CHAPTER 10

APERIODIC POLYALPHABETIC CIPHERS

10-1. Simple Manual Aperiodic Systems

Chapter 9 showed that periodic polyalphabetic systems are generally more secure than monoalphabetic systems. However, the regular, repeating nature of the keys in periodic systems are a weakness that an analyst can exploit. Using factor analysis or the phi test, the analyst can readily determine how many alphabets there are and which letters are enciphered by which alphabets. Aperiodic polyalphabetic systems eliminate the regular, repeating use of alphabets so the analyst cannot easily tell which letters are enciphered by which alphabets. There area number of ways to use a limited set of alphabets but suppress their regular repetition. The following subparagraphs show the most common types of these, and briefly discuss their weaknesses and approaches to their solution. They are presented to make you aware of the possibility that such techniques can be used, but no detailed explanation of their solution is given.

a. Word Length Aperiodic. The simplest type of aperiodic changes alphabets with each word instead of each letter. The analyst cannot tell which letters are encrypted by which alphabet until the text is recovered. However, the major weakness of this system is that when repeats occur, they are likely to be word length, and plaintext word patterns show through as clearly as with monoalphabetics. When alphabets are known, the generatrix method makes the plaintext obvious.

b. Numerically Keyed Aperiodic. Another approach, similar to word-length encipherment, is to change alphabets after a number of letters, determined by a numerical key. The numerical key is often based on the repeating key. The key is generated by the same process used with a numerically keyed transposition sequence. The letters in the repeating keyword are numbered alphabetically. Then the key determines how many letters are enciphered consecutively by each alphabet. For example, here is a short message enciphered by a numerically keyed aperiodic based on the keyword BLACK.

	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	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
5	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
1	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	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	B
4	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

2	5	1	3	4	2	5	1	3
en	emyat	t	ack	ingo	na	llfro	n	ts
FO	PXJLE	T	CEM	SXQY	OB	WWQCZ	N	VU

This system, while more complicated than a word-length aperiodic, allows many repeats and patterns to appear. When the alphabets are known, use of the generatrix method also quickly reveals the plaintext.

c. Interruptor Letter Aperiodic. Another approach to breaking up the cyclic nature of periodic systems is through the use of an interruptor letter. In interruptor letter systems, the alphabets are used in rotation like a periodic system, but whenever a preselected plaintext (or alternatively, ciphertext) letter is encountered, the rotation is interrupted and encipherment returns to the first alphabet. This is a more secure method than the previous two, but it can have the effect of creating repeats that would not otherwise occur. For example, if a plaintext R is used as an interruptor letter, every time REINFORCEMENTS appears in the text, encipherment from the second letter on will be identical every time. The letter after the initial R will be enciphered by the first alphabet each time because of the interruption. The same thing will happen with any word that begins with the interruptor letter. Use of a ciphertext interruptor letter instead of a plaintext letter will avoid many of these repeats, but the interruptions will generally occur much less often in such a case.

10-2. Long-Running Key Aperiodic

Much more common than the simple manual aperiodic systems described in the previous paragraph are those that use a long-running, ever changing key. These systems may be enciphered manually, by cipher machine, or by computer, as first discussed in paragraph 8-1. Figure 8-1 gave an example of using a book key where the key letters were a quotation. A quotation, particularly from a book, provides a ready source of long-running keys, but it is relatively unsecure, because the key itself is so orderly. More often, the keys will be random or pseudorandom. The keys are applied to the plaintext using an alphabet chart like the Vigenere square in Figure 8-1. The keys may be generated by a pseudorandom, repeatable process or by a random, nonrepeatable process. Both the sending and receiving cryptographer must have a copy of the same book or pad of keys. When these are intended for single usage of the keys, the system is called a one-time pad system. Truly random one-time pad systems are absolutely unbreakable when used properly. When keys are reused, however, whether by mistake or by design, the messages with the reused keys are likely to be recoverable. Manual one-time pad systems are slow systems to use and present logistics problems for any large scale usage. The volume of keys must be at least equal to the volume of messages to be sent, When more than one communications link shares the use of copies of the same pad, careful procedures must be set up to prevent reuse of the same keys by different users.

