CHAPTER 9

SOLUTION OF PERIODIC POLYALPHABETIC SYSTEMS

Section I
Systems Using Standard Cipher Alphabets

9-1. Approaches to Solution

When standard alphabets are used with monoalphabetic systems, three approaches are possible. The simplest occurs when text can be immediately identified. Identification of only two or three letters in a standard unilateral alphabet is sufficient to reconstruct and confirm the entire alphabet. The other two methods, where text is not readily identifiable, are to match frequency patterns to the normal A through Z pattern and to generate all possible solutions. All three of these methods also apply to standard alphabet periodic polyalphabetics.

9-2. Solution by Probable Word Method

When the alphabets in a periodic system are known or suspected to be standard, the identification of one plaintext word is usually enough to recover the whole system. The period must be identified first, as explained in the previous chapter, either by analysis of repeat intervals or by the phi test. Then when a word is recognized from repeats or stereotypes, the alphabets can be written and tried throughout the cryptogram. If they produce good plaintext throughout, the problem is solved.

```
EIYMB EKVWO YBTOE ILMFK CRRAK  WJWBZ ELUYO NZUZF ZNTIH YMZXT
IMSWG WRRPC HFGNV ZQALN QCNGJ  VBFSQ RVFPO ENISI CIMHJ SJDBT
ALSDI CSOGH ZYAWW JCEQE MRCFY  KIIXC SERRE RGZPB RMJDC IMRHZ
SFZXT TWQHW YHVAG UYDUS QPGJD  BTSGZ JYAGK KARXQ MJE
```

Repeats	Distance	Factors
ZXT	105	3, 5, 7
CIM	54	3, 6, 9
JBDT	77	7, 11

Factor analysis does not show us a clearcut period length, but if we select the four letter repeat as the most likely causal repeat, 7 appears to be the correct period. If we also try *STOP* as the four letter repeat, it gives us the following text and alphabets.

```
re    nais    cer e   t sen    smov    he av    idge    ing
EIYMB EKVWO YBTOE ILMFK CRRAK  WJWBZ ELUYO NZUZF ZNTIH YMZXT

e   p men    owar    ud dy     erso    ofb a   r svi    stop
IMSWG WRRPC HFGNV ZQALN QCNGJ  VBFSQ RVFPO ENISI CIMHJ SJDBT

   my po    ions    ngr i   h  ave    nhea    yr ei    rced
ALSDI CSOGH ZYAWW JCEQE MRCFY  KIIXC SERRE RGZPB RMJDC IMRHZ

  ing p   f our    htho    st  op    sonc    and i
SFZXT TWQHW YHVAG UYDUS QPGJD  BTSGZ JYAGK KARXQ MJE
```

```
p:   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
C1:  N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
C2:  E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
C3:
C4:
C5:
C6:  R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
C7:  K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
```

From the partial plaintext that this produces, *STOP* is clearly correct. Such words as *RECONNAISSANCE, HEAVY,* and *REINFORCED* are apparent, any one of which will complete the solution. For another type of probable word approach, applicable to periodics or aperiodic, see paragraph 10-3c on crib dragging.

9-3. Solution by Frequency Matching

With monoalphabetic systems using standard alphabets, the solution was very easy whenever a message was long enough to give a recognizable pattern. The characteristic pattern of highs and lows of a standard sequence cannot be easily concealed. The same technique applies to polyalphabetic systems, although messages necessarily must be longer to produce a recognizable pattern for each separate alphabet.

```
FNPDM GJRMF FTFFZ IQKTC LGHAS   EOSIM PVLZF LJEWU WTEAH EOZUA
NBHNJ SXFFT JNRGR KOEXP GZSEY   XHNFS EZAGU EORHZ XOMRH ZBLTF
BYQDT DAKEI LKSIP UYKSX BTERQ   QTWPI SAOSF TQKTS QLZVE EYVAE
JSNFB IFNEI OZJNR RFSPR TEHNJ   ROJSI UOCZB GQPLI STUAE KSSQT
EFXUJ NFGKO UHLZF HPRYV TUSCP   JDJSE BLSYU IXDSJ JAEVF KJNQF

FIFMP EHYQD
```

a. Factor analysisshows common factors of three and six for all repeat intervals. Based, on this, a frequency count for six alphabets is produced, as listed in Figure 9-1. If the period were actually three, the first and fourth, the second and fifth, and the third and sixth frequency counts would be similar. This is clearly not the case, so the period is confirmed as six.

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
0	2	0	0	3	5	0	0	0	10	0	0	0	0	2	4	4	0	4	3	6	0	0	1	0	0

TOTAL LETTERS = 44 IC = 2.638478

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
4	0	2	2	7	1	0	1	2	0	0	1	1	6	2	1	0	4	5	2	1	1	1	0	0	0

TOTAL LETTERS = 44 IC = 1.731501

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
0	1	1	0	6	2	0	1	0	0	0	5	2	2	3	4	2	2	0	3	0	0	1	3	4	1

TOTAL LETTERS = 43 IC = 1.468439

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
0	1	0	3	3	6	3	0	4	2	3	2	0	0	0	1	0	4	1	1	1	3	0	1	0	4

TOTAL LETTERS = 43 IC = 1.439646

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
3	3	0	1	0	7	1	7	1	0	1	0	1	0	2	0	3	1	8	1	0	0	1	1	0	1

TOTAL LETTERS = 43 IC = 2.303433

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
2	0	0	0	1	0	3	1	4	2	5	1	1	3	1	0	1	0	2	4	2	1	0	1	3	5

TOTAL LETTERS = 43 IC = 1.295681

Figure 9-1. Periodic frequencies.

b. The easiest patterns to match are generally those with the highest ICs. The first, second, and fifth alphabets have the highest ICs, and all can be matched fairly easily. In the first, plaintext A equals ciphertext B. In the second, plaintext A equals ciphertext A, and in the fifth, plaintext A equals ciphertext O. Other alphabets can be matched, too, but using these as an example, the partially reconstructed text is shown below.

```
en  y  ir   r ef   c sc   t r  e  u  ov  r  ie   i da   a ta
FNPDM GJRMF FTFFZ IQKTC LGHAS  EOSIM PVLZF LJEWU WTEAH EOZUA

  t i s  r  in  d  ne   s re    t es   m t e  t  wo  t  al  
NBHNJ SXFFT JNRGR KOEXP GZSEY  XHNFS EZAGU EORHZ XOMRH ZBLTF

n pd   m di   e o u  e  at  c   sw   e ns   c ss   l d e  m 
BYQDT DAKEI LKSIP UYKSX BTERQ  QTWPI SAOSF TQKTS QLZVE EYVAE

is  n  en   a in   r or   t i  r  e  to  n  pp   e ta   e pt
JSNFB IFNEI OZJNR RFSPR TEHNJ  ROJSI UOCZB GQPLI STUAE KSSQT

  j i n  w  th  r  or   f rc    p re   e t i  e  ia  r  in  
EFXUJ NFGKO UHLZF HPRYV TUSCP  JDJSE BLSYU IXDSJ JAEVF KJNQF

r em   t pd
FIFMP EHYQD
```

