

Chapter 5

How to Use a Computer to Solve Ciphers

You may have ideas of using a computer to solve the ciphers shown in *The Cryptogram*. In many instances, this is very practicable – at least to assist in some of the clerk-work, if not to obtain a complete solution. There are even programs available for those who have computers, but no ability or desire to do their own programming. In these cases, the computer is used as a tool just like a pencil.

Because the computer must be programmed for a particular set of circumstances, there will always be a possibility that a manual encipherment will have a twist that is outside the range of the particular program. You should not therefore expect a 100% success rate. A study of why a cipher cannot be solved may lead to a better program. This is one of the challenges of using a computer.

Some ciphers lend themselves to a blend of human thought and machine trials to achieve a successful solution. The Aristocrat is an example. Programs are available which will replace a chosen letter in all its occurrences in the text, saving a great deal of paper and pencil work. Other types of cipher will yield to "brute force" trials, in which every possible combination is tried by the computer until a valid answer is obtained. Examples of this type are Caesar ciphers, some Cryptarithmic puzzles, and the Homophonic. A human would rarely wish to use such a method, and part of the computer challenge is to see whether a short-cut can be programmed.

The computer can be very helpful in placing tips at the correct places in ciphertxts, providing an entry for cryptanalysis. If a tip is not available, there are programs that will run letter frequency counts, distributions, digram and trigram frequencies, indices of coincidence, etc., which not only assist with the cryptanalysis, but may enable the type of cipher to be determined (if unknown) and possibly the original language as well.

The computer naturally lends itself to the solution of ciphers produced by mechanical or computer means. Some of the famous machines of WWII, such as the Enigma, can be duplicated quite simply on small home computers. However, as these ciphers are usually outside the range of paper and pencil solution, they are not normally considered in *The Cryptogram*.

The computer will, of course, do a very fast job of encipherment, and in some cases a suitable enciphering program will lead to the design of a better deciphering algorithm.

It is not usually vital that the computer program run at maximum possible speed. An answer in half an hour, or a trial running all night, is not unreasonable, so many of the published programs deliberately use BASIC in order to be compatible with the largest number of machines (and the largest number of computer users). For the same reason, it is not necessary to have the latest, biggest, or fastest computer; much good work is done with machines that are now obsolete compared to modern operating systems and large applications. Even a 10-year-old computer is likely to have enough disk and memory to be able to deal with a 300,000-entry word list, and to be powerful enough to handle some brute force attacks and to support a faster language than BASIC. The size of the programs is often quite small. Of course, if you wish to hold an 80,000 word list in memory to help with pattern word searches, you will need a large machine; and, if you wish to try a brute force technique, you may wish to use a faster language than BASIC. The Computer Column appears in *The Cryptogram* for more advanced computer users.