

Stream ciphers

Recall that a stream cipher enciphers the i -th plaintext letter (or bit) with the i -th key letter (or bit).

Stream ciphers may be classified as either synchronous or self-synchronous.

Definition. A *synchronous stream cipher* is a stream cipher whose key stream is generated independently from the message.

Example: An LFSR is a key generator for a synchronous stream cipher.

If the transmission of the ciphertext is interrupted, sender and receiver must resynchronize their key streams before continuing.

Definition. A *self-synchronous stream cipher* is a stream cipher whose i -th key is a function of the n previous ciphertext letters, for some n :

$$k_i = f(c_{i-1}, c_{i-2}, \dots, c_{i-n})$$

with initial values for k_1, \dots, k_{n-1} .

If the transmission of the ciphertext is interrupted, the receiver can recover after n correct characters of ciphertext have been received.

Synchronous stream ciphers

Synchronous stream ciphers are often constructed from block ciphers.

Let E be a block enciphering algorithm, for example, $E = DES_K$.

Of course, a block cipher may be used as simply a block cipher. This mode of operation is called Electronic Code Book or ECB. It is simple, but has the disadvantages that repeated plaintext may produce repeated ciphertext, and blocks may be recorded and replayed by an active wiretapper. For example, a wiretapper may record a bank transfer of a large sum of money and replay the amount and source account with the destination account changed to his.

Counter mode uses a block cipher to encipher a counter to produce the key stream.

Output feedback mode (OFB) uses a block cipher to encipher the value in a register, which is loaded with the result.

Do not use a synchronous stream cipher to encipher a file or database. If a character is inserted into the middle of a file, and it is reenciphered with the same key stream, then the rest of the file can be broken easily.

Self-synchronous stream ciphers

As a trivial example, consider a variation of Vigenère which uses each ciphertext letter as the next key letter, (“primed” with ‘X’):

M = AUTOKEY
K = XXRKYIM
C = XRKYIMK

This is trivial to break because there are only 26 possible values for k_1 . But Vigenère discovered that a non-repeating key stream can be generated from the message it enciphers.

In Chaining or Cipher FeedBack Mode (CFB), each ciphertext character is shifted into a shift register. The value in the shift register is enciphered by a block algorithm to produce the next key. If the block algorithm is a nonlinear one, like DES, then the key is not exposed as it was in the trivial example above.

In Block Chaining, before enciphering each plaintext block M_i , some bits of the previous ciphertext block C_{i-1} are inserted into unused bit positions of M_i (or else sequence numbers are inserted as in counter mode). This action protects against insertion, deletion and modification, but reduces the number of bits per block. That is, the ciphertext is longer than the plaintext.

The ultimate form of Block Chaining is Cipher Block Chaining (CBC): $C_i = E(M_i \oplus C_{i-1})$.