Chapter 9

The Cipher Exchange and Cipher Guidelines

The Cipher Exchange (**CE**) is that department of *The Cryptogram* that deals with ciphers which are **NOT** simple substitutions of the Aristocrat/Patristocrat variety. Here you will find the fruits of several hundred years of development of cryptography, as cryptanalysts discovered new ways to attack a cipher, and the encipherers then complicated the ciphers to compensate. Some of the ACA systems were used historically in precisely the form we use; some are simplified to highlight unique aspects of that cipher type; and some were invented by ACA members.

CE ciphers given in *The Cryptogram* are all solvable by pencil and paper methods, although computers and other mechanical aids are often used to assist. The ciphers are printed in approximate order of difficulty (as determined by experience) in *The Cryptogram*. They are listed in alphabetical order below, together with the length recommended for a suitable plaintext.

AMSCO (period times 8-12 lines deep)

The first entry may be either a digraph or a single letter. In both even and odd periods the first column and the first row always alternate.

Solvers should be aware that a null is not required when the end of the text does not fill out the digraph-single letter or single letter-digraph pattern.

Key: 41325
pt: Incomplete columnar with alternating single letters and digraphs.

4	1	3	2	5
in	c	om	p	le
t	ec	o	lu	m
na	r	wi	t	ha
l	te	r	na	t
in	g	si	n	gl
e	le	t	te	r
sa	n	dd	i	gr
a	ph	s		

CT:
CECRT EGLEN PHPLU TNANT EIOMO WIRSI TDDSI NTNAL INESA ALEMH ATGLR GR.

AUTOKEY (40-55 letters) See: **Vigenère**

This example is a Vigenère Autokey.
Find Vigenère Table in Appendix 2 or use the insert.

pt: The autokey can be used with Vigenère, Variant, Beaufort or Porta.
Key: PRIMER

K: P R I M E R T H E A U T O K E Y C A N B E U S E D W I T H
pt: t h e a u t o k e y c a n b e u s e d w i t h v i g e n e
CT: I Y M M Y K H R I Y W T B L I S U E Q X M N Z Z L C M G L

K: V I G E N E R E V A R I A N T B E A U F O R T O
pt: e r v a r i a n t b e a u f o r t o r p o r t a
CT: M M B E E M R R O B V I U S H S X O L U C I M O

CT:
IYMMY KHRIY WTBLI SUEQX MNZZL CMGLM MBEEM RROBV IUSHS XOLUC IMO.

BACONIAN (25-letter plaintext maximum)

```
A = aaaaa  E = aabaa  I/J= abaaa  N = abbaa  R = baaaa W = babaa
B = aaaab  F = aabab   K = abaab  O = abbab  S = baaab X = babab
C = aaaba  G = aabba   L = ababa  P = abbba  T = baaba Y = babba
D = aaabb  H = aabbb   M = ababb  Q = abbbb U/V= baabb Z = babbb
```

Replace each plaintext letter with its Baconian equivalent.

Example 1:

pt:

```
     s     u     c     c     e     s     s
baaab baabb aaaba aaaba aabaa baaab baaab
```

The a-units and b-units are concealed; in this example the initial letter of each word indicates a or b: A-M = a, N-Z = b.

CT:

Now is a good time to attend college. School work is a good teacher and a good builder of character. Every man should be a student and learn all that there is about a subject.

Example 2:

pt:

```
  n     o     w     i     s     a     g     o     o     d     t
abbaa abbab babaa abaaa baaab aaaaa aabba abbab abbab aaabb baaba
```

For each CT letter let A-M = a, N-Z = b.

CT:

BOWED ASTER PINED JOKED THEIR BLACK HASTE ARRAY INSET CHEST SLING.

BAZERIES (150-250 letters)

pt: Simple substitution plus transposition.

First a number less than a million is chosen (say 3752). It is spelled out and used as the key in a 5x5 ciphertext Polybius square entered in left-to-right horizontal rows. A 5x5 plaintext Polybius square is used with the alphabet in normal order vertically. In the ciphertext and plaintext squares, I and J (I/J) are combined in one cell.

pt

a	f	l	q	v
b	g	m	r	w
c	h	n	s	x
d	i	o	t	y
e	k	p	u	z

CT

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

The plaintext is divided into groups governed by the key numbers, in this example: 3, 7, 5, and 2. Letters within each group are reversed. The result is enciphered using the squares to match. The ciphertext is then written in 5-letter groups.

pt:
s i m/p l e s u b s/t i t u t/i o/n p l/u s t r a n s/p o s i t/i o/n

Reversed Groups (RV):
m i s/s b u s e l p/t u t i t/o i/l p n/s n a r t s u/t i s o p/o i/n

CT:
A C Y/Y U X Y M R Q/K X K C K/G C/R Q I/Y I T N K Y X/K C Y G Q/G C/I

CT: ACYYU XYMRQ KXKCK GCRQI YITNK YXKCY GQGCI.

BEAUFORT (width of period times 10-15 lines deep)

The plaintext is written into a block under the key. All letters in the first column are enciphered using the first key letter, those in the second column using the second, and so on. Using Appendix 4 to encipher the first plaintext letter **c**, look down the key column for **R** and across the plaintext (pt) row **c**. Where the **R row** and **c column** intersect, find the ciphertext **P**.

pt: C equals K minus P

Key: R E C I P R O C A L (period = 10)

pt:	c e q u a l s k m i n u s p	**CT:**	P A M O P G W S O D E K K T

CT: PAMOP GWSOD EKKT.

BIFID (125-150 letters) See: **CM BIFID; TWIN BIFIDS**

Select a period (usually 5-13). Write the plaintext in period length groups. Below each letter write its two coordinates from the 5x5 Polybius square vertically. Now read the numbers horizontally in each period group, replacing each pair of numbers with the letter it represents in the Polybius square.

For this example the period is 7. The keyword, EXTRAORDINARY, is written into the square in a clockwise spiral. The ciphertext is written in 5-letter groups. For other cases the ciphertext can be written in period-length groups.

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

pt: Odd periods are popular.

pt: o d d p e r i o d s a r e p o p u l a r
row#: 2 3 3 2 1 1 4 2 3 4 1 1 1 2 2 2 4 2 1 1
col#: 5 5 5 4 1 4 5 5 5 4 5 4 1 4 5 4 3 2 5 4

CT: 23 32 11 45 55 41 45 23 41 11 25 54 54 14 22 42 11 54 32 54
CT: M W E I N G I M G E O Y Y R L V E Y W Y

CT: MWEIN GIMGE OYYRL VEYWY.

CADENUS (period not over 6)

Columnar tramp using a keyword to shift the order of the columns and at the same time to shift the starting point of each column. The latter is done by attaching a letter of the alphabet (25-letter alphabet as shown with V and W in the same cell) to each row of plaintext in the block. The first column of plaintext goes into the 2nd column of the cipher block (as determined by the key) but it begins with its 22nd letter, (Y here), since the key letter (**E** here, of **EASY**) is attached to the 22nd letter of the key column. Other columns are treated similarly. The final cipher is taken off by rows from the cipher block.

pt: A severe limitation on the usefulness of the Cadenus is that every message must be a multiple of twenty-five letters long.

CT:
SYSTR ETOMT ATTLU SOATL EEESF
IYHEA SDFNM SCHBH NEUVS NPMTO
FAREN USEIE EIELT ARLME NTIEE
TOGEV ESITF AISLT NGEEU VOWUL.