c. The letter combinations produced by the three recovered alphabets are consistent with good plaintext. Expanded plaintext can be recognized in many places. The first word is *ENEMY* for example. Filling in added plaintext is a surer and quicker means of completing the solution at this point than trying to match more alphabets. Here is the complete solution.

```
enemy airbo rnefo rcesc aptur  edbug ovair field indaw natta
FNPDM GJRMF FTFFZ IQKTC LGHAS  EOSIM PVLZF LJEWU WTEAH EOZUA

ckthi smorn ingpd enemy stren  gthes timat edatt wobat talio
NBHNJ SXFFT JNRGR KOEXP GZSEY  XHNFS EZAGU EORHZ XOMRH ZBLTF

nspdi mmedi ateco unter attac  kswer eunsu ccess fulpd enemy
BYQDT DAKEI LKSIP UYKSX BTERQ  QTWPI SAOSF TQKTS QLZVE EYVAE

iscon centr ating armor inthi  rdsec torin appar entat tempt
JSNFB IFNEI OZJNR RFSPR TEHNJ  ROJSI UOCZB GQPLI STUAE KSSQT

tojoi nupwi thair borne force  spdre quest immed iater einfo
EFXUJ NFGKO UHLZF HPRYV TUSCP  JDJSE BLSYU IXDSJ JAEVF KJNQF

rceme ntspd
FIFMP EHYQD
```

p:	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
C1:	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	A
C2:	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
C3:	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
C4:	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
C5:	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
C6:	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F

9-4. Solution by the Generatrix Method

With standard alphabets or any known alphabets, the method of completing the plain component can be used. This method, when applied to periodic systems, is commonly called the generatrix method. The advantage of this method over frequency matching is that it will work even with fairly short cryptograms. Just as with a monoalphabetic system (see paragraph 4-11), the first step is a trial decryption at any alphabet alignment, followed by listing the plain component sequence vertically underneath each letter of the trial decryption. Whenever the plain and cipher sequences are identical and in the same direction, no trial decryption is necessary. The key difference with periodic systems is that the process must be applied to the letters of each alphabet separately. Plaintext will not be immediately obvious when you look at the generated lines of letters from only a single alphabet, so selection must be initially based on letter frequencies and probabilities rather than recognizable text. The process is illustrated with the following cryptogram enciphered with direct standard alphabets.

QNMZC TAAED FASRR TITYI UGPGW QVMAX TRMRM ZHMNZ KFQEI RIOUX

XAAGR UGPG

a. The cryptogram has a period of five, which can be confirmed either through periodic-phi tests or factor analysis of all the repeats, including two letter repeats, which are not underlined.

b. The most obvious step to try is to substitute *STOP* for the four letter repeat. It does not produce plaintext elsewhere, however. More powerful methods of solution are required.

c. The cryptogram can be readily solved by the generatrix method. The first step is to separate the letters produced by each alphabet. The letters from each of the five alphabets are listed separately below. Notice that if you read all the first letters, it produces the first group of the cryptogram. The second letters produce the second group and so on.

QTFTUQTZKRXU NAAIGVRHFIAG MASTPMMMQOAP ZERYGARNEUGG CDRIWXMZIXR

d. No trial decryption is required, because the same sequence is expected for both the plain and cipher components. Therefore, the next step is to complete the plain component sequence for each letter grouping. This is illustrated in Figure 9-2.