10-3. Solution of Long-Running Key Aperiodic

The solution of messages enciphered in long-running key systems may be possible in three situations. First, the key generation process may be known in advance from prior recoveries or other sources. Second, the keys may be so orderly that they are recognizable when partially recovered, as can occur when plaintext is used as the source of keys. Third, the same sequence of keys is reused. We are primarily concerned with the third case, where keys are reused.

a. Depth Recognition. A reuse of long-running keys is called a depth. Messages using the same keys are called messages in depth. If the keys begin at the same point in two or more messages, the messages are in flush depth. If the keys begin at different points in two or more messages, but include reused keys for at least part of the messages, they are in offset depth. The solution of messages in depth first requires you to recognize that the depth exists.

(1) One way to recognize depth is through exploitation of indicator systems. In one-time pad systems and in many types of cipher machine or computer systems, the starting point or settings for the keys must be known by the enciphering and deciphering cryptographers. This information on the keys is often passed from cryptographer to cryptographer through the use of an indicator system. The first way to recognize a depth is to find two messages or transmissions with identical indicators. Identical indicators will often tip-off that a flush depth is occurring.

(2) The second way to recognize depth is to find repeated text between two or more messages. Except for short accidental repeats, repeated ciphertext will only occur when the same plaintext is enciphered with the same keys. In periodic

systems and simple manual aperiodic, this will often occur within a single message as the same keys are reused. With long-running key aperiodic, this will only occur between messages when keys are reused. If all depths are expected to be flush depths, the search for repeats is a matter of superimposing messages and looking for repeats in the same position in each message. If depths are offset, they are more difficult to find by inspection alone.

(3) The third way to recognize depth is to use a type of coincidence test known as the kappa test. Whether whole words and phrases are repeated using the same keys or not, individual characters using the same keys will occur frequently when depths are present. When two messages are matched together, letter by letter, and do not use the same keys, 1 out of 26 letters (or 3.85 percent) will randomly match. Of course, if a different alphabet is used, or if characters other than letters are also used, the expected number of matches by chance alone will be 1 out of the total number of different characters used. On the other hand, if the messages are correctly placed in depth, a letter by letter comparison (the kappa test) will produce matches about 6.67 percent of the time. Also, the results can be expressed as a kappa index of coincidence showing the ratio of observed coincidences to random expectation. As with searching for repeats, it is much easier to find flush depths than it is to find offset depths, but with computer support, messages can be matched in every possible alignment to search for depths.

(4) As an example of depth recognition, consider the three messages that follow. Each has similar indicator groups that suggest the messages may be in depth with each other. Messages 1 and 2 have identical indicators. Message 3 differs only in the last digit of the second group.

Message 1:

```
JJ632 0406 HJJBW KBZGA OWSON  SRJCF AGORU EOGVA CNWIH GLVZX
MDSAF EMFGP VNNNN ABJPZ TJNVL  QMGGN TVBAP MDODN ODMIO NOIWO
XANAC CNLXS EMBWV CVZYD FTPUC  TQNAW ZUTUH JJ632
```

Message 2:

```
JJ632 0406 FWFQA VSAIA UOSOS  SHMQD YGLNO YOOQV GNVSD BOIIG
XDRAF GFEMM GTCZN VMYSN UHCYM  GZBPP BOVYW BLQIO AKEXM NMNTN
SODPA UNBMO QYYQS GOBMA WSUQL  JJ632
```

Message 3:

```
JJ632 0407 KDHYW QOEBJ DBJGH  PYGEP HOQNY OOISH UYMHX MGTUC
EYWTG RLRKQ YKISC QNPTB JFCRA  EKZXA LLCOZ HIKYE UJPKC SHWHN
VWAXF APEVG XJDQS FISYL SQLCY  JAGRP JJ632
```

(5) There are no repeats longer than three letters between any of the three messages. Because of the identical indicators, we first try to match messages 1 and 2 at a flush depth using the kappa test. The number of matches multiplied by 26 and divided by the number of comparisons equals the kappa IC. Do not count the indicator groups in the comparisons.

```
1: JJ632 0406 HJJBW KBZGA OWSON  SRJCF AGORU EOGVA CNWIH GLVZX
2: JJ632 0406 FWFQA VSAIA UOSOS  SHMQD YGLNO YOOQV GNVSD BOIIG

1: MDSAF EMFGP VNNNN ABJPZ TJNVL  QMGGN TVBAP MDODN ODMIO NOIWO
2: XDRAF GFEMM GTCZN VMYSN UHCYM  GZBPP BOVYW BLQIO AKEXM NMNTN

1: XANAC CNLXS EMBWV CVZYD FTPUC  TQNAW ZUTUH JJ632
2: SODPA UNBMO QYYQS GOBMA WSUQL  JJ632
```