K**: EASY**

pt block					CT block			
E	**A**	**S**	**Y**	Key	**A**	**E**	**S**	**Y**
2	1	3	4		1	2	3	4
a	**s**	e	v	**A**	**S**	**Y**	**S**	**T**
e	r	e	l	Z	R	E	T	O
i	m	i	**t**	**Y**	M	T	A	T
a	t	i	o	X	T	L	U	S
n	o	n	t	V/W	O	A	T	L
h	e	u	s	U	E	E	E	S
e	f	u	l	T	F	I	Y	H
n	e	**s**	s	**S**	E	A	S	D
o	f	t	h	R	F	N	M	S
e	c	a	d	Q	C	H	B	H
e	n	u	s	P	N	E	U	V
i	s	t	h	O	S	N	P	M
a	t	e	v	N	T	O	F	A
e	r	y	m	M	R	E	N	U
e	s	s	a	L	S	E	I	E
g	e	m	u	K	E	I	E	L
s	t	b	e	J	T	A	R	L
a	m	u	l	I	M	E	N	T
t	i	p	l	H	I	E	E	T
e	o	f	t	G	O	G	E	V
w	e	n	t	F	E	S	I	T
y	f	i	v	**E**	F	A	I	S
e	l	e	t	D	L	T	N	G
t	e	r	s	C	E	E	U	V
l	o	n	g	B	O	W	U	L

CHECKERBOARD (60-90 pairs)

A 5x5 Polybius square is used. In the simpler case one 5-letter keyword is to the left of the square and one above it (a). In the complex case, two 5-letter keywords are above and to the left. A plaintext letter is represented by two letters: its coordinates, in row/column order, from outside the square.

(a)

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

(b)

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

Example using square (a).

pt: n u m b e r s c a n a l s o b e u
CT(a): BH AT CW CE KI LI LT KE AE BH AE KW LT AW CE KI AT

pt: s e d a s c o o r d i n a t e s
CT(a): LT KI KT AE LT KE AW AW LI KT BI BH AE LE KI LT

CT(a):
BH AT CW CE KI LI LT KE AE BH AE KW LT AW CE KI AT LT KI KT AE LT KE AW AW LI KT BI BH AE LE KI LT.
or
BHATC WCEKI LILTK EAEBH AEKWL TAWCE KIATL TKIKT AELTK EAWAW LIKTB IBHAE LEKIL T.

Example using square (b).

pt: n u m b e r s c a n a l s o b e u
CT(b): HR RY CG SS EA LA OT KS RS BR AS EG LY AG CS EI AT

pt: s e d a s c o o r d i n a t e s
CT(b): LT KA ET RE OY EE RG AG LA KY HI HH RS OS EI LY

CT(b):
HR RY CG SS EA LA OT KS RS BR AS EG LY AG CS EI AT LT KA ET RE OY EE RG AG LA KY HI HH RS OS EI LY.
or
HRRYC GSSEA LAOTK SRSBR ASEGL YAGCS EIATL TKAET REOYE ERGAG LAKYH IHHRS OSEIL Y.

COMPLETE COLUMNAR TRANSPOSITION (period times 8-15 lines deep)
Written into a rectangular block by filling each row..

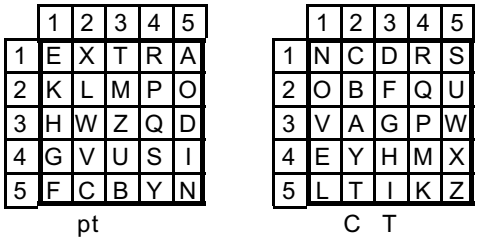
Taken out by columns in order of the key.

pt: filled block
Key: 312

3	1	2
f	i	l
l	e	d
b	l	o
c	k	x

CT: IELKL DOXFL BC.

CM BIFID (Conjugated Matrix Bifid) (150-200 letters) See: **BIFID**



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

pt

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

C T

pt: Odd periods are popular.

Proceed as for Bifid, but after reading out the numbers horizontally, substitute them with the letter found in the second 5x5 Polybius square. The keyword for the latter is NOVELTY, written in alternating verticals.

```
pt:     o d d p e r i   o d s a r e p   o p u l a r
row#:   2 3 3 2 1 1 4   2 3 4 1 1 1 2   2 2 4 2 1 1
col#:   5 5 5 4 1 4 5   5 5 4 5 4 1 4   5 4 3 2 5 4

CT: 23 32 11 45 55 41 45 23 41 11 25 54 54 14 22 42 11 54 32 54
CT: F  A  N  X  Z  E  X  F  E  N  U  K  K  R  B  Y  N  K  A  K
```

Ciphertext is usually written in period-length groups.

CT: FANXZEX FENUKKR BYNKAK.

DIGRAFID (120-220 letters)

A fractionated cipher using a tableau in which both alphabets are mixed. The plaintext is divided into digraphs, and the digraphs are written in groups, the number of digraphs in each group being the period of the cipher. Each digraph has a unique 3-digit number from the tableau and these are written vertically under the corresponding digraph. The 3-digit numbers are fractionated (as in a Trifid) and the new 3-digit numbers are put through the tableau to get the ciphertext digraphs. The first letter of the digraph is found in the horizontal alphabet, the second in the vertical, and the intersection number is placed between them.

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

1	2	3
4	5	6
7	8	9

v	d	p	1
e	f	q	2
r	g	s	3
t	h	u	4
i	j	w	5
c	k	x	6
a	m	y	7
l	n	z	8
b	o	#	9

pt: This is the forest pri

pt (with fractionation 3*):

Th	Is	Is	Th	Ef	Or	Es	Tp	Ri
4	5	5	4	2	5	2	4	6
8	6	6	8	2	1	3	9	1
4	3	3	4	2	3	3	1	5
CT: Hj	Mx	Ws	Wj	Ad	Wg	Fc	Sp	Yi

CT: HJMXWS WJADWG FCSPYI.

pt (with fractionation 4**):

Th	Is	Is	Th	Ef	Or	Es	Tp	Ri
4	5	5	4	2	5	2	4	6
8	6	6	8	2	1	3	9	1
4	3	3	4	2	3	3	1	5
CT: Hj	Tk	Vh	Yu	Ff	Wd	Sq	Yp	Ri

CT: HJTKVHYU FFWDSQYP RI.

*Fractionation 3 means 3 pairs of letters/6 letters.
** Fractionation 4 means 4 pairs of letters/8 letters.

FOURSQUARE (50-70 pairs)

Four 5x5 Polybius squares are set up. Squares 1 and 3 are plain unkeyed (I/J in same cell); squares 2 and 4 are keyed. In this example, squares 2 and 4 have a vertical route.

The first letter of each plaintext pair is found in square 1 and the second in square 3. The two cells are considered opposite corners of a rectangle. Cipher substitutes are found at the other corners of that rectangle, first in square 2 and the second in square 4.