QTFTUQTZKRXU		NAAIGVRHFIAG		MASTPMMMQOAP		ZERYGARNEUGG		CIRIWXMZIXR	
296962902836	62	888855876885	84	688966662886	79	098658889655	77	78885360838	64
RUGUVRUALSYV		OBBJHWSIGJBH		NBTUQNNNRPBQ		AFSZHBSOFVHH		DJSJXYNAJYS	
865658687865	78	844175885147	62	849628888642	73	868074886577	74	71813688168	57
SVHVWSVBMTZW		PCCKIXTJHKCI		OCUVROOOSQCR		BGTAICTPGWII		EKTKYZOBKZT	
857558546905	67	677283917278	67	876588888278	83	459887965588	82	92926084209	51
TWIWXTWCNUAX		QDDLJYUKILDJ		PDVWSPPPTRDS		CHUBJDUQHXJJ		FLULZAPCLAU	
958539578683	76	277716628771	61	675586669878	81	776417627311	52	67670867786	68
UXJXYUXDOVBY		REEMKZVLJMEK		QEWXTQQQUSET		DIVCKEVRIYKK		GMVMABQDMBV	
631366378546	58	899620571692	64	295392226899	66	785729588622	69	56568427645	58
VYKYZVYEPWCZ		SFFNLAWMKNFL		RFXYURRRVTFU		EJWDLFWSJZLL		HNWNBCRENCW	
562605696570	57	866878562867	77	863668885966	79	915776581077	63	78584789875	76
WZLZAWZFQXDA		TGGOMBXNLOGM		SGYZVSSSWUGV		FKXEMGXTKAMM		IOXOCDSFODX	
507085062378	51	955864387856	74	856058885655	69	623965392866	65	88387786873	73
XAMABXAGRYEB		UHHPNCYOMPHN		THZAWTTTXVHW		GLYFNHYULBNN		JPYPDETGPEY	
386843858694	72	677687686678	82	970859993575	76	576687667488	78	16667995696	70
YBNBCYBHSZFC		VIIQODZPNQIO		UIABXUUUYWIX		HMZGOIZVMCOO		KQZQEFUHQFZ	
648476478067	67	588287068288	70	688436666583	69	760588056788	68	22029667260	42
ZCOCDZCITAGD		WJJRPEAQORJP		VJBCYVVVZXJY		INAHPJAWNDPP		LRARFGVIRGA	
078770789857	73	511869828816	63	514765550316	48	888761858766	78	78886558858	76
ADPDEÁDJUBHE		XKKSQFBRPSKQ		WKCDZWWWAYKZ		JOBIQKBXOEQQ		MSBSGHWJSHB	
876798716479	79	322826486822	53	527705558620	52	184822438922	53	68485751874	63
BEQEFBEKVCIF		YLLTRGCSQTLR		XLDEAXXXBZLA		KPCJRLCYPFRR		NTCTHIXKTIC	
492964925786	71	677985782978	83	377983334078	62	267187766688	72	89797832987	77
CFRFGCFLWDJG		ZMMUSHDTRUMS		YMEFBYYYCAMB		LQDKSMDZQGSS		OUDUIJYLUJD	
768657675715	70	066687798668	77	669646667864	74	727286702588	62	86768167617	63
DGSGHDGMXEKH		ANNVTIEUSVNT		ZNFGCZZZDBNC		MRELTNEARHTT		PVEVJKZMVKE	
758577563927	71	888598968589	91	086570007487	52	689798988799	97	65951206529	50
EHTHIEHNYFLI		BOOWUJFVTWOU		AOGHDAAAECOD		NSFMUOFBSIUU		QWFWKLANWLF	
979789786678	91	488561659586	71	885778889787	90	886668648866	80	25652788576	61
FIUIJFIOZGMJ		CPPXVKGWUXPV		BPHIEBBBFDPE		OTGNVPGCTJVV		RXGXLMBOXMG	
686816880561	63	766352556365	59	467894446769	74	895856579155	73	83537648365	58
GJVJKGJPAHNK		DQQYWLHXVYQW		CQIJFCCCGEQF		PUHOWQHDUKWW		SYHYMNCPYNH	
515125168782	51	722657735625	57	728167775926	67	667852776255	66	86766876687	75
HKWKLHKQBIOL		ERRZXMIYWZRX		DRJKGDDDHFRG		QVIPXRIEVLXX		TZIZNODQZOI	
725277224887	61	988036865083	64	781257777685	70	258638895733	67	90808872088	58
ILXLMILRCJPM		FSSAYNJZXASY		ESKLHEEEIGSH		RWJQYSJFWMYY		UAJAOPERAPJ	
873768787166	74	688868102886	70	982779998587	88	851268165666	60	68188698861	69
JMYMNJMSDKQN		GTTBZOKAYBTZ		FTLMIFFFJHTI		SXKRZTKGXNZZ		VBKBPQFSBQK	
166681687228	61	599408286490	64	697686661798	79	832809253800	48	54246268422	45
KNZNOKNTELRO		HUUCAPLBZCUA		GUMNJGGGKIUJ		TYLSAULHYOAA		WCLCQRGTCRL	
280882899788	77	766786740768	72	566815552861	58	967886776888	88	57772859787	72
LOAOPLOUFMSP		IVVDBQMCADVB		HVNOKHHHLJVK		UZMTBVMIZPBB		XDMDRSHUDSM	
788867866686	84	855742678754	68	758827777152	66	606945680644	58	37678876786	73
MPBPQMPVGNTQ		JWWECRNDBEWC		IWOPLIIIMKWL		VANUCWNJAQCC		YENESTIVETN	
664626655892	65	155978874957	75	858678886257	78	588675818277	72	69898985998	88
NQCQRNQWHOUR		KXXFDSOECFXD		JXPQMJJJNLXM		WBOVDXOKBRDD		ZFOFTUJWFUO	
827288257868	71	233678897637	69	136261118736	45	548573824877	68	06869615668	61
ORDRSORXIPVS		LYYGETPFDGYE		KYQRNKKKOMYN		XCPWEYPLCSEE		AGPGUVKXGVP	
887888838658	85	766599667569	81	262882228668	60	376596677899	82	85656523556	56
PSESTPSYJQWT		MZZHFUQGEHZF		LZRSOLLLPNZO		YDQXFZQMDTFF		BHQHVWLYHWQ	
689896861259	77	600766259706	54	708887776808	74	672360267966	60	47275576752	57

Figure 9-2. Generatrix method.

e. To aid in selection of the most likely generated letter sequences, numeric probability data has been added to each line of the listing. The numbers listed below each letter are assigned on the basis of logarithmic weights of the letter probabilities. To the right of each group of logarithmic weights is the sum of the weights for that group. Using this kind of weighting lets us determine the relative probabilities of each line by adding the weights for each letter. The weights in Figure 9-2 have been added according to the log weights shown in Table 9-1.

Table 9-1. Logarithmic weights of letter probabilities.

Letter:	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
Log weight:	8	4	7	7	9	6	5	7	8	1	2	7	6	8	8	6	2	8	8	9	6	5	5	3	6	0

f. The listing in Figure 9-2 was computer generated. When this work must be done manually, it is easier to generate the sequences without the probability data. Then scan the generated rows for each alphabet to visually select those with the most high frequency letters. Finally, if necessary, the probability data can be added only for the selected rows.

g. Only rarely will the correct rows consist entirely of those with the highest totals. Normally, you will have to try different combinations of the high probability rows until you find the correct match. The best place to start is with those rows that stand out the most from others in the same alphabet groups. In the illustrated problem shown below, alphabets four and five provide the most likely starting point. In each case, the sum of the log weights for one row are well above any others. These are listed below, superimposed above each other with room for the other three alphabets to be added.

1:
2:
3:
4: MRELTNEARHTT 97
5: YENESTIVETN 88

h. As the rows are superimposed, the plaintext will appear vertically. The next step is to see which high probability rows from other alphabets will fit well with the starting pair. Trying both of the two highest probability rows for alphabet three produces the next two possibilities.

1:				
2:				
3:	AOGHDAAAECOD	90	ESKLHEEEIGSH	88
4:	MRELTNEARHTT	97	MRELTNEARHTT	97
5:	YENESTIVETN	88	YENESTIVETN	88

i. Reading the plaintext vertically, the grouping on the right is better than the one on the left. The DTS sequence in the left grouping is unlikely, and all the letter combinations on the right are acceptable. Furthermore, the EMY combination at the beginning of the right grouping suggests *ENEMY.* The letter sequences for the first two alphabets which begin with E and N respectively are both high probability sequences. The complete solution is shown below.

1:	EHTHIEHNYFLI	91
2:	NAAIGVRHFIAG	84
3:	ESKLHEEEIGSH	88
4:	MRELTNEARHTT	97
5:	YENESTIVETN	88

"ENEMY HAS RETAKEN HILL EIGHT SEVEN THREE IN HEAVY FIREFIGHT LAST NIGHT"

Section II

Systems Using Mixed Alphabets With Known Sequences

9-5. Approaches to Solution

When mixed sequences are used in periodic systems, a variety of different techniques can be used to solve them. When the plain and cipher sequences are known, the same techniques used with standard alphabets can be used, adapted to the known sequences. When one or both of the sequences are unknown, new techniques must be used. Each situation is a little different. The major paragraphs of this section deal with each situation: both sequences are known, the ciphertext sequence is known, or the plaintext sequence is known. Techniques for solving periodics when neither sequence is known are covered in the next section.

