ze ro ze ro st
CQ IH NS NS QR EX IU GO OG OE GO XK AV DT CB XK AV XK AV YV

op ar t   x  e ry    ep ar at  o    il    eg    at ze ro fo
TQ RH OC NS NB GS LG FN RH GO CV MX VM SL FU CM GO XK AV KT

ur fo ur    ve st op
GH KT GH DT CB YV TQ
```

(17) DT CB is clearly FIVE. The word on line five, after op=TQ is AR TI LX LE *RY*. The second row includes the numbers *-F IV EF OU RT HR EX E-*. These additions are placed in the matrix.

```
R H U G A

B D E F K
L   N P Q

S   X Y Z
V I C T O
```

(18) The missing M and W are easily placed alphabetically. The rows are placed in correct order by shifting the last row to the top and placing the remaining rows alphabetically. The keyword is VICTOR HUGO.

(19) To solve Playfair systems like this, it is important to remember to try all possibilities and to keep the work as simple as possible. It is very easy to overlook possible arrangements, so work very carefully. Always look for the digraph pairs with the least possibilities to plot to keep the work from getting very complex. If the square appears to be alphabetical in construction, use the alphabeticity to help you put rows and columns in the correct order whenever you can.