STREAM CIPHERS : APPLICATIONS AND TECHNIQUES

Dr. H. J. Beker

There are three types of cipher system in common usage today : block ciphers, cipher feedback systems and stream ciphers.

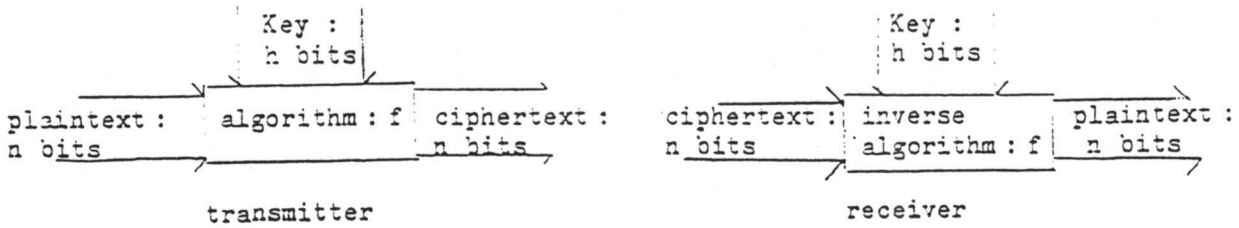
In each case an h-bit key $\underline{k}$, say, ($\underline{k} = (k_1, k_2, \ldots, k_n)$) is provided by the user and then mixed with the data to provide ciphertext. The difference between the three systems is in the type of function that is used for the mixing. For a block cipher the function employed produces a block of ciphertext bits $\underline{c} = (c_1, c_2, \ldots, c_n)$ say, by acting upon a block of message, $\underline{m} = (m_1, m_2 \ldots, m_n)$ and $\underline{k}$, i.e. $\underline{c} = f(\underline{k}, \underline{m})$ and $n > 1$. A typical cipher feedback system may produce a single bit of ciphertext c_{n+1}, by acting upon a number of previous bits, of ciphertext $c_1, c_2, \ldots, c_n$, say, together with the key $\underline{k}$ and a single bit of message m_{n+1} say, i.e. $c_{n+1} = f(\underline{k}, c_1, c_2, \ldots, c_n, m_{n+1})$. So in this case the next ciphertext bit produced depends on a number of previous ciphertext bits. With a stream cipher, $c_{n+1} = f_{n+1}(\underline{k}, m_{n+1})$ so that a single bit of ciphertext is produced from a function of the key and a single bit of message. Notice that the function changes from bit to bit. In fact, it is normally the modulo 2 addition (XOR) of the function of key and single bit of message that provides the next bit of ciphertext. Figure 1 shows examples of each of these systems.

Over the last two or three years block ciphers have been under much discussion. The primary reason for this interest has been the introduction of the Data Encryption Standard (DES), which is a block cipher utilizing 56 bits of key and 64 bits of data to produce a 64-bit ciphertext block. One great advantage of a block cipher is its flexibility: it can be used as a conventional block cipher (the code-book form), in a cipher feedback configuration or as a stream cipher. Thus a block cipher is a reasonable choice for a standard. However, there are many situations where a standard is not required and in fact may not be desirable. For these custom-designed systems, flexibility is not necessarily needed. In such circumstances there may be a definite requirement for a stream cipher rather than either of the other modes available. This is the case for many communications systems since a major disadvantage of both block ciphers and cipher feedbacks is that they propagate errors caused by the

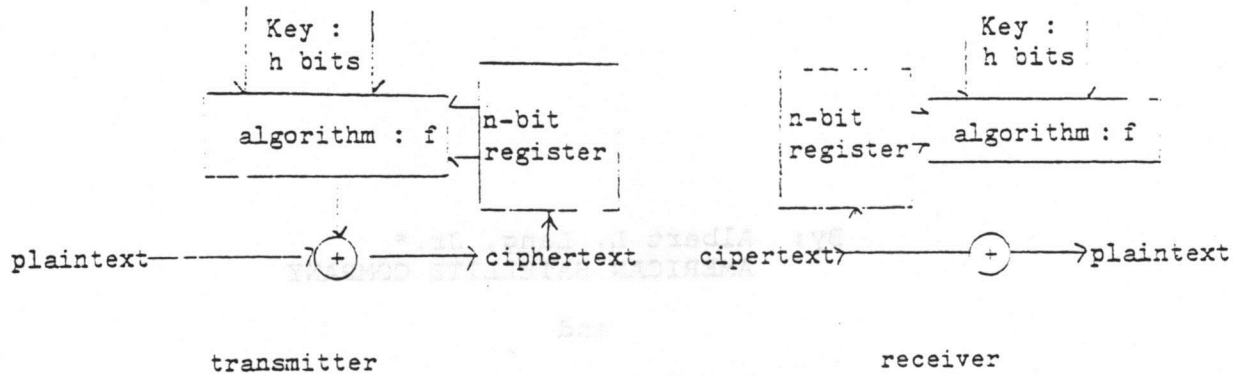
transmission path. This should be clear since decipherment of every message bit within each of these systems is dependent on more than one bit of ciphertext. Thus a single ciphertext bit in error will affect more than one message bit.

If a particular communications system requires a stream cipher then it may, in many situations, be advantageous to design a stream cipher directly rather than utilize a block cipher. Many of the techniques available for stream cipher design can be cheaper and provide greater speed in operation then a block cipher design which may be required to operate in a variety of modes.

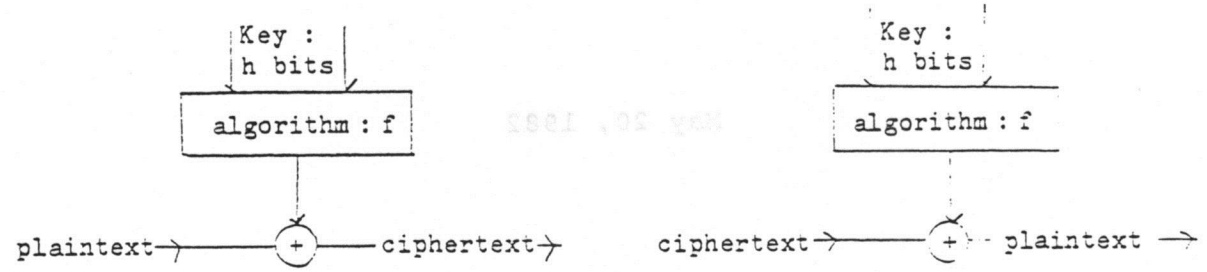
In this paper we will give a few examples of communication systems where stream ciphers are advantageous : namely a telegraph cipher system and a 16kbit/sec digital voice system. We will then consider some of the available techniques for constructing stream cipher algorithms; in particular the requirements of such a system will be discussed and ways of meeting the requirements will be illustrated.



(a)



(b)



(c)

Figure 1

Examples of (a) block cipher (b) cipher feedback (c) stream cipher