9-6. Solving Periodics With Known Mixed Sequences

Exactly the same techniques that were used with standard alphabets can be used with any known mixed sequences.

a. Successful assumption of plaintext allows you to directly reconstruct the cipher alphabets, as before.

b. The generatrix method works, making sure that a trial decryption is first performed with the sequences set at any alignment. All possible letter combinations are then generated by completing the plain component sequence, as before. The key points to remember are to perform the trial decryption and to use the plain component as the generatrix sequence, not a standard sequence.

c. Frequency matching also works, but there are some differences in its application. Frequency counts must be arranged in the cipher sequence order, not in standard order. The pattern that the frequency counts are matched to must be adjusted to the order of the known plain component. Rearrange the patterns of peaks and troughs to fit the plain component. For example, shown below is the pattern for a standard plain sequence and the pattern that results if a keyword mixed sequence based on POLYALPHABETIC is used as the plain component.

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
7	1	3	4	13	4	2	3	7	-	-	4	3	8	8	3	-	8	6	9	3	1	2	-	2	-

P	O	L	Y	A	H	B	E	T	I	C	D	F	G	J	K	M	N	Q	R	S	U	V	W	X	Z
3	8	4	2	7	3	1	13	9	7	3	4	4	2	-	-	3	8	-	8	6	3	1	2	-	-

The new pattern resulting from the mixed plaintext sequence is just as easy to match frequency counts to as the more familiar standard pattern. If it should prove difficult to match by eye alone, there is also a statistical test, called the chi test, which can be used to aid the matching process. Paragraph 9-7 demonstrates the use of the chi test.

9-7. Solving Periodics With Known Cipher Sequences

The technique of frequency matching can be used any time the cipher sequence is known, whether or not the plain sequence is also known. When the plain sequence is known, the frequency patterns of the cipher sequences are best matched to the expected plain pattern as explained in paragraph 9-6. When the plain sequence is unknown, the frequency patterns of the cipher sequences can be matched to each other. In either case, the key is that the known cipher sequence allows the frequency count to be arranged in the order of the original cipher sequence. The following problem demonstrates frequency matching with a known cipher component sequence. The cipher component sequence in the problem in Figure 9-3 is a keyword mixed sequence based on NORWAY.

```
MZTNK XLBTQ JVMQF WQTIX JJBTF  OCMEF HMHBM KTDPO IZYGR NJDHF
IEKAD AAPID NRBUF IYMET HDOPL  WLOID AQYEF KCWDF TPFAH MAUBR
HCWYQ JJMVR SLSBD HTTPO FDMQF  JLLNQ FEOIH QQYUQ KCLPO GLBQX
JJHBL WLQVF JDKNI JMTHF TCOVZ  ORHAD KCWDF XZWXF IPWCO XHWZP
KEOUF IJTPZ FAUUP HCYRF MDMTE  TRKDF MRWCO HMCNH TVGUL KRK
```

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

TOTAL LETTERS = 50 IC = 1.804082

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

TOTAL LETTERS = 50 IC = 1.697959

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

TOTAL LETTERS = 50 IC = 1.697959

N	O	R	W	A	Y	B	C	D	E	F	G	H	I	J	K	L	M	P	Q	S	T	U	V	X	Z
4	0	1	0	3	1	4	2	3	3	0	1	2	4	0	0	0	0	5	3	0	3	5	3	1	1

TOTAL LETTERS = 49 IC = 1.282313

N	O	R	W	A	Y	B	C	D	E	F	G	H	I	J	K	L	M	P	Q	S	T	U	V	X	Z
0	5	3	0	0	0	0	0	5	1	15	0	3	1	0	1	3	1	2	4	0	1	0	0	2	2

TOTAL LETTERS = 49 IC = 3.161565

Figure 9-3. Known cipher components.

a. Examination of the frequency patterns in Figure 9-3 shows that they do not match the usual standard sequence-pattern. This means that the plain component sequence was not a standard sequence.

b. If the cipher sequences can be correctly matched against each other, the cryptogram can then be reduced to monoalphabetic terms and solved easily.

c. Figure 9-4 is a portion of a computer listing that matches the frequency count of the cipher letters of the first alphabet with the frequency count of second alphabet letters at every possible alignment. The alignments are evaluated by the chi test. In the chi test, each pair of frequencies for an alignment is multiplied. The products of all the pairs are totaled to produce the chi value for that alignment. Figure 9-5 shows the computation carried out for the first alignment. The chi test is also called the cross-product test.

MATCHING ALPHABET 1 AND ALPHABET 2

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

MATCH 1 : 70

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

MATCH 2 : 102

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

MATCH 3 : 128

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

MATCH 4 : 90

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

MATCH 5 : 172

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

MATCH 6 : 78

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

MATCH 7 : 103

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

MATCH 8 : 88

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

MATCH 9 : 64

Figure 9-4. Chi test computer extract.

N	O	R	W	A	Y	B	C	D	E	F	G	H	I	J	K	L	M	P	Q	S	T	U	V	X	Z
2	2	0	3	2	0	0	0	0	0	3	1	6	5	7	6	0	4	0	1	1	4	0	0	3	0
N	O	R	W	A	Y	B	C	D	E	F	G	H	I	J	K	L	M	P	Q	S	T	U	V	X	Z
0	0	5	0	3	1	0	7	4	3	0	0	1	0	5	0	6	3	2	3	0	2	0	2	0	3
0	+0	+0	+0	+6	+0	+0	+0	+0	+0	+0	+0	+6	+0	+35	+0	+0	+12	+0	+3	+0	+8	+0	+0	+0	+0

Figure 9-5. Computation of chi value.

d. Figure 9-6 shows the highest chi values for each match of the first alphabet with the other four alphabets. For all matches except the fourth alphabet, the chi values were clearly the highest. Two matches are shown for the fourth alphabet, because the difference between the two values is not significant. Either match could be the correct one.

MATCHING ALPHABET 1 AND ALPHABET 2

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

MATCH 5 : 172

MATCHING ALPHABET 1 AND ALPHABET 3

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

MATCH 18 : 170

MATCHING ALPHABET 1 AND ALPHABET 4

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

MATCH 10 : 134

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

MATCH 19 : 132

MATCHING ALPHABET 1 AND ALPHABET 5

N	O	R	W	A	Y	B	C	D	E	F	G	H	I	J	K	L	M	P	Q	S	T	U	V	X	Z
2	2	0	3	2	0	0	0	0	0	3	1	6	5	7	6	0	4	0	1	1	4	0	0	3	0
X	Z	N	O	R	W	A	Y	B	C	D	E	F	G	H	I	J	K	L	M	P	Q	S	T	U	V
2	2	0	5	3	0	0	0	0	0	5	1	15	0	3	1	0	1	3	1	2	4	0	1	0	0

MATCH 25 : 185

Figure 9-6. Best matches.

e. To resolve which of the two matches with the fourth alphabet is correct, the highest chi values for matches between the second and fourth and the third and fourth alphabets have also been determined. These are shown in Figure 9-7.