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

pt: co me qu ic kl yw en ee dh el px
CT: LE WI XA FN EX CU DX UV DP GX HZ

CT: LE WI XA FN EX CU DX UV DP GX HZ.
or **LEWIX AFNEX CUDXU VDPGX HZ.**

FRACTIONATED MORSE (110-150 plaintext letters)

Each letter of the plaintext is first enciphered using Morse code with "x" between letters and "xx" between words. (xxx does not exist.) Normally punctuation is not enciphered, but for clarity or variation it may be added at the constructor's discretion. Morse code letters, numbers, and punctuation can be found in Appendix 1.

pt: c o m e a t o n c e.
MC:
– · – · x – – – x – – x · x x · – x – x x – – – x – · x – · – · x
· x x

This series of dots, dashes, x's is taken off in units of three, each trigraph set vertically and cipher letters assigned to each group using a keyword alphabet:

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

   – · – – · · – – x x – ·
   · x – – x – x – – – · x
   – – x x x x x – · · x x
```

CT: C B I I L T M H V V F L.

CT: CBIIL TMHVV FL.

GRANDPRÉ (150-200 plaintext letters)

An 8x8 square is filled with 8-letter words horizontally. The first letter of each word when reading vertically must form a ninth word. Each plaintext letter is represented by a 2-digit number; the coordinates are taken from the square. A letter appearing more than once in the square may be represented by more than one digit-pair. Unless otherwise specified, ALL 26 letters appear in the square.

While an 8x8 square is traditional and preferred, it is not required. The square can be no smaller than 6x6 and no bigger than 10x10. In the case of the 10x10, words are numbered 0-9.

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

pt: The first column is the keyword.

pt: t h e f i r s t c o l u m
CT: 84 27 82 34 56 71 77 26 44 54 64 63 78

pt: n i s t h e k e y w o r d
CT: 52 66 65 84 27 82 36 61 88 73 54 71 13.

GRILLE (12x12 square maximum)

Position 1: Perforations are shown. First quarter of the message is written in across.
Position 2: Turn the grille 90 degrees clockwise. Second quarter of the message is written in.
Position 3: Grille is turned 180 degrees clockwise from its original position. Third quarter of the message is written in.
Position 4: Grille is turned 270 degrees clockwise from its original position. Final quarter of the message is written in.

pt: the turning grille

```
X · · ·      t · · ·      · · · u      · · · ·      · i l ·
· · · X      · · · h      · r · ·      n · g ·      · · · ·
· X · X      · e · t      · · · ·      g · · ·      · · l ·
· · · ·      · · · ·      · n i ·      · · · r      e · · ·
Grille     Position 1   Position 2   Position 3   Position 4
```

CT: T I L U
N R G H
G E L T
E N I R

CT: TILUN RGHGE LTENI R.

This grille would be reported in the sols as "1 8 10 12".

GROMARK (100-150 letters) (**GRO**nsfeld with **M**ixed **A**lphabet and **R**unning **K**ey)

Set up as a K2M with columns taken off the transposition block in alphabetical order (See Keywords in Chapter 8). A 5-digit primer is chosen and a running numerical key is formed by adding successive pairs of digits (dropping 10's). The 1st plus 2nd give the 6th, 2nd plus 3rd give 7th, etc. Applying the key to the plaintext, the digit determines how far to the right to count before finding the substitute in the cipher alphabet. Final ciphertext is written in 5-letter groups with the primer before the first group and the last digit after the last letter as a check.

Key: ENIGMA (264352)

Transposition block

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

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

encipherment: **K:** 23452579772664982037023072537978066
pt: thereareuptotensubstitutesperletter
CT: NFYCKBTIJCNWZYCACJNAYNLQPWWSTWPJQFL

CT: 23452 NFYCK BTIJC NWZYC ACJNA YNLQP WWSTW PJQFL 6.

GRONSFELD (period times 12-15 lines deep)

This one is enciphered just like the Vigenère. The key is limited.
CT = K+pt. [Cipher = Key + Plaintext]

pt: This one uses ten of the twenty-six Vigenère alphabets.
Key: 9321492, period 7

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
0	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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

Key:	9	3	2	1	4	9	2								
	t	h	i	s	o	n	e		C	K	K	T	S	W	G
	u	s	e	s	t	e	n		D	V	G	T	X	N	P
	o	f	t	h	e	t	w		X	I	V	I	I	C	Y
pt:	e	n	t	y	s	i	x	**CT:**	N	Q	V	Z	W	R	Z
	v	i	g	e	n	e	r		E	L	I	F	R	N	T
	e	a	l	p	h	a	b		N	D	N	Q	L	J	D
	e	t	s						N	W	U				

CT: CKKTS WGDVG TXNPX IVIIC YNQVZ WRZEL IFRNT NDNQL JDNWU.

HEADLINES (Five headlines from recent news)

The five headlines are encrypted using simple substitution with the same mixed alphabet at different settings against itself, as with a K3 key.

The mixed alphabet derives from a keyword alphabet, mixed by taking columns from a transposition block in a sequence determined by a second keyword. Cipher settings are determined by a third keyword.

Key Block:

```
A P O T H E C A R Y   Hat = APOTHECARY
1 7 6 9 5 4 3 2 8 10
C H E M I S T A B D   Key = CHEMIST
F G J K L N O P Q R
U V W X Y Z
```

Substitution Block:

```
   1     2   3   4     5     6     7     8   9     10
   C F U A P T O S N Z I L Y E J W H G V B Q M K X D R  pt

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

The three keywords (HAT, KEY and SETTING) are related by context to aid in analysis when solving. At least two of the three keywords are required for SOL credit.

Hat: APOTHECARY **Key**: CHEMIST **Setting**: DRUGS

pt:

```
1. Bush Signs Intelligence Overhaul Legislation
2. Bin Laden Urges Fighters to Strike Oil Facilities
3. Pfizer: Painkiller may pose increased cardiovascular risk
4. Carrey masters disguises in 'Lemony Snicket'
5. Martinez blasts ex-teammate Schilling
```

CT:

```
1. *GCTJ TNWOT NOALZZNWLODL PHLXJFCZ ZLWNTZFANPO
2. *VZS *IUXYS FDHYO CZHWPYDO PT OPDZMY TZI CURZIZPZYO
3. *OAYLWF: OTYIDYEEWF XTJ ONZW YIUFWTZWC UTFCYNQTZUPETF FYZD
4. *GQHHPA YQDKPHD WFDNBFDPD FR '*UPYXRA *DRFGEPK'
5. *UIOYGWQH CVIJYJ QP-YQIUUIYQ *JSXGVVGWD
```

Variations of keying method include taking columns UP the transposition block, substituting with a plaintext block, and reading the setting UP the substitution block.

HOMOPHONIC (50-75 pairs)

The plaintext alphabet is straight with I/J in the same cell. A plaintext or key letter J is replaced with I before encrypting. A 4-letter keyword determines where each of the number sequences will start in each row. 01-25 are in sequence in row 1, 26-50 in row 2, 51-75 in row 3, 76-00 in row 4. The keyword is given by 01, 26, 51, 76 (here GOLF). Each plaintext letter is enciphered by any of the 4 numbers below it.

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
20	21	22	23	24	25	**01**	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19
38	39	40	41	42	43	44	45	46	47	48	49	50	**26**	27	28	29	30	31	32	33	34	35	36	37
66	67	68	69	70	71	72	73	74	75	**51**	52	53	54	55	56	57	58	59	60	61	62	63	64	65
96	97	98	99	00	**76**	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95

pt: w o r d d i v i s i o n s m a y b e k e p t
CT: 16 26 11 99 69 46 33 03 88 79 54 83 12 06 38 94 67 24 04 00 27 89

CT:
16 26 11 99 69 46 33 03 88 79 54 83 12 06 38 94 67 24 04 00 27 89.

INCOMPLETE COLUMNAR TRANSPOSITION (period times 15-18 lines deep)

Written into block horizontally. Taken out by columns in order of key.

pt: Unfilled block
Key: 312

3	1	2
u	n	f
i	l	l
e	d	b
l	o	c
k		

CT: NLDOF LBCUI ELK.