2 to 1: offset 0
13 matches out of 115 comparisons
Kappa IC = 2.94

(6) As shown by the kappa test, the number of matches is well above random expectation. The two messages appear to be in flush depth with each other. Next we try message 3 matched with the first two at a flush depth.

```
1: JJ632 0406 HJJBW KBZGA OWSON  SRJCF AGORU EOGVA CNWIH GLVZX
2: JJ632 0406 FWFQA VSAIA UOSOS  SHMQD YGLNO YOOQV GNVSD BOIIG
3: JJ632 0407 KDHYW QOEBJ DBJGH  PYGEP HOQNY OOISH UYMHX MGTUC

1: MDSAF EMFGP VNNNN ABJPZ TJNVL  QMGGN TVBAP MDODN ODMIO NOIWO
2: XDRAF GFEMM GTCZN VMYSN UHCYM  GZBPP BOVYW BLQIO AKEXM NMNTN
3: EYWTG RLRKQ YKISC QNPTB JFCRA  EKZXA LLCOZ HIKYE UJPKC SHWHN

1: XANAC CNLXS EMBWV CVZYD FTPUC  TQNAW ZUTUH JJ632
2: SODPA UNBMO QYYQS GOBMA WSUQL  JJ632
3: VWAXF APEVG XJDQS FISYL SQLCY  JAGRP JJ632
```

3 to 1 and 2: offset 0
9 matches out of 235 comparisons
Kappa IC = 1.00

(7) The flush match of message 3 is clearly not a correct match, because of the low kappa index of coincidence. We next try offsets of 1, 2, 3, 4, and 6 letters to the right.

```
1:  JJ632 0406 HJJBW KBZGA OWSON  SRJCF AGORU EOGVA CNWIH GLVZX
2:  JJ632 0406 FWFQA VSAIA UOSOS  SHMQD YGLNO YOOQV GNVSD BOIIG
3:  JJ632 0407  KDHY WQOEB JDBJG  HPYGE PHOQN YOOIS HUYMH XMGTU

1:  MDSAF EMFGP VNNNN ABJPZ TJNVL  QMGGN TVBAP MDODN ODMIO NOIWO
2:  XDRAF GFEMM GTCZN VMYSN UHCYM  GZBPP BOVYW BLQIO AKEXM NMNTN
3:  CEYWT GRLRK QYKIS CQNPT BJFCR  AEKZX ALLCO ZHIKY EUJPK CSHWH

1:  XANAC CNLXS EMBWV CVZYD FTPUC  TQNAW ZUTUH JJ632
2:  SODPA UNBMO QYYQS GOBMA WSUQL  JJ632
3:  NVWAX FAPEV GXJDQ SFISY LSQLC  YJAGR PJJ63 2
```

3 to 1 and 2: offset 1
13 matches out of 234 comparisons
Kappa IC = 1.44

```
1:  JJ632 0406 HJJBW KBZGA OWSON  SRJCF AGORU EOGVA CNWIH GLVZX
2:  JJ632 0406 FWFQA VSAIA UOSOS  SHMQD YGLNO YOOQV GNVSD BOIIG
3:  JJ632 0407   KDH YWQOE BJDBJ  GHPYG EPHOQ NYOOI SHUYM HXMGT

1:  MDSAF EMFGP VNNNN ABJPZ TJNVL  QMGGN TVBAP MDODN ODMIO NOIWO
2:  XDRAF GFEMM GTCZN VMYSN UHCYM  GZBPP BOVYW BLQIO AKEXM NMNTN
3:  UCEYW TGRLR KQYKI SCQNP TBJFC  RAEKZ XALLC OZHIK YEUJP KCSHW

1:  XANAC CNLXS EMBWV CVZYD FTPUC  TQNAW ZUTUH JJ632
2:  SODPA UNBMO QYYQS GOBMA WSUQL  JJ632
3:  HNVWA XFAPE VGXJD QSFIS YLSQL  CYJAG RPJJ6 32
```