MATCHING ALPHABET 1 AND ALPHABET 4

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

MATCH 10 : 134

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

MATCH 19 : 132

MATCHING ALPHABET 2 AND ALPHABET 4

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

MATCH 15 : 132

MATCHING ALPHABET 3 AND ALPHABET 4

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

MATCH 2 : 141

Figure 9-7. Matches with the fourth alphabet.

f. The matches of alphabet four with alphabets two and three clarify which of the matches with the first alphabet was correct. This becomes apparent when we set up the other four alphabets.

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

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

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

4:

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

g. The match of N of the first alphabet with P of the fourth alphabetic correct. The second alphabet and third alphabet matches confirm this.

h. The next step in the solution is to reduce the cryptogram to monoalphabetic terms using the matches just determined. An A through Z sequence is arbitrarily used for the plain component, and the message is decrypted just as if it were the original.

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

```
rveir ympdv otabm dpeva okpdm   bdarm mnvot prrad nvote akrum
MZTNK XLBTQ JVMQF WQTIX JJBTF   OCMEF HMHBM KTDPO IZYGR NJDHF

nfymk eabvk aypem nbarx mekas   dmkvk eporm pdmqm votmo rafoe
IEKAD AAPID NRBUF IYMET HDOPL   WLOID AQYEF KCWDF TPFAH MAUBR

mdmnv okafe umdok mread keabm   omziv kfkvo tpoev pdzad lmpba
HCWYQ JJMVR SLSBD HTTPO FDMQF   JLLNQ FEOIH QQYUQ KCLPO GLBQX

okvos dmcfm oeyip oneum vdkfb   byvmk pdmqm yvmgm nompd yimhu
JJHBL WLQVF JDKNI JMTHF TCOVZ   ORHAD KCWDF XZWXF IPWCO XHWZP

pfkem nkeab kafeu mdokm readl   vyyqm rympd mnqio vtues pyy
KEOUF IJTPZ FAUUP HCYRF MDMTE   TRKDF MRWCO HMCNH TVGUL KRK
```

i. Reduced to monoalphabetic terms, many more repeats in the text that were suppressed by the multiple alphabets now appear. The solution is completed the same as any other monoalphabetic system.

9-8. Solving Periodics With Known Plaintext Sequences by Direct Symmetry

When the plaintext sequence is known, but not the ciphertext sequence, a solution technique known as direct symmetry is possible. Direct symmetry depends on the probable word method for the initial entry into the cryptogram. It makes use of the fact that the columns can be reconstructed in their original order as recoveries are made. Consider the next example, which uses a standard plaintext sequence.

```
MBNFQ ZLHQV ERNMS EXWFJ MBUFU   LWZIA LBSMK CFXKN WSNZW TREQA
XWHRN ACTKP EVBZJ PREZB TCZWH   TKTDN LBWAU PRZOQ KFEIW KBSRD
EVRWA MBIHO MBNFQ ZLHQV ERNMB   IVZIN MVCHR MXXRD EXDFU NLWGV
ITUCG JBUFW ALWML KFSLL IFQRX   YVIHE JKAHO
```

a. The period is five. The 14 letter repeat is probably *RECONNAISSANCE.*

```
recon naiss ance  a   o   re o                e e              c     n s
MBNFQ ZLHQV ERNMS EXWFJ MBUFU  LWZIA LBSMK CFXKN WSNZW TREQA

  i           a         n                   e          n             e
XWHRN ACTKP EVBZJ PREZB TCZWH  TKTDN LBWAU PRZOQ KFEIW KBSRD

a      re    recon naiss ance                r       r       a   o    a
EVRWA MBIHO MBNFQ ZLHQV ERNMB  IVZIN MVCHR MXXRD EXDFU NLWGV

        e o   a e
ITUCG JBUFW ALWML KFSLL IFQRX  YVIHE JKAHO
```

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
E													Z				M								
L				B									R												
		N						H																	
				M										F				Q							
													Q					V							

b. With recovered letters filled in, we can see that the beginning phrase is the stereotype, *RECONNAISSANCE PATROL REPORTS.*

```
recon naiss ancep atrol repor  ts    te e              c     n s
MBNFQ ZLHQV ERNMS EXWFJ MBUFU  LWZIA LBSMK CFXKN WSNZW TREQA

 si          a   l  n                    ter r  n  n          e
XWHRN ACTKP EVBZJ PREZB TCZWH  TKTDN LBWAU PRZOQ KFEIW KBSRD

a      re    recon naiss ance                r      rt    at or  ar s
EVRWA MBIHO MBNFQ ZLHQV ERNMB  IVZIN MVCHR MXXRD EXDFU NLWGV

  p    epo   are
ITUCG JBUFW ALWML KFSLL IFQRX  YVIHE JKAHO
```

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
E													Z				M		L						
L				B									R					W	X						
		N						H							U		W								
				M										F				Q							
											J		Q		S		U	V							

c. With a known plain component, the columns are in their original order. This means that the partially reconstructed cipher sequences are also in the right order. Each cipher sequence is the same sequence, and whatever one row reveals about the spacing of letters can be transferred to other rows as well. For example, in the second row, X follows immediately after W. X can then be placed after W in row three. Similarly, all common letters can be placed by carefully counting the intervals and placing the same letters at the same intervals in each row. Here is what the matrix looks like after all such values are placed.

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
E	F	H	J		Q	R	S		U	V	W	X	Z				M		L			N	B		
L			N	B			E	F	H	J		Q	R	S		U	V	W	X	Z				M	
		N	B			E	F	H	J		Q	R	S		U	V	W	X	Z				M		L
Z				M		L			N	B			E	F	H	J		Q	R	S		U	V	W	X
	L			N	B			E	F	H	J		Q	R	S		U	V	W	X	Z				M

d. Filling all the new values into the text reveals many more possibilities. Completion of the solution is routine from this point.

```
recon naiss ancep atrol repor   tst   tene    is e locat   ngs
MBNFQ ZLHQV ERNMS EXWFJ MBUFU   LWZIA LBSMK CFXKN WSNZW TREQA

msite       ardal  ngaf   tyk       e ter r  nt n  ig t  ent
XWHRN ACTKP EVBZJ PREZB TCZWH   TKTDN LBWAU PRZOQ KFEIW KBSRD

army   re p recon naiss ancef    rt e rr po rtst  at or war s
EVRWA MBIHO MBNFQ ZLHQV ERNMB   IVZIN MVCHR MXXRD EXDFU NLWGV

  p   depot  areb  ingb  iltu    r pi  d  p
ITUCG JBUFW ALWML KFSLL IFQRX   YVIHE JKAHO
```

e. The direct symmetry technique can also be used as an alternate method when the cipher sequence is the known sequence. The matrix can be inverted, placing the cipher sequence on the top of the matrix and the plaintext equivalents inside in separate rows for each alphabet. Each row will be the plaintext sequence in the correct order. Horizontal intervals recovered in one row can then be duplicated in each sequence just as was demonstrated above for cipher sequence recovery. Unlike the technique of frequency matching, it depends on successful plaintext assumptions, however. It is not as powerful a method of solution, but if plaintext can be readily identified, it may be the quickest way to solve a cryptogram.