INTERRUPTED KEY (40-60 letters)

The plaintext is enciphered with 1, 2, 3 or more letters of the keyword which is interrupted at random, by plaintext word division, or according to some other scheme. Return to the first key letter each time the keyword is interrupted. The entire keyword must be used at least once.

(Vigenère used in this example.)

pt: This cipher can be used with any of the periodics.
K: ORANGE

K: O R A N O R A N G E O R O R A O R A N O R A O O
pt: t h i s c i p h e r c a n b e u s e d w i t h a
CT: H Y I F Q Z P U K V Q R B S E I J E Q K Z T V O

K: O R A N G O O R O R A O R A N G
pt: n y o f t h e p e r i o d i c s
CT: B P O S Z V S G S I I C U I P Y

CT: HYIFQ ZPUKV QRBSE IJEQK ZTVOB POSZ VSGSI ICUIP Y.

KEY PHRASE (75-100 letters)

The cipher alphabet is a 26-letter phrase which must be complete (not: TOBEORNOTOTBETHATISTHEQUES(tion)) and matched to a straight plaintext alphabet.

Word divisions are retained, and proper nouns and indicated by *.

Alphabets
pt: 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
CT: G I V E M E L I B E R T Y O R G I V E M E D E A T H

pt: a c i p h e r t e x t l e t t e r m a y s t a n d f o r
CT: G V B G I M V M M A M T M M M M V Y G T E M G O E E R V

pt: m o r e t h a n o n e p l a i n t e x t l e t t e r.
CT: Y R V M M I G O R O M G T G B O M M A M T M M M M V.

CT:
G V B G I M V M M A M T M M M M V Y G T E M G O E E R V
Y R V M M I G O R O M G T G B O M M A M T M M M M V.

MONOME-DINOME (60-120 plaintext letters)

Choose a keyword for a 3x8 box, with I/J and two other letters (e.g. Y/Z) sharing entries. Place eight digits above the columns and the remaining two on the second and third rows of the box. The order of the digits may be selected with the box keyword or in any other way (for example, RMASTERTON
6318927054
Using the first two numbers as rows and the rest as column numbers).

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

Letters in the top row are encrypted with a single digit, the column digit, and letters in the second and third rows with the row digit followed by the column digit.

```
pt: h  i  g  h  f  r  e  q  u  e  n  c  y  k  e  y  s  s  h  o  r
CT: 72 2 76 72 70  6  1 39 30  1  4 75 38 71  1 38  8  8 72  5  6

t  e  n  c I  p  h  e  r  t  e  x t
9  1  4 75 2 35 72  1  6  9  1 31 9
```

CT: 72276 72706 13930 14753 87113 88872 56914 75235 72169 1319.

MORBIT (50-75 plaintext letters)

Choose a 9-letter keyword to set up an array as shown. Plaintext is enciphered exactly as in the Fractionated Morse, x between letters, xx between words. The result is then taken off in units of 2, placed vertically, and numbers are taken from the array to form the ciphertext. Numbers represent alphabetical order of the key. (It is often as easy to read pairs horizontally as to rearrange them vertically.)

Key:

W	I	S	E	C	R	A	C	K
9	5	8	4	2	7	1	3	6
·	·	·	–	–	–	x	x	x
·	–	x	·	–	x	·	–	x

pt: Once upon a time.

pt:	o	n	c	e	/	u	p	o	n
MC:	– – – x	– · x	– · – · x	· x x	· · – x	· – – · x	– – – x	– ·	
CT:	**2 7**	**4 3**	**5 8**	**8 1**	**5 1**	**2 8**	**2 7**	**4**	

/	a	/	t	i	m	e
x x	· – x	x – x	· · x	– – x	· x	
6 5	**6 7**	**9 3**	**7 8**			

CT: 27435 88151 28274 65679 378.

MYSZKOWSKI (period times 12-15 lines deep)

Choose a keyword with repeated letters. Number the letters in alphabetical order with repeated letters taking the same number as their first appearance. The plaintext is written in horizontally. The ciphertext is taken off by columns in key order.

pt: Incomplete columnar with pattern word key and letters under same number taken off by row from top to bottom.

Key: BANANA

B	A	N	A	N	A		A	A	A	B	N	N
2	1	3	1	3	1		1	1	1	2	3	3
i	n	c	o	m	p		N	O	P	I	C	M
l	e	t	e	c	o		E	E	O	L	T	C
l	u	m	n	a	r		U	N	R	L	M	A
w	i	t	h	p	a		I	H	A	W	T	P
t	t	e	r	n	w		T	R	W	T	E	N
o	r	d	k	e	y		R	K	Y	O	D	E
a	n	d	l	e	t		N	L	T	A	D	E
t	e	r	s	u	n		E	S	N	T	R	U
d	e	r	s	a	m		E	S	M	D	R	A
e	n	u	m	b	e		N	M	E	E	U	B
r	t	a	k	e	n		T	K	N	R	A	E
o	f	f	b	y	r		F	B	R	O	F	Y
o	w	f	r	o	m		W	R	M	O	F	O
t	o	p	t	o	b		O	T	B	T	P	O
o	t	t	o	m			T	O		O	T	M

CT:
NOPEE OUNRI HATRW RKYNL TESNE SMNME TKNFB RWRMO TBTOI LLWTO ATDER OOTOC MTCMA TPEND EDERU RAUBA EFYFO POTM.

NICODEMUS (period times 15-18 lines deep)

Three steps are used:
1. Column transposition.
2. Vigenère encipherment with the same key.
3. Take off 5 letters at a time from each column in order.

Since last block maybe less than 5 deep, all remaining letters from each column are taken off in column order.

pt: the early bird gets the worm
Key: CAT

C A T	A C T	A C T
2 1 3	1 2 3	1 2 3
t h e	h t e	H V X
e a r	a e r	A G K
l y b	y l b	Y N U
i r d	r i d	R K W
g e t	e g t	E I M
s t h	t s h	T U A
e w o	w e o	W G H
r m	m r	M T

CT: HAYRE VGNKI XKUWM TWMUG TAH.

NIHILIST SUBSTITUTION (period times 8-12 lines deep)

A 5x5 Polybius square is used with a second keyword which also sets the period length. Each plaintext letter is designated by a 2-digit number, its row and column in the square. The message is written in period. Each plaintext letter is then replaced by the sum of its value (the 2-digit number) and the value of the key letter above it (found from the same square). Numbers from 100 to 110 are written 00 to 10.

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

pt: The early bird

Key:

E	A	S	Y
21	22	11	54
T	H	E	E
44	33	21	21
65	**55**	**32**	**75**

A	R	L	Y
22	43	15	54
43	**65**	**26**	**08**

B	I	R	D
23	12	43	25
44	**34**	**54**	**79**

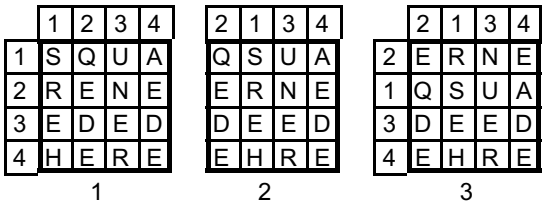
pt: t h e e a r l y b i r d
CT: 65 55 32 75 43 65 26 08 44 34 54 79.

NIHILIST TRANSPOSITION (10x10 maximum)

The same key is applied to rows and columns.