3 to 1 and 2: offset 2
8 matches out of 233 comparisons
Kappa IC = 0.89

```
1: JJ632 0406 HJJBW KBZGA OWSON  SRJCF AGORU EOGVA CNWIH GLVZX
2: JJ632 0406 FWFQA VSAIA UOSOS  SHMQD YGLNO YOOQV GNVSD BOIIG
3: JJ632 0407    KD HYWQO EBJDB  JGHPY GEPHO QNYOO ISHUY MHXMG

1: MDSAF EMFGP VNNNN ABJPZ TJNVL  QMGGN TVBAP MDODN ODMIO NOIWO
2: XDRAF GFEMM GTCZN VMYSN UHCYM  GZBPP BOVYW BLQIO AKEXM NMNTN
3: TUCEY WTGRL RKQYK ISCQN PTBJF  CRAEK ZXALL COZHI KYEUJ PKCSH

1: XANAC CNLXS EMBWV CVZYD FTPUC  TQNAW ZUTUH JJ632
2: SODPA UNBMO QYYQS GOBMA WSUQL  JJ632
3: WHNVW AXFAP EVGXJ DQSFI SYLSQ  LCYJA GRPJJ 632
```

3 to 1 and 2: offset 3
6 matches out of 232 comparisons
Kappa IC = 0.67

```
1: JJ632 0406 HJJBW KBZGA OWSON  SRJCF AGORU EOGVA CNWIH GLVZX
2: JJ632 0406 FWFQA VSAIA UOSOS  SHMQD YGLNO YOOQV GNVSD BOIIG
3: JJ632 0407       K DHYWQ OEBJD  BJGHP YGEPH OQNYO OISHU YMHXM

1: MDSAF EMFGP VNNNN ABJPZ TJNVL  QMGGN TVBAP MDODN ODMIO NOIWO
2: XDRAF GFEMM GTCZN VMYSN UHCYM  GZBPP BOVYW BLQIO AKEXM NMNTN
3: GTUCE YWTGR LRKQY KISCQ NPTBJ  FCRAE KZXAL LCOZH IKYEU JPKCS

1: XANAC CNLXS EMBWV CVZYD FTPUC  TQNAW ZUTUH JJ632
2: SODPA UNBMO QYYQS GOBMA WSUQL  JJ632
3: HWHNV WAXFA PEVGX JDQSF ISYLS  QLCYJ AGRPJ J632
```

3 to 1 and 2: offset 4
9 matches out of 231 comparisons
Kappa IC = 1.01

```
1: JJ632 0406 HJJBW KBZGA OWSON  SRJCF AGORU EOGVA CNWIH GLVZX
2: JJ632 0406 FWFQA VSAIA UOSOS  SHMQD YGLNO YOOQV GNVSD BOIIG
3: JJ632 0407       KDHYW QOEBJ  DBJGH PYGEP HOQNY OOISH UYMHX

1: MDSAF EMFGP VNNNN ABJPZ TJNVL  QMGGN TVBAP MDODN ODMIO NOIWO
2: XDRAF GFEMM GTCZN VMYSN UHCYM  GZBPP BOVYW BLQIO AKEXM NMNTN
3: MGTUC EYWTG RLRKQ YKISC QNPTB  JFCRA EKZXA LLCOZ HIKYE UJPKC

1: XANAC CNLXS EMBWV CVZYD FTPUC  TQNAW ZUTUH JJ632
2: SODPA UNBMO QYYQS GOBMA WSUQL  JJ632
3: SHWHN VWAXF APEVG XJDQS FISYL  SQLCY JAGRP JJ632
```

3 to 1 and 2: offset 5
17 matches out of 230 comparisons
Kappa IC = 1.92

(8) The offset of five is clearly the best match of those tried, and the kappa index of coincidence is a good value for a correct match. The three messages are now correctly placed in depth.

b. Depth Reading. When the messages are superimposed properly, they can be solved by a process known as depth reading. With only a few messages, the process of applying the key must be known. With manual systems, standard alphabets are commonly used. With cipher machine or computer based systems, the process of baud addition is usually known or can be figured out easily. The three messages in our example use the standard alphabet Vigenere square of Figure 10-1.

Plaintext

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

Figure 10-1. Vigenere square.

(1) With three messages in depth, almost any correct assumption of plaintext will lead to a quick solution. For example, trying the word *REPLACEMENT* as the first word of message 3 produces the results shown below.

```
                          rchte amarr  i
1: JJ632 0406 HJJBW KBZGA OWSON  SRJCF AGORU EOGVA CNWIH GLVZX

                          ctive gearw  i
2: JJ632 0406 FWFQA VSAIA UOSOS  SHMQD YGLNO YOOQV GNVSD BOIIG

                          repla cemen  t
3: JJ632 0407             KDHYW QOEBJ  DBJGH PYGEP HOQNY OOISH UYMHX

Key:                      TZSNW OKSXW  K

1: MDSAF EMFGP VNNNN ABJPZ TJNVL  QMGGN TVBAP MDODN ODMIO NOIWO
2: XDRAF GFEMM GTCZN VMYSN UHCYM  GZBPP BOVYW BLQIO AKEXM NMNTN
3: MGTUC EYWTG RLRKQ YKISC QNPTB  JFCRA EKZXA LLCOZ HIKYE UJPKC

1: XANAC CNLXS EMBWV CVZYD FTPUC  TQNAW ZUTUH JJ632
2: SODPA UNBMO QYYQS GOBMA WSUQL  JJ632
3: SHWHN VWAXF APEVG XJDQS FISYL  SQLCY JAGRP JJ632
```