Section III

Solving Periodics With Unknown Sequences

9-9. Solving Periodics by Indirect Symmetry

When neither the plaintext nor the ciphertext sequence is known, the matrix cannot be initially recovered with sequences in the correct order. Frequency matching cannot be used, either. However, some of the interval relationships are preserved even when the columns are not placed in the correct order, and these interval relationships can be exploited to aid in matrix recovery.

a. To illustrate how interval relationships are preserved, consider the following two matrices. The first is the matrix in its original form. The second is the same matrix, rearranged with the plain component in A through Z order. This is the form in which you will normally recover a matrix with unknown sequences until enough is known to rearrange the columns in the correct order.

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

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

b. The key principle to understand when working with ananalyst's matrix, like the second one above, is that every pair of columns and every pair of rows represents an interval in the original matrix. To illustrate this, look at the plaintext A column and the plaintext G column in the bottom matrix. The letters D and R appear in the first cipher sequence. If you count the distance between the D and R in the original (top) matrix, you see that the interval is nine. Similarly, the interval for the other pairs in the two columns, R and X, U and P, and M and S, are also nine. For any two columns that you compare, the horizontal interval between the letters in each alphabet will be the same. The interval will not always be nine, of course. It depends on which two columns you are comparing. The point is that between any pairs in the same row in the same two columns, the interval will be the same.

c. Next compare the letters in the first cipher sequence and the second in the bottom matrix. In the first column, the letters D and R appear, which we already noted are nine letters apart horizontally in the original matrix. The letters R and X appear in another column in the first and second sequences, as do U and P, and M and S. The first and second cipher sequences are an interval of nine apart. Whichever pair of letters you look at in the first and second cipher sequences, they are nine apart in the original cipher sequence. Each pair of cipher sequences represents a different interval. For example, the interval between the first and third cipher sequence is eleven. The interval between the first and fourth is seven. The interval between the second and third is two, and so on.

d. There are a number of ways in which we can use an understanding of these interval relationships to help solve a polyalphabetic cryptogram. The use of interval relationships where sequences are unknown and columns are out of order is called indirect symmetry. This contrasts with the earlier situation with known sequences and columns in the correct order, where we used direct symmetry to aid in the solution.

e. To put indirect symmetry to use, consider the following example. Initial recoveries in a polyalphabetic system have produced the following information.

a	b	c	d	e	f	g	h	i	j	...
R	.	.	.	T	.	.	.	M	.	...
M	.	.	.	F	.	.	.	.	.	...
T	.	.	.	.	.	M	.	.	.	...

f. In comparing the plaintext A and E columns, we see that the letters R and T and the letters M and F are the same interval apart. We do not know what the interval is, but we know it is the same in each case.

g. The same interval appears when we compare the first and third cipher sequences, where R and T appear in the first column. Since we know the interval will be the same for any pair of letters between the first and third sequences, and we know M and F have the same interval as R and T, we can add the letter F in the plaintext I column in the third sequence under the letter M.

h. Any time we can establish an interval relationship for two pairs in a rectangular pattern as above, and can find three of the four letters, also in a rectangular pattern elsewhere, we can add the fourth letter to complete the pattern. The pairs must be read in the same direction in each case. Notice that we cannot add F in the plaintext G column in the first sequence. The interval from the first to the third sequence is not the same as the interval from the third to the first.

i. Matching pairs are usually found by reading horizontally in one case, and vertically with one letter in common in the second case, as in the above example. Matching relationships may be found anywhere in matrix, however, and are not restricted to cases with one letter in common. You can find most such matching pairs by examining every column in which you have recovered at least three letters. For each letter in the column, look for a match with letters on the same row that are the same as one of the other letters in the column. When you find such letters, check for every possible complete rectangular relationship, and see if you can find the same relationship with one letter missing elsewhere. Often the addition of one or two letters is all you need to recognize more plaintext in the cryptogram and complete a solution.

j. If you have reason to believe that the plaintext sequence is the same as the cipher sequences, you can use the plaintext sequence in establishing interval relationships, too. All the techniques that apply to the ciphertext sequences apply to the plaintext sequence as well, when it is the same sequence.

9-10. Extended Application of Indirect Symmetry

Indirect symmetry can be used in other ways, too. For example, when enough letters have been recovered, you can list all the pairs of letters between each pair of sequences, and develop partial decimated chains of letters for each, as was explained in paragraph 4-8 with monoalphabetic substitution. These partial chains from different alphabet combinations can then be combined together geometrically to recover the original sequence. This technique is illustrated in the following indirect symmetry problem.

```
refer encey ourme ssage numbe  reigh teigh tthre esixs top
SMHPT ZZOPH KRION FJTYN WRSFN  SMKYZ JMKYZ JNPVN ZJKRX JOFSB

JMILM JMPPM VEVST JMIZK CTWFN  SMWEY LNBKG KKRET VHMSG ZJIEL

         si xthre eeigh tfour  fours evens top
ZOGSJ RMBZV ANPVN ZMKYZ JCRCT  EOVVX ZWBLX JOFOA TMEXB PUBGA

          o nesev enzer ozero  hours
YBWPG ZYXJA WMNPF ZZJPT KFBVA  IOVVX HOSOM KZBZV AZRIN YUBV
```

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

a. Through recognition of the stereotyped beginnings and the use of many numbers, the text shown has been recovered, and the recovered values filled into the matrix.

More values can be filled into the text, but we will first concentrate on the application of indirect symmetry.

b. To recover additional values through indirect symmetry, examine each column with more than two recovered letters in it. Beginning with the fifth column, take each letter in turn, and scan the same row as the selected letter for letters that are the same as those in the column. The first letter, Z, has no letters in common in its row with the letters M, B, P, and N.

c. For the second letter, M, the common letter Z does appear in its row. Having found a common letter, examine each rectangular relationship that exists between the two columns. We first see that Z and W have the same interval as M and Z. Links with this common letter will not add any more values, however.

d. The next rectangular relationship shows that P and L have the same interval as M and Z. Reading M and Z vertically, we look for P or L on the same rows as the M and Z to complete the relationship. We find neither P in the second row nor L in the first row. If either occurred, we could fill in the other. The letters can be written in a column off to the side for future use.

e. Having observed all relationships from the column with the common letter Z, we look for another column with a common letter on the M row. B and P do not occur except in our added column. The letter N does occur in the second row, however. Examining relationships in the N column, we see that Z and J have the same interval as M and N reading horizontally. With that established, we read M and N vertically and look for Z in the second row or J in the last row. This time we find Z in the second row. We can add J in the last row in the same column with Z to complete the rectangular relationship.

f. Continuing this process, all the letters shown in bold print can be added to the matrix without making any new plaintext recoveries.