Enter the plaintext in square 1 by rows as shown. Transpose columns by key order into square 2. Transpose rows of square 2 by key order into square 3. Taken off by columns or rows from square 3.

pt: square needed here
Key: 2134



	1	2	3	4
1	S	Q	U	A
2	R	E	N	E
3	E	D	E	D
4	H	E	R	E

1

	2	1	3	4
1	Q	S	U	A
2	E	R	N	E
3	D	E	E	D
4	E	H	R	E

2

	2	1	3	4
2	E	R	N	E
1	Q	S	U	A
3	D	E	E	D
4	E	H	R	E

3

C1: EQDER SEHNU EREAD E. (taken off by columns)

or

C2: ERNEQ SUADE EDEHR E. (taken off by rows)

NULL (25-letter plaintext maximum)

This is a concealment cipher (a form of Steganography).

First letters, last letters, taken in order or reverse order, letters following each vowel, second letters in every other word, taking letters out of each word in a key order, e.g. 21534, etc. are some of the other ways a null may be constructed. In the following example, the middle letter of each word reveals the message.

pt: help

CT: THE GREAT OLD PUMPERS.

PERIODIC GROMARK (75-125 letters) See: **GROMARK**

The plaintext is written out in period determined by the key length (6 here). The numerical key from the transposition block (264351 here) is also used as the "chain-added" key. Keyword letters are written in order above each period group as shown below, repeating as needed. These key letters determine the starting position of the cipher alphabet for that particular group with each letter in the group shifting according to the chain-added key.

Key: ENIGMA (264351)

Transposition block

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

alphabets:
pt: 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
CT: (A J R X)(E B K S Y)(G F P V)(I D O U)(M H Q W)(N C L T Z)
0 4 9 13 17 21
encipherment:

K: E +4 N +21 I +13 G +9 M +17 A +0 E +4 N +21 I +13
pt: Wintry shower swillc ontinu eforth enextf ewdays accord ingtot
#: 264351 807869 875457 529922 718149 899537 784804 522849 740236
CT: RHNAAX NRUZBN IUARXC RTPATB RLIGDS VCIRCV OYPVRA AZZMUS REQYEV

K: G +9 M +17
pt: hefore cast
#: 142597 5674
CT: MMURGW TLUD

CT:
264351 RHNAAX NRUZBN IUARXC RTPATB RLIGDS VCIRCV OYPVRA AZZMUS REQYEV MMURGW TLUD 4.

PHILLIPS (125-160 letters)

Starting with a basic 5x5 Polybius square (#1 below), the first row is shifted down one row at a time form squares #2, 3, 4 and 5. Row two is then shifted down a row at a time to form squares #6, 7 and 8. Each square is used in turn to encipher 5 plaintext letters. Each plaintext letter is enciphered by taking as substitute the letter diagonally down to the right using the proper square. A plaintext letter in the fifth column is replaced by the letter from the first column and the row below it; a plaintext letter in the fifth row is replaced by the letter in the first row and to its right.

pt: Squares one and five are actually the same as are squares two and eight. The overall period is forty.

Key: DIAGONALS

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

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

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

SQ	**#1**					**#2**					**#3**					**#4**					**#5**					**#6**				
pt	s	q	u	a	r	e	s	o	n	e	a	n	d	f	i	v	e	a	r	e	a	c	t	u	a	l	l	y	t	h
CT	K	Z	W	L	Y	T	G	E	D	T	Q	E	T	A	R	B	T	Y	G	T	L	F	X	W	L	P	P	O	X	L

SQ	**#7**					**#8**					**#1**					**#2**					**#3**					**#4**				
pt	e	s	a	m	e	a	s	a	r	e	s	q	u	a	r	e	s	t	w	o	a	n	d	e	i	g	h	t	t	h
CT	T	Y	K	U	T	K	G	K	Y	T	K	Z	W	L	Y	T	G	X	S	E	Q	E	T	I	R	Z	Q	A	A	Q

SQ	**#5**					**#6**					**#7**					**#8**		**#1**
pt	e	o	v	e	r	a	l	l	p	e	r	i	o	d	i	s	f	o	r	t		y
CT	T	C	I	T	Y	K	P	P	V	B	L	H	E	F	H	G	R	E	Y	X		O

CT:
KZWLY TGEDT QETAR BTYGT LFXWL PPOXL TYKUT KGKYT KZWLY TGXSE QETIR ZQAAQ TCITY KPPVB LHEFH GREYX O.

PHILLIPS-C (125-160 letters) See: **PHILLIPS**

Encrypted like Phillips, but with columns instead of rows shifted for each new key block.

pt: Squares one and five are actually the same as are squares two and eight. The overall period is forty.

Key: DIAGONALS

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

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

SQ	**#1**	**#2**	**#3**	**#4**	**#5**	**#6**
pt	s q u a r	e s o n e	a n d f i	v e a r e	a c t u a	l l y t h
CT	K Z W L Y	R K B F R	C F L R S	O P L Y P	L F X W L	M M O Y T

SQ	**#7**	**#8**	**#1**	**#2**	**#3**	**#4**
pt	e s a m e	a s a r e	s q u a r	e s t w o	a n d e i	g h t t h
CT	R K L U R	L K L Y R	K Z W L Y	R K V D B	C F L Q S	C Q X X Q

SQ	**#5**	**#6**	**#7**	**#8**	**#1**
pt	e o v e r	a l l p e	r i o d i	s f o r t	y
CT	T C I T Y	B M M V R	Y N C S N	K U B Y V	O

CT:
KZWLY RKBFR CFLRS OPLYP LFXWL MMOYT RKLUR LKLYR KZWLY RKVDB CFLQS CQXXQ TCITY BMMVR YNCSN KUBYV O.

PHILLIPS-RC (150-180 letters) See: **PHILLIPS**

Encrypted like Phillips, but with both columns and rows shifted for each new key block.

pt: Squares one and five are actually the same as are squares two and eight. The overall period is forty.

Key: DIAGONALS

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

#1

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

#2

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

#3

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

#4

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

#5

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

#6

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

#7

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

#8

SQ	**#1**				**#2**				**#3**				**#4**				**#5**				**#6**			
pt	s	q	u	a	r	e	s	o	n	e	a	n	d	f	i	v	e	a	r	e	a	c	t	u
CT	K	Z	W	L	Y	R	G	F	I	R	U	F	Q	A	R	N	P	Y	G	P	L	F	X	W

SQ	**#7**				**#8**				**#1**				**#2**				**#3**				**#4**			
pt	e	s	a	m	e	a	s	a	r	e	s	q	u	a	r	e	s	t	w	o	a	n	d	e
CT	R	Y	K	U	R	K	G	K	Y	R	K	Z	W	L	Y	R	G	V	C	F	U	F	Q	G

SQ	**#5**				**#6**				**#7**				**#8**				**#1**	
pt	e	o	v	e	r	a	l	l	p	e	r	i	o	d	i	s	f	o	r	t	y	
CT	T	C	I	T	Y	F	P	P	V	S	L	M	E	H	M	G	U	F	Y	V	O	

CT:
KZWLY RGFIR UFQAR WPYGP LFXWL PPOYB RYKUR KGKYR KZWLY RGVCF UFQGR VQAAQ TCITO FPPVS LMEHM GUFYV O.

PLAYFAIR (40-50 pairs)

A 5x5 Polybius square is used. The plaintext is separated into pairs. Double letters in a pair require insertion of a null between them.

Encipher by pairs:

1. When the 2 letters are in the same column of the keysquare, each is enciphered by the letter directly below it. Bottom cycles to the top.

