perhaps we're on the right track. Let's put the rest of the message through the transformation. Two behind F is H; two behind K is M; and so our first word could be HOME . . .

Caesar's Cypher, then, is a substitution code that relies on 'sliding' the alphabet up or down a given number of places to determine the new value of each character. It can be refined further by using a string of key transformations — 24225, for example. In this case the first letter would be shifted two places, the second four, the third two, and so on. When the end of the key string is reached, we loop back to the beginning again. Using this key string, our sample message would be:

FKKC XMINSOCN AMPPOC

In this instance, frequency analysis will be entirely useless because there is no uniformity to the substitution — a letter will have different substitutes depending upon its position in the overall message. Another simple self-contained cypher renders the same message thus:

H PRUOECMUE OREMOTCS

If we look closely, we can see that this string of characters is in fact an anagram of HOME COMPUTER COURSE, complete with the two spaces between the words. Here, we are simply trying to determine the encrypting algorithm, given samples of both plain text and encrypted text — a surprisingly common procedure. If the cypher is to be understandable by the recipient of the message, then the jumbling up of the letters must be in some way predictable. This particular cypher, known as the Bar Fence for reasons that will soon become obvious, also requires the decoder to know the key — in this case it is 3. Let us take the first five characters and write them out with three spaces between:

H*** ***P***R***U

Recognise anything? Well try this then: write out the plain text message on three lines, going down and up between the lines, thus:

H * P R U
O E C M U E * O R E
M O T C S

The asterisks represent the spaces between words, and the method of encryption is plain.

The examples that we have cited so far have all been cyphers — defined as a method of secret writing using substitution or transformation of letters according to a key. Codes are rather different in that they tend to substitute whole blocks for other, normally smaller, blocks (thus allowing data compression at the same time). Their drawback is that they require both parties to possess a code book before messages can be communicated. One example of this technique uses a commonly available novel, newspaper or other piece of text and indicates the words that go to make up the message by simply giving the sequence number in which they occur. A piece of text like:

'Johnny went home and asked his mother if he might play a computer game. "Of course!", said his mother.'

could be the key to the code 3,10,3. Perhaps you can deduce the message . . .

A computer of any type is of tremendous value when attempting to either encrypt or decrypt messages in cypher. A prime requirement of Caesar's Cypher, for example, is the ability to move through an alphanumeric string, adding or subtracting a constant to the ASCII value of each character, which can then be printed. That constant must be capable of amendment when the program is run, and should make the alphabet wrap around (that is, looking up A where the key is one, should give Z). Thus:

PDWPO WHH BKHGO

Caesar's Cypher

This program (written in Commodore BASIC) will encode text into Caesar's Cypher using a five element multi-key string. The message appears in plain text as it is being entered, and when RETURN is pressed the encrypted version is printed. The message should be entered without spaces or punctuation

```
10 INPUT "ENTER A FIVE FIGURE KEY";K$
20 INPUT "ENTER THE MESSAGE";M$
30 FOR I=1 TO LEN(M$)
40 LET J=I — INT(I/5)*5+1
50 REM *** ROTATES THROUGH KEY
60 LET M=ASC(MID$(M$,I,1)) — VAL(MID$(K$,
   J,1))
70 IF M<65 THEN LET M=M+26
80 PRINT CHR$(M);
90 NEXT I
```

For the Spectrum, line 60 should be replaced with:

```
60 LET M=CODE(M$(I)) — VAL(K$(J))
```

Cryptanalysis
One of the earliest uses of computers was to crack the very complex multi-key substitution codes in use by both sides during the Second World War. The Germans had developed a machine called ENIGMA that generated its own cyphers. The immensely complicated cryptograms that resulted caused the Allies to devote a great deal of effort to their interpretation. Success finally came to the Colossus group, working at Bletchley Park, of which Alan Turing was a prominent member

COURTESY OF THE SCIENCE MUSEUM