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

g. It would be easy at this point to return to plaintext recovery to complete the solution, but another technique can be used to recover the original cipher sequences and rebuild the matrix. This technique involves listing all links that result by matching each cipher sequence with every other cipher sequence. Sequence 1 is matched with sequences 2, 3, 4, and 5, in turn. Then sequence 2 is matched with 3, 4, and 5; sequence 3 is matched with 4 and 5; and sequence 4 is matched with 5. If the plaintext sequence were the same as the ciphertext sequence, it would only have been necessary to match the plaintext with each cipher sequence to get all combinations. When all links have been plotted and combined into partial chains wherever possible, the results are shown below.

```
1-2: ECHKOR TWZM FJN IL AS
1-3: EHOV TZB SIP WM KR FN
1-4: FZP WL KE SV JM OC TI AR
1-5: OSTFX IZN ER WJ KA CV
2-3: CHKORV WZMB FJN LP AS
2-4: AOE NMP SRC FWI JZL
2-5: LZJX CRS MN OA WF
3-4: XFTSO NZIVC BP ML RE JW
3-5: HRA BNX PZF KVS MJ IT
4-5: PN LJ EA VT CS IF ZX
```

h. Each set of partial chains represents a decimation of the original sequence. Sometimes, you will be fortunate at this point to find that one of the partial chains directly represents the original sequence (decimation one). When this happens, the original sequence is the obvious starting point. It does not occur in this example, so the best technique is usually to select a set with one of the longer chains as a starting point and relate all other sequence combinations to it. Notice that the chains produced by sequences 1-2 and by sequences 2-3 are obviously produced by the same interval, since many of the partial chains are identical. They make a good starting point for this problem. Begin by listing each chain fragment on paper, horizontally. Write the separate chains in different rows so they will not run into each other.

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

i. The next step is to relate other chains to the existing plot. By examining the intervals or patterns that letters from other chains have in relation to the starting chains, they can be added by following the same rule. For example, the 1-3 combination can be added by observing that it will fit the starting chains by skipping every other letter. This will also enable linking the fifth fragment, AS, with the fourth. After adding all the 1-3 chains, the plot looks like this example.

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

j. Next, search for another combination that can be added to the plot. The 3-4 combination links by counting backwards every fifth letter, as shown by the V and C of the NZIVC chain. This ties all the chain fragments together into one longer chain. When all combinations are added, each by their own rule, it results in almost complete recovery.

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

k. This technique is known as linear chaining. Sometimes you will be unable to combine the fragments into one long chain. When all intervals are even, you will always end with two separate 13-letter chains, which may be combined by trial and error or by figuring out the structure of the original matrix. A second technique, called geometric chaining, which could have been applied here also, is explained in paragraph 9-11.

l. Continuing, the chain above must be a decimation of the original sequence. Since V, W, and X are spaced consistently nine apart, trying a decimation of 9 produces the next sequence.

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

m. With G missing from alphabetical progression, the sequence is keyword mixed, based on GAMES. We can now return to the polyalphabetic matrix and rearrange the columns using the GAMES sequence on each cipher row.

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

n. The unused letters can be determined by returning to the plaintext and deciphering the rest of the message. The plaintext sequence turns out to be a simple transposition mixed sequence based on OLYMPIC. The repeating key is KOREA.

o. The approach shown to solving this problem is not necessarily the way in which you would solve it in actual practice. It would probably be more effective to return to the plaintext earlier than was done in this example. This approach was selected to show the variety of indirect symmetry techniques that can be used, not necessarily because it would yield the quickest solution.

9-11. Solution of Isologs

Whenever isologs are encountered between periodic messages with different period lengths, it is possible to recover the original cipher sequences without any initial plaintext recovery. The cryptograms can then be reduced to monoalphabetic terms and quickly solved. Two different techniques may be used, depending on whether the same alphabets or different alphabets are used in the isologs.

a. When isologous cryptograms use the same alphabets with different repeating keys, the cipher sequences can be recovered by the indirect symmetry process. Take the following two messages, for example.

Message 1:

```
AOPDY JBFKW ATILB XCTKZ KIKVN  SHUAJ COWLA PDBRU KRXAT WALBZ
ZVYZZ YRNCI FPPOJ OBYJQ SESQK  SPGUK XIKVW AVUCW MYTXY ZCYZB
PHBJE SCWXC TKZKV PKN
                          (period 3)
```

Message 2:

```
DCFHC SBOHH BOENY GMGKB HQOQF  FIXHS CVURB KKWUX UEXEQ HBFHP
SYCCZ NZSFZ MDFST WBNFB VNXEB  VYDUS VQOQR TMXMI MNQJR VJOSE
YQBQC CFSAX KODTV WHS
                          (period 4)
```

(1) To solve the isologs, the two messages are first superimposed with the alphabets numbered for each.

```
1: AOPDY JBFKW ATILB XCTKZ KIKVN   SHUAJ COWLA PDBRU KRXAT WALBZ
   12312 31231 23123 12312 31231   23123 12312 31231 23123 12312
2: DCFHC SBOHH BOENY GMGKB HQOQF   FIXHS CVURB KKWUX UEXEQ HBFHP
   12341 23412 34123 41234 12341   23412 34123 41234 12341 23412

1: ZVYZZ YRNCI FPPOJ OBYJQ SESQK   SPGUK XIKVW AVUCW MYTXY ZCYZB
   31231 23123 12312 31231 23123   12312 31231 23123 12312 31231
2: SYCCZ NZSFZ MDFST WBNFB VNXEB   VYDUS VQOQR TMXMI MNQJR VJOSE
   34123 41234 12341 23412 34123   41234 12341 23412 34123 41234

1: PHBJE SCWXC TKZKV PKN
   23123 12312 31231 231
2: YQBQC CFSAX KODTV WHS
   12341 23412 34123 412
```

(2) With periods of 3 and 4, there are 12 different ways in which the alphabets of the first are matched to the alphabets of the second. These begin with the first alphabet of message 1 matched with the first alphabet of message 2 and continue through alphabet 3 matched with alphabet 4. After these 12 matches, the cycle of matches starts over again. For other periods, the number of different alphabet matches is the least common multiple of the two period lengths. The least common multiple of 6 and 4 is 12. The least common multiple of 6 and 9 is 18. For periods of 8 and 9, 72 different alphabet matches are required.