2. When the two plaintext letters are in the same row, each is enciphered by the letter directly to its right. The last letter on the right cycles to the first letter in the same row.

3. When 2 letters are in different rows and columns, they are enciphered by the 2 letters which form a rectangle with them, beginning with the letter in the same row as the first letter of the pair.

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

pt: co me qu ic kl yw en ex ed he lp
CT: DL HF SN CN CR ZX CQ QG FE EQ ON.

POLLUX (80-100 plaintext letters)

Each digit from 0 to 9 represents a dot, dash, or a divider. Two dividers are used to separate words. We usually use 4 dots and 3 of the other symbols in any order. Morse code alphabet is used.

The best solving procedure is to try to locate the x's, remembering that 3 x's in a row are impossible. Because of the length of Morse characters, either the second, third, fourth, or fifth number in the ciphertext must be a divider (unless special signs or numbers are used).

```
1 2 3 4 5 6 7 8 9 0
x - · · x · - - x ·
```

pt: Luck helps.

Morse code: ·-··x··-x-·-·x-·-xx····x·x·-··x·--·x···

CT: 08639 34257 02417 68596 30414 56234 90874 5360.

PORTA (period times 10-15 lines deep)

This periodic uses only 13 alphabets. The first half (A-M) is reciprocal with the second half. The position of the second half is determined by a key designation (A,B or C,D, etc.). The keys are used in the keyword which also determines the period. In the A,B alphabet, pt a = CT N, pt b = CT O, pt n = CT A, pt o = CT B, etc. In the C,D alphabet, pt a = CT O, pt o = CT A, etc.

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

pt: encipherment is reciprocal

Key: PORTA

K =	P	O	R	T	A						
pt=	e	n	c	i	p	**CT**=	Y	G	X	R	C
	h	e	r	m	e		O	Y	J	V	R
	n	t	i	s	r		G	M	Q	J	E
	e	c	i	p	r		Y	W	Q	G	E
	o	c	a	l			H	W	V	U	

CT: YGXRC OYJVR GMQJE YWQGE HWVU.

PORTAX (period times 16-24 lines deep, 8-12 lines paired)

A slide is made up of two alphabets which have been labeled A1 and A2 in the diagram below. The fixed part of the slide contains the first half of the alphabet (A-M). The bottom row of the slide consists of the second half of the alphabet (N-Z). The second alphabet is written below in columns of two characters. The sequence on the sliding part repeats to allow for the slide.

```
                      A B C D E F G H I J K L M        A1/1 (fixed)
N O P Q R S T U V W X Y Z N O P Q R S T U V W X Y Z     A1/2
                                                          (sliding)
A C E G I K M O Q S U W Y A C E G I K M O Q S U W Y     A2
B D F H J L N P R T V X Z B D F H J L N P R T V X Z
```

Enciphering is by pairs. The message is written horizontally into a block under a keyword. Vertical pairs are enciphered. The first letter of the pair (top) is found in the upper alphabet (A1/1 OR A1/2), the second is found in the lower one (A2). These are taken as diagonally opposite corners of a rectangle. The other corners are taken as the substitutes, the letter from the top being taken first. If the two letters are on the same vertical line, the other two letters on that line are the substitutes.

The slide shown is set for the key letters U or V (found below A of the upper part of the top alphabet). Using that key, "in" becomes JL, "no" becomes UA, and "na" becomes DB. The resulting cipher is taken off by horizontal rows.

pt: the early bird gets the worm

K: EASY

```
      K =   E A S Y

      pt =  t h e e     CT =  N I J A
            a r l y           M P B G
            b i r d           Q C W K
            g e t s           H Q J E
            t h e w           U I K Y
            o r m x           M P A T
```

CT: NIJAM PBGQC WKHQJ EUIKY MPAT.

PROGRESSIVE KEY (100-150 letters)

The plaintext is set up in period length groups. Ordinary periodic (here Vigenère) encipherment using the keyword yields a "primary" ciphertext as shown below just under the plaintext. Then a second encipherment of the same type using a progressing key letter (Kp) for each group gives the final ciphertext. For a progression index of 1, the derived progressive key for the second encipherment is A for the first group, B for the second group, etc. For a progression index of 2, the progressive key would be A, C, E, etc. for successive groups.

Key: GRAPEFRUIT, period 10

```
 K:  G R A P E F R U I T  G R A P E F R U I T  G R A P E F R U I T
pt:  t h i s c i p h e r  c a n b e u s e d w  i t h a n y o f t h
C1:  Z Y I H G N G B M K  I R N Q I Z J Y L P  O K H P R D F Z B A
Kp:          A                    B                    C
C2:  Z Y I H G N G B M K  J S O R J A K Z M Q  Q M J R T F H B D C
```

CT: ZYIHG NGBMK JSORJ AKZMQ QMJRT FHBDC NJHJP WXFNO.

QUAGMIRE I (period times 15-18 lines deep)

The Quagmires are numbered in the same way as keywords (See Chapter 8). Thus, a Quagmire 1 uses a K1 keyword plan. An indicator keyword is also used to determine the period and the ciphertext alphabet settings. It may appear vertically under any letter of the plaintext alphabet. The encipherments follow each letter of the indicator key in turn.

pt: The Quag One is a periodic cipher with a keyed plain alphabet run against a straight cipher alphabet.

Key: SPRINGFEV(ER)
Indicator key under ***A*** is **FLOWER** (period 6).

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

	1	2	3	4	5	6							
pt:	t	h	e	q	u	a	**CT:**	Q	P	M	G	Q	R
	g	o	n	e	i	s		B	U	J	U	Y	I
	a	p	e	r	i	o		F	D	M	P	Y	A
	d	i	c	c	i	p		I	F	Q	Y	Y	J
	h	e	r	w	i	t		J	J	H	J	Y	C
	h	a	k	e	y	e		J	L	U	U	T	P
	d	p	l	a	i	n		I	D	V	W	Y	M
	a	l	p	h	a	b		F	S	G	A	E	S
	e	t	r	u	n	a		D	W	H	I	Z	R
	g	a	i	n	s	t		B	L	I	R	V	C
	a	s	t	r	a	I		F	C	Z	P	E	L
	g	h	t	c	i	p		B	P	Z	Y	Y	J
	h	e	r	a	l	p		J	J	H	W	L	J
	h	a	b	e	t			J	L	P	U	P	

CT:
QPMGQ RBUJU YIFDM PYAIF QYYJJ JHJYC JLUUT PIDVW YMFSG AESDW HIZRB LIRVC FCZPE LBPZY YJJJH WLJJL PUP.

QUAGMIRE II (period times 15-18 lines deep)

The Quagmires are numbered in the same way as keywords (See Chapter 8). Thus a Quagmire 2 uses a K2 keyword plan. An indicator keyword is also used to determine the period and the ciphertext alphabet settings. It may appear vertically under any letter of the plaintext alphabet. The encipherments follow each letter of the indicator key in turn.

pt: In the Quag Two a straight plain alphabet is run against a keyed cipher alphabet.

Key: SPRINGFEV(ER)
Indicator key under plaintext alphabet ***A*** is **FLOWER** (period 6).