(2) Recovering the key from the assumption of *REPLACEMENT* and using it to decipher the other two messages produces good segments of plaintext in each message. It is easy to build on these assumptions to recover additional plaintext. For example, assuming that the second message begins *PROTECTIVE GEAR* and that the word after *TEAM* in the first message is *ARRIVING* leads to additional recoveries.

```
                    resea rchte amarr  iving
1: JJ632 0406 HJJBW KBZGA OWSON  SRJCF AGORU EOGVA CNWIH GLVZX

                    prote ctive gearw  illbe
2: JJ632 0406 FWFQA VSAIA UOSOS  SHMQD YGLNO YOOQV GNVSD BOIIG

                          repla cemen  tfiri
3: JJ632 0407             KDHYW QOEBJ  DBJGH PYGEP HOQNY OOISH UYMHX

Key:                QFRXW TZSNW OKSXW  KWBPZ

1: MDSAF EMFGP VNNNN ABJPZ TJNVL  QMGGN TVBAP MDODN ODMIO NOIWO
2: XDRAF GFEMM GTCZN VMYSN UHCYM  GZBPP BOVYW BLQIO AKEXM NMNTN
3: MGTUC EYWTG RLRKQ YKISC QNPTB  JFCRA EKZXA LLCOZ HIKYE UJPKC

1: XANAC CNLXS EMBWV CVZYD FTPUC  TQNAW ZUTUH JJ632
2: SODPA UNBMO QYYQS GOBMA WSUQL  JJ632
3: SHWHN VWAXF APEVG XJDQS FISYL  SQLCY JAGRP JJ632
```

(3) This process of assuming text can be continued to a complete solution. Correct assumptions are easily verified. Incorrect assumptions are quickly disproved.

(4) The most difficult step is making the first correct assumption. Message beginnings are the most likely area to yield results, because they are likely to be very stereotyped. Sometimes, just trying the letters RE at the beginning of a message will be enough to suggest the text of the messages in depth with it. When message beginnings do not yield results, more powerful techniques are available.

c. Crib Dragging. When you cannot assume the beginning of a message, you can still often correctly assume a particular word that will be in a message. The assumptions can come from familiarity with previous messages, results of traffic analysis and direction finding, or other intelligence sources. Once you suspect a word is in one of two or more messages in depth, you can systematically try the word at every position, recover the keys each position would produce, and try the keys in the other message or messages to see if the keys produce more plaintext. This is a laborious process performed manually, but a sure one. Fortunately, there are some short cuts that can be used to simplify the process.

(1) Two messages in depth can generally be combined in such a way that you can skip the step of key recovery and proceed directly to checking for plaintext. With the Vigenere square of Figure 10-1, this can be accomplished by treating one message as if it were plaintext, the other as ciphertext, and producing the resulting key stream, which is actually a combination of the two ciphertexts. To demonstrate this process, consider the beginnings of messages 1 and 2 from the previous example. If we combine message 1 and message 2 as if they were plaintext and ciphertext respectively, it produces a combination text for the first groups of YNWPE, Message 1 letters are used as keys in the Vigenere square. Message 2 letters represent the internals of the Vigenere square. For example, key H matched against internal F produces plaintext Y.

Message 1:	H	J	J	B	W	...
Message 2:	F	W	F	Q	A	...
Combination:	Y	N	W	P	E	...