(3) Analysis continues by plotting the links for each alphabet pair. For example, the first link is A1=D1, the second link is O2=C2, and the third link is P3=F3. The next example shows all links plotted and combined into partial chains.

```
1-1: SXADK IE NFM BH WR CJ
2-2: YOCX LN SF BW ZPD QE AT
3-3: TKBY PF HI RU ZS VM
1-4: KOSVY UXG DH BE
2-1: PYCM AH KU JT ZD
3-2: KTGD OWI JS RE ZC HQ
1-3: BB KK (all links the same)
2-4: FOV ZB AE YN KS JQ PW
3-1: KH WU TQ RZ JF XV EC
1-2: IQB NSC WH LR XJ
2-3: AB KO CF SV YR
3-4: IZVQ TO PK LF EN WS
```

(4) The 1-3 plot shows that the same alphabets were used in both these positions.

(5) The partial chains can be combined into one long chain by a process of geometric chaining. Geometric chaining will often produce results when linear chaining is not effective. Geometric chaining is plotted horizontally and vertically, instead of in one straight line. Relationships between alphabet matches can be discovered more readily with this method.

(6) Geometric chaining begins, as with linear chaining, by selecting one alphabet match to plot horizontally. We can select the 1-1 match for its 5-letter chain as a starting point. Next, select a second alphabet match to intersect it plotted vertically. For our example, we will use the 2-2 match, producing the following initial plot.

		Y				
		O				
		C				
	S	X	A	D	K	

(7) To this initial plot, we add as many other fragments from the 1-1 and 2-2 matches as we can at this time. We can also set up plots separated from these for each one that cannot be linked to it.

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

(8) The next step is to find another alphabet match that can easily be added to the plot. For example, the 1-2 match proceeds in the diagram along a lower left to upper right diagonal, as shown by the NSC and XJ fragments. All the 1-2 fragments can be added by the same diagonal rule. This ties in the separate plots from above, also.

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

(9) Each additional alphabet combination can be added to the plot now. In many cases, you may see different possibilities for rules. For example, the 3-4 match can be seen to proceed by an up 3, left 1 rule, as shown by the TO link. A simpler equivalent is to plot by the upper left to lower right diagonal, as shown by the PK link. The simplest way to describe the 3-3 match is up 1, right 2, as shown by the TK or BY links. This is similar to a knight's move in chess. When all matches are plotted, they produce this diagram.

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

(10) The rows can easily be extended into one 26-letter chain at this point, but if alphabetic progression can be spotted by any other rule, it can be used instead. For example, starting with the V in the upper left part of the diagram, VWXY appears by a descending knight's move. Continuing from the Y that repeats near the left side, the sequence can be extended further. The complete sequence appears below.

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

(11) Using the new recovered sequence and the relationships between the alphabets of messages 1 and 2, the matrices for both messages can be set up. Using the first cipher sequence for message 1, all the cipher sequences for message 2 can be lined up with it using the links already plotted. Here is how the message 2 alphabets line up with alphabet one. The first 1-1, 1-2, 1-3, and 1-4 links from the isologs are shown in bold print to demonstrate how they were lined up.

C1: G R A I N B C D E F H J K L M O P Q S T U V W X Y Z
C2:
C3:

C1: B C D E F H J K L M O P Q S T U V W X Y Z G R A I N
C2: M O P Q S T U V W X Y Z G R A I N B C D E F H J K L
C3: G R A I N B C D E F H J K L M O P Q S T U V W X Y Z
C4: I N B C D E F H J K L M O P Q S T U V W X Y Z G R A

(12) Similarly, the alphabets in the first matrix can be completed by plotting the relationships between the second message and the first. The solution then becomes a matter of reducing them to monoalphabetic terms.

(13) In cases where the two periods have a common factor, the sequences can still be recovered, but they cannot be fully aligned. In this case, the chi test can be used to match the sequences by frequencies, if necessary, once the sequences are known.

b. A different technique must be used if different alphabets are used between the isologs, not just different repeating keys. For example, consider the next two messages.

Message 1:

AUUJB NFMOI AXCQD LHXPE OCPZD XMZAN HUGQV OIAZZ POPAA FOZUY
OQEOX BRDHA MVUUO SFBNW XJXWO XVEZP IPHYM WODOT CMOTU CTUPT
UOYRO SBBMP CMMXA ATYAN (period 3)

Message 2:

ZCIPY RZXLG ZXSNP CNLNH LQDZU FXALR SIGIH MQTCA GTNMQ TCZGG
ZYZTG GORIB NDISF YZGUB KGKEZ IMDJS HLIYN EZKFF XXLOG CYCSG
KTHJL VTINA ORDLW MPDZK (period 4)

(1) The sequences are different in the two messages, and they cannot be directly chained together. If you listed the links resulting from the two messages using the previous technique, they would lead nowhere and contradictions would quickly develop. The cipher sequences of each must be kept separate.

(2) The method of recovering the cipher sequences when they are different is to set up periodic matrices one over the other, as shown below. Message 1 and message 2 equivalents are then plotted in the correct sequence for each in the same columns. Initially, this will result in more than 26 columns, but as incomplete columns are combined with each other, the matrices will collapse to the correct width. This method could be used with more than two isologs also, by superimposing as many matrices as there are isologous messages.

```
1: AUUJB NFMOI AXCQD LHXPE OCPZD  XMZAN HUGQV OIAZZ POPAA FOZUY
   12312 31231 23123 12312 31231  23123 12312 31231 23123 12312
2: ZCIPY RZXLG ZXSNP CNLNH LQDZU  FXALR SIGIH MQTCA GTNMQ TCZGG
   12341 23412 34123 41234 12341  23412 34123 41234 12341 23412

1: OQEOX BRDHA MVUUO SFBNW XJXWO  XVEZP IPHYM WODOT CMOTU CTUPT
   31231 23123 12312 31231 23123  12312 31231 23123 12312 31231
2: ZYZTG GORIB NDISF YZGUB KGKEZ  IMDJS HLIYN EZKFF XXLOG CYCSG
   34123 41234 12341 23412 34123  41234 12341 23412 34123 41234

1: UOYRO SBBMP CMMXA ATYAN
   23123 12312 31231 23123
2: KTHJL VTINA ORDLW MPDZK
   12341 23412 34123 41234
```

Message 1:

1	A			J			F			I			C		
2		U			B			M			A			Q	
3			U			N			O			X			D

Message 2:

1	Z				Y				L				S		
2		C				R				G				N	
3			I				Z				Z				P
4				P				X				X			

(3) The first three groups of each message are plotted above. Each time a previously used letter appears in the same sequence, the two columns can be combined. For example, in message 2, the Zs in the third sequence allow those two columns to be combined, and similarly, the Xs in the fourth sequence can be combined. In the next example, the complete messages are plotted and all possible columns are combined.

Message 1:

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

Message 2:

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

(4) These matrices can easily be completed by direct symmetry, remembering that the sequence in each matrix is different.

Message 1:

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

Message 2:

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

(5) Either cryptogram can now be reduced to monoalphabetic terms and solved, as before.