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

	1	2	3	4	5	6						
pt:	i	n	t	h	e	q	**CT:**	J	I	C	I	C	O
	u	a	g	t	w	o		S	L	Y	K	I	L
	a	s	t	r	a	I		F	V	C	H	E	B
	g	h	t	p	l	a		D	X	C	C	O	R
	i	n	a	l	p	h		J	I	O	E	W	A
	a	b	e	t	i	s		F	M	W	K	K	T
	r	u	n	a	g	a		X	B	G	W	H	R
	i	n	s	t	a	k		J	I	B	K	E	D
	e	y	e	d	c	I		B	J	W	Z	A	B
	p	h	e	r	a	l		U	X	W	H	E	H
	p	h	a	b	e	t		U	X	O	X	C	U

CT:
JICIC OSLYK ILFVC HEBDX CCORJ IOEWA FMWKK TXBGW HRJIB KEDBJ WZABU XWHEH UXOXC U.

QUAGMIRE III (period times 20-25 lines deep)

The Quagmires are numbered in the same way as keywords (See Chapter 8). Thus a Quagmire 3 uses a K3 keyword plan. An indicator keyword is also used to determine the period and the ciphertext alphabet settings. It may appear vertically under any letter of the plaintext alphabet. The encipherments follow each letter of the indicator key in turn.

pt: The same keyed alphabet is used for plain and cipher alphabets.
Key: AUTOMOBILE
Indicator key shown here under plaintext ***A*** **is HIGHWAY** (period 7).

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

	1	2	3	4	5	6	7								
pt:	t	h	e	s	a	m	e	**CT:**	K	R	S	L	W	M	I
	k	e	y	e	d	a	l		T	J	D	V	I	A	B
	p	h	a	b	e	t	I		M	R	G	Q	M	T	M
	s	u	s	e	d	f	o		L	L	I	V	I	F	U
	r	p	l	a	i	n	a		I	X	R	H	T	N	Y
	n	d	c	i	p	h	e		O	N	V	R	H	H	I
	r	a	l	p	h	a	b		I	I	R	M	C	A	O
	e	t	s						V	E	I				

CT: KRSLW MITJD VIABM RGQMT MLLIV IFUIX RHTNY ONVRH HIIIR MCAOV EI.

QUAGMIRE IV (period times 25-30 lines deep)

The Quagmires are numbered in the same way as keywords (See Chapter 8). Thus a Quagmire 4 uses a K4 keyword plan. An indicator keyword is also used to determine the period and the ciphertext alphabet settings. It may appear vertically under any letter of the plaintext alphabet. The encipherments follow each letter of the indicator key in turn.

pt: This one employs three keywords
Key: (pt): SENSORY, (CT): PERC(EP)TION
Indicator shown here under plaintext ***S*** is **EXTRA** (period 5)**.**

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

	1 2 3 4 5		
pt:	t h i s o	**CT:**	V B M R F
	n e e m p		C Y I S P
	l o y s t		M P B R R
	h r e e k		H E I C X
	e y w o r		R R E I G
	d s		D X

CT: VBMRF CYISP MPBRR HEICX RREIG DX.

RAGBABY (80-150 letters)

Historically the Ragbaby has used a 24-letter keyed alphabet. A 26- or 36-letter keyed-alphabet could be used.

Construct a 24-letter keyed alphabet (KA) with I/J and W/X paired:
KA: G R O S B E A K C D F H I L M N P Q T U V W Y Z

If J or X appears in the keyword it may be replaced with I or W, respectively; however, it is preferable to choose a key that uses neither letter.

A hyphenated word is considered a single word, as is a word with an apostrophe.

Example 1:

pt: t w o - s q u a r e
#: 2 3 4 5 6 7 8 9 10

Example 2:

pt: Word divisions are kept.

Number the letters of each plaintext word in sequence beginning with 1 for the first letter of the first word, 2 for the first letter of the second word, etc. The sequence goes to 24 and repeats (25=1). Each plaintext letter is enciphered by moving to the right the designated number of spaces, using the letter found there as its substitute.

pt: w o r d d i v i s i o n s a r e k e p t
#: 1 2 3 4 2 3 4 5 6 7 8 9 10 3 4 5 4 5 6 7
CT: Y B B L H N G Q D U F G L D E F H F Y R.

RAILFENCE (3-7 rows, 10-15 times number of rows)

The plaintext may start at any point on the cycle, is written in zig-zag, and is taken off by rows or vice versa.

Key types are indicated in the solutions.
For example: "4 0" indicates four rows and no offset. Offsets run from 0 to 2R-3, where R is the number of rows.

pt: Civil war field cipher.

```
c       l       f       d       h
  i   i   w   r   i   l   c   p   e
    v       a       e       i       r
```

CT: CLFDH IIWRI LCPEV AEIR.

REDEFENCE (3-7 rows, 10-15 times the number of rows)

The plaintext may start at any point in the cycle, is written in zig-zag, and is taken off by rows according to a key (here 213).

Key types are indicated in the solutions.
For example: "3 2" indicates three rows and an offset of 2.

pt: Civil war field cipher.

```
 2:  c       l       f       d       h
 1:    i   i   w   r   i   l   c   p   e
 3:      v       a       e       i       r
```

CT: IIWRI LCPEC LFDHV AEIR.

ROUTE TRANSPOSITION (8x8 square maximum, 8x10 rectangle maximum)

There are many routes and combinations of routes from which to choose: horizontal, vertical, alternating horizontal, alternating vertical, diagonal, alternating diagonal, clockwise inward spiral, counterclockwise inward spiral, clockwise outward spiral, and counterclockwise outward spiral. Don't forget about the various starting positions!

This example is written into the block by alternating diagonals and taken out by clockwise spiral. The block must be complete.

pt: there are many routes

```
t h a
e e r
r e y
m n r
a o e
u t s
```

CT: THARY RESTU AMREE ENO.

RUNNING KEY (40-50 letters)

The plaintext is divided in half and written in two rows, one under the other. The top half acts as the key, the bottom half acts as the plaintext and the encipherment is the cipher. (Vigenère is used with this example.)

pt: This cipher can be used with any of the periodics.

Key: T H I S C I P H E R C A N B E U S E D W
pt: i t h a n y o f t h e p e r i o d i c s
CT: B A P S P G D M X Y G P R S M I V M F O

CT: BAPSP GDMXY GPRSM IVMFO.

SERIATED PLAYFAIR (10-15 groups paired) See: **PLAYFAIR**

The plaintext is written horizontally in 2-line periodic groups. This is shown below in period 6.

pt: Come quickly we need help immediately. tom.

pt: comequ eneedh mediat
icklyw xelpim elytom

Vertical pairs thus formed are enciphered by the Playfair rules (1-3). When a vertical pair would be a double letter a null is inserted. Using the 5x5 Polybius square

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

pt: comequ eneedh mediat
icklyw xelpim elytom

gives

CT: **NLBCSP QQCDCM HCFTRH**
CDFGXZ GCGQTB FGWHGB.

The cipher is taken off horizontally in 5-letter groups.

CT: NLBCS PCDFG XZQQC DCMGC GQTBH CFTRH FGWHG B.

SLIDEFAIR (key length times 10-18 lines deep)

Enciphering is done in pairs. A keyword is used to fix the period. **Period length is the length of the keyword.** The first plaintext letter is found in the top alphabet and the second in one of the lower alphabets, depending on which letter of the keyword is in use. The plaintext pair is thought of as forming diagonally opposite corners of a rectangle. The letters from the other corners are the substitutes, that from the top taken first. If the letters form a vertical pair in the alphabets, the cipher equivalent is the pair just to the right.

Abbreviated Vigenère Table:

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

Abbreviated Variant Table:

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	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

Abbreviated Beaufort Table:

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

For example: Using the abbreviated tables found above, if the **key letter is B**, then

		Vigenère CT	**Variant CT**	**Beaufort CT**
pt	ca becomes	**ZD**	**BB**	**BZ**
pt	de becomes	**EF**	**FC**	**XY**

The following example uses Vigenère encipherment.

