Parabola Volume 19, Issue 3 (1983)

SECRET CODES III

BY

JOHN LOXTON

According to Francis Bacon, perfect ciphers may be recognised by the following virtues : "that they be not laborious to write and read; that they be impossible to decipher; and, in some cases, that they be without suspicion." In previous articles in Parabola (volume 18, number 3, and volume 19, number 1), I have described the basic substitution and transposition ciphers. They are both easy enough to write and read, but unfortunately very easy to decipher and so almost beneath suspicion. (On the other hand, Caesar's wife was without suspicion, but she was apparently not a mere cipher.) In this article, I will describe some ciphers of greater virtue than the ones mentioned above.

Polyalphabetic substitution

An obvious way to strengthen the basic substitution cipher is to use several different substitutions in turn to encipher the letters of the message. An extra key is given to specify the substitution to be used at each stage. For example, in the Vigenère cipher, there are 25 substitution alphabets, each of which is a cyclic shift of the normal alphabet on the top line. The 26 alphabets are labelled with the letters A to Z. There are various schemes for choosing the key which specifies which of the substitutions is to be used.

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

(a) Repeating key. Here the key is a word or phrase, repeated as many times as may be necessary to encrypt the message. For example, if the key is PROVE and the message is "the mathematician loves theorems," the resulting cipher is

message	THE	MATHEMATICIAN	LOVES	THEOREMS
key	PRO	VEPROVEPROVEP	ROVEP	ROVEPROV
cipher	IYS	HEIYSHEIZQDEC	CCQIH	KVZSGVAN

The first letter, T, is coded by substitution alphabet P in which T corresponds to I; the second letter, H, is coded by substitution alphabet R in which H corresponds to Y, and so on. Note that the various E's may be coded by different substitution alphabets. In fact, the five E's in the message are coded as S, S, I, Z and V. Thus, we cannot identify E by looking for the most common letters in the cipher as we did in cracking the simple substitution cipher. However, if the message is long enough, there are bound to be repeated matchings between the letters of the key and the message. In our example, the repeated group IYSHE discloses the fact that the first two groups of 5 letters of the message are the same and that these two groups have been coded by the same key. The analyst would guess that the key consists of five letters. Now the cipher text can be broken up into five strings of letters each of which has been coded with a simple substitution. (In the example, IIICHG have been coded with substitution alphabet P, YYZCKV by substitution alphabet R, and so on.) Each of these strings can be subjected to a frequency analysis and successfully decoded if the message is long enough. This procedure was discovered by Kasiski in 1863.

(b) Running key. Since the repetitions of the repeating key lead to its downfall, we can instead try a non-repeating key, thus

message	THE	MATHEMATICIAN	LOVES	THEOREMS
key	THE	SQUAREONTHEHY	POTEN	USEISEQU
cipher	MOI	EQNHVQOGBJMHL	ACOIF	NZIWJICM

This cipher was held to be unbreakable until it was cracked by Kerckhoff in 1883. (This is a recurring theme in the history of cryptography.) It is vulnerable because the letters of both the message and the key will occur with the usual frequencies for English text. For example, E occurs with frequency 0.131, so E coded with substitution alphabet E occurs with frequency $(0.131)^2 \approx 0.0169$. A much longer cipher text is required for the statistical analysis, but the idea and the inevitable conclusion are the same as for a simple substitution cipher. In practice, the cryptanalyst usually has many ciphers encrypted using the same key and he can exploit the fact that the first letter of each cipher must come from the same substitution alphabet.

