3.5 Stream Encryption Approaches

There are two different approaches to stream encryption they are; **synchronous** methods and **self-synchronous** methods.

3.5.1 Synchronous stream ciphers

In a synchronous stream cipher the key stream is generated independently of the message stream. The algorithm that generates the stream must be deterministic so the stream can be reproduced for decryption. This means that if a ciphertext is lost during transmission, the sender and receiver must resynchronize their key generators before they can proceed. Furthermore, this must be done without repeating any part of the key. The starting state of the generator is initialized by a "seed" as illustrated in figure (3.5).

Synchronous stream ciphers have the advantage of not propagating errors. A transmission error effecting one character will not affect subsequent characters. From another point of view; this is a disadvantage in that it is easier for an opponent to modify (without detection) a single ciphertext character.

![Figure (3.5) synchronous stream cipher](image-url)
3.5.2 Self-Synchronous Stream ciphers

A self-synchronous stream ciphers derives each key character from a fixed number $n$ of preceding cipher text character. This is done by using a cipher feed back mode (CFB) because the ciphertext characters participate in the feed back loop. It is some times called chaining, because each ciphertext character depend on preceding cipher-text character (chain) the feed back as shown figure (3.6). The feedback register $R$ is a shift register when each cipher text character $C_i$ is shifted into one end of $R$ immediately after being generated, the character at the other end is discarded. Register $R$ is initialized to the seed 10. During each iteration, the value of $R$ is used as input to a block encryption algorithm (EB), the right most character of the algorithm becomes the next key character. If a ciphertext character is altered or lost during transmission, the receiver's shift register will differ from the transmitter's, and subsequent cipher text will not be correctly deciphered until the error character is shifted out of the register.

Figure (3.6) self-synchronous stream cipher
3.6 Nonlinear Shift Register

Linear feedback shift registers are unsafe because they have relatively small linear complexity, and hence a relatively small fragment of the key streams (LFSR sequence) can be used to obtain the entire sequence by solving a set of linear equations. To increase the linear complexity of LFSR, one or more output sequences of LFSR's are combined with some nonlinear function to produce relatively high linear complexity. For example shift register \textbf{SR1} generates sequence \((S1)\) with sequence length of \(2^n - 1\), and shift register \textbf{SR2} generates sequence \((S2)\) with sequence length of \(2^m - 1\), then the output sequence \((S3)\) will be:

\[S3 = S1 \ast S2\quad \text{with period (sequence length)} = (2^n - 1) \ast (2^m - 1)\]

Key stream generator is a shift register with non linear feedback function, as illustrated in figure (3.8). In this type, one LFSR is used with \(n\)-stages and non-linear feed back functions, the simplest nonlinear function is "AND" function.

![Figure 3.8 Nonlinear Feedback Shift Register with Nonlinear Function](image)

\textbf{Example:}

If we choose R1, R2, R3 with 5,6,7 stages respectively which they are relatively prime the maximal length of the period will be \((2^5 - 1) (2^6 - 1) (2^7 - 1)\)
Geffe, Pless, Hadmard, and Threshold are examples of this type, with the following nonlinear functions:

1. **Geffe**: Nonlinear generator consists of three LFSR of \( \{3, 4, 5\} \) bit stages, with nonlinear function \( (S_1^S_2) \oplus (-S_1^S_3) \) and maximal length of \( (2^3 - 1)(2^4 - 1)(2^5 - 1) = 3255 \) bits.

2. **Hadamard**: a Nonlinear generator consists of two LFSR of \( \{5, 7\} \) bit stages, with nonlinear function \( (S_1^S_2) \) and maximal length of \( (2^5 - 1)(2^7 - 1) = 3937 \) bits.

3. **Threshold**: nonlinear generator consists of three LFSR of \( \{3, 4, 5\} \) bit stages, with nonlinear function \( (S_1^S_2) \oplus (S_1^S_3) \oplus (S_2^S_3) \) and maximal length of \( (2^3 - 1)(2^4 - 1)(2^5 - 1) = 3255 \) bits.