Key: DIGRAPH

pt: The Slidefair can be used with Vigenère , Variant or Beaufort.

K: **D I G R A P H**

pt:	th	es	li	de	fa	ir	ca	**CT:**	EW	KM	CR	NU	AF	CX	TJ
	nb	eu	se	dw	it	hv	ig		YQ	MM	YY	FU	TI	GW	ZP
	en	er	ev	ar	ia	nt	or		KH	JM	PK	BS	AI	EC	KV
	be	au	fo	rt					CF	MI	IL	CI			

CT:
EW KM CR NU AF CX TJ YQ MM YY FU TI GW ZP KH JM PK BS AI EC KV CF MI IL CI.

SWAGMAN (3-6 times key square)

A transposition cipher. Pick a random numerical key of 4-8 digits. Make a key square using the same digits randomly with no row or column containing a repeated number. Plaintext is written horizontally to complete a rectangle, using nulls if necessary. Ciphertext is formed by placing plaintext letters into the cipher squares vertically in order of key numbers. The final cipher is taken off vertically.

pt: Don't be afraid to take a big leap if one is indicated. You cannot cross a river or a chasm in two small jumps.

Key: 32145

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

K:	3 2 1 4 5	3 2 1 4 5	3 2 1 4 5	3 2
	1 5 3 2 4	1 5 3 2 4	1 5 3 2 4	1 5
	2 4 5 3 1	2 4 5 3 1	2 4 5 3 1	2 4
	5 3 4 1 2	5 3 4 1 2	5 3 4 1 2	5 3
	4 1 2 5 3	4 1 2 5 3	4 1 2 5 3	4 1

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

CT:
ENDSC MORDA NIBOI SICTN ASTGB LTEWA OAREE FSAID VPYRM OEAIA FUILR LDOCO TJNRA AENOU NCMIT SOAPH SKATI.

TRIDIGITAL (75-100 letters)

A 10-letter keyword is used to produce a numerical key which is placed above a block 10 columns wide. A keyword alphabet (26 letters) is written into the block leaving the last column blank. Each pt. letter is enciphered by the digit above it. The digit above the last column is used as a word separator.

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

pt: t h e i d e s o f m a r c h
CT: 0 3 0 9 5 6 0 7 9 5 8 9 1 0 7 7 3.

CT: 03095 60795 89107 73.

TRIFID (120-150 letters) See: **TWIN TRIFID**

Start with a 27-letter alphabet (# as the 27th symbol). Select a period (5-15) and write plaintext in period length groups. Below each plaintext letter write its three coordinates vertically using the key array. Reading horizontally, replace each 3-digit number with the letter it represents from the keyword alphabet identified by its vertical coordinates in the array. Complete each period-length group before going on to the next, i.e., use second and third rows of numbers as shown by "/". The period of the example is 10.

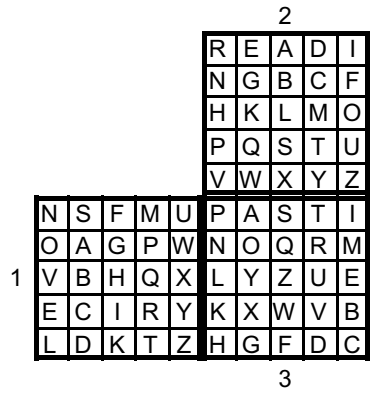
```
1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 3 3 3 3 3 3 3 3 3
1 1 1 2 2 2 3 3 3 1 1 1 2 2 2 3 3 3 1 1 1 2 2 2 3 3 3
1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3
E X T R A O D I N Y B C F G H J K L M P Q S U V W Z #

pt: t r i f i d s a r e / f r a c t i o n a t / e d c i p h e r s
#:  1 1 1 2 1 1 3 1 1 1   2 1 1 2 1 1 1 1 1 1   1 1 2 1 3 2 1 1 3
 :  1 2 3 2 3 3 2 2 2 1   2 2 2 1 1 3 2 3 2 1   1 3 1 3 1 2 1 2 2
 :  3 1 2 1 2 1 1 2 1 1   1 1 2 3 3 2 3 3 2 3   1 1 3 2 2 3 1 1 1
CT: E Y M X V U C R Y Y / Y Y E A Y V Y O V V / X I T D P A T H E
```

Ciphertext is written in 5-letter groups or period length.

CT: EYMXV UCRYY YYEAY VYOVV XITDP ATHE.

TRI-SQUARE (100-125 groups)

Three 5x5 Polybius key squares are used. The plaintext is written in pairs. The first plaintext letter is found in square 1, the second in square 2. A ciphertext trigraph is formed for each plaintext digraph: Any letter in the same column with the first plaintext letter in square 1 may be used as the first cipher letter. The intersection in square 3 of the row containing the first plaintext letter in square 1 with the column containing the second plaintext letter in square 2 gives the second cipher letter. Any letter in the same row in square 2 as the second plaintext letter may be used as the third ciphertext letter.



pt: t h r e e k e y s q u a r e s u s e d x
CT: RHL QXR LXO EVZ BAT XSE RXD DIU AAA BFZ.

TWIN BIFID (100-150 letters each, 18 letter minimum repeat) See: **BIFID**

Two bifid messages using the same Polybius key square but with different periods, have a phrase of the plaintext in common. For use in the Cipher Exchange, it is recommended that one period be odd and one even.

TWIN TRIFID (100-150 letters each, 16 letter minimum repeat) See: **TRIFID**

Two trifid messages using the same key but with different periods, have a phrase of the plaintext in common. For use in the Cipher Exchange, it is recommended that one period be odd and one even.

TWO-SQUARE (45-65 pairs)

Two 5x5 Polybius squares are set up up. The message is divided into pairs. The first letter of each pair is found in square 1, the second in square 2. The cipher equivalents are those letters forming the opposite corners of a rectangle determined by the pt pair. If the plaintext letters are in the same row the cipher equivalents are the same letters reversed.

1

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

2

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

pt: an ot he rd ig ra ph ic se tu px
CT: IR RT EH MK GI ME QG RU NM MZ SV.

VARIANT (period times 10-15 lines deep)

The plaintext is written into a block under a key word. All letters in the first column are enciphered using the first key letter; the second column uses the second key letter, etc.

To encipher the example below: Find the first letter of the plaintext, c, look down the K (key) column of the tableau (See Appendix 3) for A and across the top (A, Plaintext) row for I. Where A's row meets c's column find the ciphertext, C.

pt: C equals P minus K.
Key: APPLE

K:	A	P	P	L	E
pt:	c	e	q	u	a
	l	s	p	m	i
	n	u	s	k	

CT:	C	P	B	J	W
	L	D	A	B	E
	N	F	D	Z	

CT: CPBJW LDABE NFDZ.

VIGENÈRE (period times 10-15 lines deep)

The plaintext is written into a block under the key

For this example, the block is 14 across. All letters in the first column are enciphered using P as key, in the second using O, etc. Thus to encipher the first letter of the plaintext, **i**, look down the K (key) column of the tableau (See Appendix 2) for **P** and across the top (pt) row for **i**. Where **P**'s row meets **i**'s column find ciphertext **X**.

pt: In the Vigenère, C equals K plus P where A is zero, B is one, etc.

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

CT: XBEFE GXNEO IKMET EFYLD ZWLVW IEJTF PYIDO LRPFB AQCSP RC.