(c) The one-time pad. From the analysis of the ciphers in (a) and (b) above, we see that the key in a really secure cryptosystem must be as long as the message (so that the key has no obvious repetitions) and the key must be random (so that there is no possibility of a frequency analysis based on the occurrences of various letters in English text). This idea was proposed by Vernam in 1926. The sender somehow acquires a large supply of random key which he uses to code his message in the same way as in (b) above. The sender must also deliver a copy of his random key to the receiver by classified carrier pigeon or some other secure method and the receiver is then in a position to decode the message. Naturally, the key cannot be used again, hence the name one-time pad. The main difficulty of the system is clear; it requires the exchange of large amounts of key before messages are sent. On the other hand, the code is totally secure. The reason is that the key is random, so that each letter of the key is equally likely to be any of the letters from A to Z, independent of whatever the rest of the key may be. As far as the cryptanalyst is concerned all possible ways of deciphering a given letter of the cipher text are equally likely and so all messages of the same length as the cipher text are equally likely. The cipher is unbreakable. It is reported that the one-time pad is used on the hot line between Washington and Moscow and it is apparently used by Russian "field operatives." However, the large volume of key required prevents widespread use of this system.

Polygraphic substitution

There is another way to prevent the cryptanalyst from using the dreaded frequency analysis. Instead of encoding the message letter by letter, we can operate on pairs of letters (digraphs), or triples (trigraphs), or in general, on polygraphs. This can increase the security of the system, at the expense of greater complexity in the coding and decoding.

The most popular manual system of this sort is the Playfair cipher invented by Wheatstone. The alphabet is written in a 5 × 5 array to form the key:

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

The coding is done by breaking the message into pairs of letters and applying the following geometrical rules:

(a) If the letters of a digraph are in the same row of the table, substitute the letter immediately to the right of each letter. For example PR is coded as QU and DF as EB.

(b) If the letters of a digraph are in the same column, substitute the letters immediately beneath them. For example, QX is coded as XT.

(c) If neither (a) nor (b) applies, the letters of the digraph are the opposite corners of a rectangle. Substitute the letters appearing in the other two corners of this rectangle. For example, CL is coded as EI and BX as DV.

The Playfair cipher can be cracked by using digraph frequency counts and comparing the counts with the expected frequencies of digraphs in English text. This is harder than the frequency analysis for a simple substitution code because the common digraphs are not as sharply differentiated as are the common letters in English. However, the statistical method will again succeed if enough cipher text is available for analysis.

Another polygraphic system was invented by Hill in 1929. It was never adopted in practice because of the difficulty of carrying out the coding and decoding operations by hand. If Hill had invented the computer as well, these problems would not have arisen. Here is a simple example to show how the system works.

message MATHEMATICIANSXLOVEXTHEOREMS

The first step is to change the letters of the message to numbers, thus

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	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

We will be doing arithmetic with these numbers, working modulo 26. That is, we consider 27 as the same as 1 since they differ by a multiple of 26, so that 27 also represents A. Again, 28, 54, 80, -24, -50 are the same as 2 modulo 26 and all represent B. The numerical version of the message is

13 1 20 8 5 13 1 20 9 3 9 1 14 19 24 12 15 22 5 24 20 8 5 15 18 5 13 19

Now break the message up into pairs of numbers

$$\begin{pmatrix}13\\1\end{pmatrix} \begin{pmatrix}20\\8\end{pmatrix} \begin{pmatrix}5\\13\end{pmatrix} \begin{pmatrix}1\\20\end{pmatrix} \begin{pmatrix}9\\3\end{pmatrix} \begin{pmatrix}9\\1\end{pmatrix} \begin{pmatrix}14\\19\end{pmatrix} \begin{pmatrix}24\\12\end{pmatrix} \begin{pmatrix}15\\22\end{pmatrix} \begin{pmatrix}5\\24\end{pmatrix} \begin{pmatrix}20\\8\end{pmatrix} \begin{pmatrix}5\\15\end{pmatrix} \begin{pmatrix}18\\5\end{pmatrix} \begin{pmatrix}13\\19\end{pmatrix}$$