(2) If we now apply the correct plaintext of message 1 to the combination text using the Vigenere square, it will directly produce the plaintext of message 2. The

combination text is again found in the key letter position in the square, and the plaintext is found in the same position for each message as the original ciphertexts.

```
     Message 1:  H J J B W ...
     Message 2:  F W F Q A ...
   Combination:  Y N W P E ...
     Message 1:  r e s e a ...
     Message 2:  p r o t e ...
```

(3) The combination text can be systematically used to try out a plaintext assumption in every position by a process known as crib dragging. *Crib* is a common synonym for *assumption* in cryptanalysts. Consider the following two messages in depth. The first message was sent by a unit undergoing an artillery barrage. It is likely that the word *ARTILLERY* will be found in the message.

```
Message 1: IOZHN EJBTK AKRZE STXVZ GCAVH  FJRVX DQNUT
Message 2: UKMWR SDCXM HVOUS OFHUD PICDV  BKUPC OEWKK
```

(4) The first step to trying out *ARTILLERY* in message 1 is to create the combination text. Message 1 is treated as plaintext and message 2 as ciphertext.

```
  Message 1: IOZHN EJBTK AKRZE STXVZ GCAVH  FJRVX DQNUT
  Message 2: UKMWR SDCXM HVOUS OFHUD PICDV  BKUPC OEWKK
Combination: MWNPE OUBEC HLXVO WMKZE JGCIO  WBDUF LOJQR
```

(5) The results of trying *ARTILLERY* in each of the first three positions are shown below.

```
  Message 1: IOZHN EJBTK AKRZE STXVZ GCAVH  FJRVX DQNUT
  Message 2: UKMWR SDCXM HVOUS OFHUD PICDV  BKUPC OEWKK
Combination: MWNPE OUBEC HLXVO WMKZE JGCIO  WBDUF LOJQR
         1:  artil lery
         2:  mngxp zysc

Combination: MWNPE OUBEC HLXVO WMKZE JGCIO  WBDUF LOJQR
         1:   arti llery
         2:   weim zffva

Combination: MWNPE OUBEC HLXVO WMKZE JGCIO  WBDUF LOJQR
         1:    art iller y
         2:    ngx wfmit f
```

(6) Obviously, not one of the first three tries is the correct placement of *ARTILLERY.* The process can be speeded up, however, by plotting the crib vertically and the resulting text for message 2 on a descending diagonal.

```
     Message 1:   IOZHN EJBTK AKRZE STXVZ GCAVH  FJRVX DQNUT
     Message 2:   UKMWR SDCXM HVOUS OFHUD PICDV  BKUPC OEWKK
   Combination:   MWNPE OUBEC HLXVO WMKZE JGCIO  WBDUF LOJQR
         Crib:  a mwn
                r  neg
                t   gix
                i    xm w
                l     p zf
                l       zfm
                e        yfi
                r         svt
                y          ca  f
```

(7) The plot above is identical in results to the three separate plots that preceded. Once this format is adopted, it is easier to write in a whole row at a time.

```
     Message 1:   IOZHN EJBTK AKRZE STXVZ GCAVH  FJRVX DQNUT
     Message 2:   UKMWR SDCXM HVOUS OFHUD PICDV  BKUPC OEWKK
   Combination:   MWNPE OUBEC HLXVO WMKZE JGCIO  WBDUF LOJQR
         Crib:  a mwnpe oubec hlxvo wmkze jgcio  wb
                r  negv flsvt ycomf ndbqv axtzf  nsu
                t   gix hnuxv aeqoh pfdsx czvbh  puwn
                i    xm wcjmk ptfdw eushm rokqw  ejlcn
                l     p zfmpn swigz hxvkp urntz  hmofq  w
                l       zfmpn swigz hxvkp urntz  hmofq  wz
                e        yfig lpbzs aqodi nkgms  afhyj  psn
                r         svt ycomf ndbqv axtzf  nsulw  cfag
                y          ca fjvtm ukixc heagm  uzbsd  jmhop
```

(8) The plaintext for message 2 appears on the sixth diagonal, as highlighted above. Once the text is spotted and the crib confirmed, it becomes a matter of depth reading, as before. The worksheet can now be set up and the rest of the text recovered.

```
                  artil lery
Message 1:  IOZHN EJBTK AKRZE STXVZ GCAVH  FJRVX DQNUT

                  olumn spot
Message 2:  UKMWR SDCXM HVOUS OFHUD PICDV  BKUPC OEWKK

Key:              ESILZ PGAB
```

(9) With cipher machine and computer based systems that use baud addition, adding two messages in depth together by baud addition eliminates the key. The baud addition of the two ciphertexts is identical to the baud addition of the two original plaintexts.

(10) Whatever type of alphabet square or system of combining bauds is used, there is usually a way to combine texts in depth to eliminate the effects of the key. If you are unsure how to approach a particular type of system, test samples you create for yourself in the system to see how ciphertext can be combined to eliminate the effect of the key.