Let $\underset{\sim}{x}$ be one of these vectors. The code for $\underset{\sim}{x}$ is obtained by multiplying $\underset{\sim}{x}$ by a suitable 2×2 matrix A. We choose the following rule with $A = \begin{pmatrix}8 & 13\\-5 & -8\end{pmatrix}$:

$$\text{message} \quad \underset{\sim}{x} = \begin{pmatrix}a\\b\end{pmatrix} \qquad \text{code} \quad \underset{\sim}{y} = \begin{pmatrix}c\\d\end{pmatrix} = \begin{pmatrix}8 & 13\\-5 & -8\end{pmatrix}\begin{pmatrix}a\\b\end{pmatrix} = \begin{pmatrix}8a + 13b\\-5a - 8b\end{pmatrix}$$

$$\text{Thus} \quad \begin{pmatrix}13\\1\end{pmatrix} \quad \text{becomes} \quad \begin{pmatrix}8 \times 13 + 13 \times 1\\-5 \times 13 - 8 \times 1\end{pmatrix} = \begin{pmatrix}117\\-73\end{pmatrix} = \begin{pmatrix}4 \times 26 + 13\\-3 \times 26 + 5\end{pmatrix} = \begin{pmatrix}13\\5\end{pmatrix}.$$

The last step comes about because we are ignoring multiples of 26. Carrying out this process on the whole message gives

$$\begin{pmatrix}13\\5\end{pmatrix} \begin{pmatrix}4\\18\end{pmatrix} \begin{pmatrix}1\\1\end{pmatrix} \begin{pmatrix}8\\17\end{pmatrix} \begin{pmatrix}7\\9\end{pmatrix} \begin{pmatrix}7\\25\end{pmatrix} \begin{pmatrix}21\\12\end{pmatrix} \begin{pmatrix}10\\18\end{pmatrix} \begin{pmatrix}16\\9\end{pmatrix} \begin{pmatrix}14\\17\end{pmatrix} \begin{pmatrix}4\\18\end{pmatrix} \begin{pmatrix}1\\11\end{pmatrix} \begin{pmatrix}1\\26\end{pmatrix} \begin{pmatrix}13\\17\end{pmatrix}$$

In letters, the message in code is

M E D R A A H Q G I G Y U L J R P I N Q D R A K A Z M Q

To decode this, the receiver converts the cipher text back into pairs of numbers and multiplies each pair by the inverse matrix A^{-1}.
In symbols, the process amounts to this :

$$\text{message } \underset{\sim}{x} \xrightarrow{\text{code}} \text{cipher } A\underset{\sim}{x} \xrightarrow{\text{decode}} A^{-1}A\underset{\sim}{x} = \underset{\sim}{x} \text{ message}$$

In our case, the decoding rule is as follows :

$$\text{code } \underset{\sim}{y} = \begin{pmatrix} c \\ d \end{pmatrix} \qquad \text{message } \underset{\sim}{x} = \begin{pmatrix} -8 & -13 \\ 5 & 8 \end{pmatrix}\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} -8c - 13d \\ 5c + 8d \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$$

(The last step uses the relations $c = 8a + 13b$, $d = -5a - 8b$ found above.)
In this way, $\begin{pmatrix} 13 \\ 5 \end{pmatrix}$ becomes $\begin{pmatrix} -8 \times 13 - 13 \times 5 \\ 5 \times 13 + 8 \times 5 \end{pmatrix} = \begin{pmatrix} 169 \\ 105 \end{pmatrix} = \begin{pmatrix} 6 \times 26 + 13 \\ 4 \times 26 + 1 \end{pmatrix} = \begin{pmatrix} 13 \\ 1 \end{pmatrix}$

and the full message can be decoded to give the numbers we started with. More generally, if $A = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ then $A^{-1} = \dfrac{1}{ps - qr}\begin{pmatrix} s & -q \\ -r & p \end{pmatrix}$. It is simplest to choose a matrix A with $ps - qr = 1$ in the specification of this code.

You might like to experiment with matrix codes. Devise a computer program to perform the coding and decoding. How much security do these systems offer? You will find more explanations and applications for matrices in Parabola, Volume 15, number 3.

At this point, about 1930, after many peaceful centuries, cryptography suffered its industrial revolution and changed dramatically just in time for World War II. Then, around 1960, cryptography reeled again under the computer revolution. I will describe some of these events in my next article.