Lecture Three

Stream Cipher and Shift Register

3. Literature Survey of Symmetric Key

Symmetric-key encryption has a very long history, as recorded by Kahn. Most systems invented prior to the 1970s are now of historical interest only. Chapter 2 of Denning is also a good source for many of the more well known schemes such as the Caesar cipher, Vigen`ere and Beaufort ciphers, rotor machines (Enigma and Hagelin), running key ciphers, and so on; see also Davies and Price and Konheim. Beker and Piper give an indepth treatment, including cryptanalysis of several of the classical systems used in World War II. Shannon's paper is considered the seminal work on secure communications. It is also an excellent source for descriptions of various well-known historical symmetric-key ciphers. Hill ciphers, a class of substitution ciphers which substitute blocks using matrix methods. The idea of confusion and diffusion was introduced by Shannon.

Kahn gives 1917 as the date when Vernam discovered the cipher which bears Vernam's name, however, Vernam did not publish the result until 1926. Massey [786] states that reliable sources have suggested that the Moscow-Washington hot-line (channel for very high level communications) is no longer secured with a one-time pad, which has been replaced by a symmetric-key cipher requiring a much shorter key. This change would indicate that confidence and understanding in the ability to construct very strong symmetric-key encryption schemes exists. The one-time pad seems to have been used extensively by Russian agents operating in foreign countries.

The highest ranking Russian agent ever captured in the United States was Rudolph Abel. When apprehended in 1957 he had in his possession a booklet the size of a postage stamp containing a one-time key.

4. Stream Cipher systems

In **stream ciphers**, the message units are bits, and the key is usual produced by a **random bit generator** (see figure (3)). The plaintext is encrypted on a bit-by-bit basis.

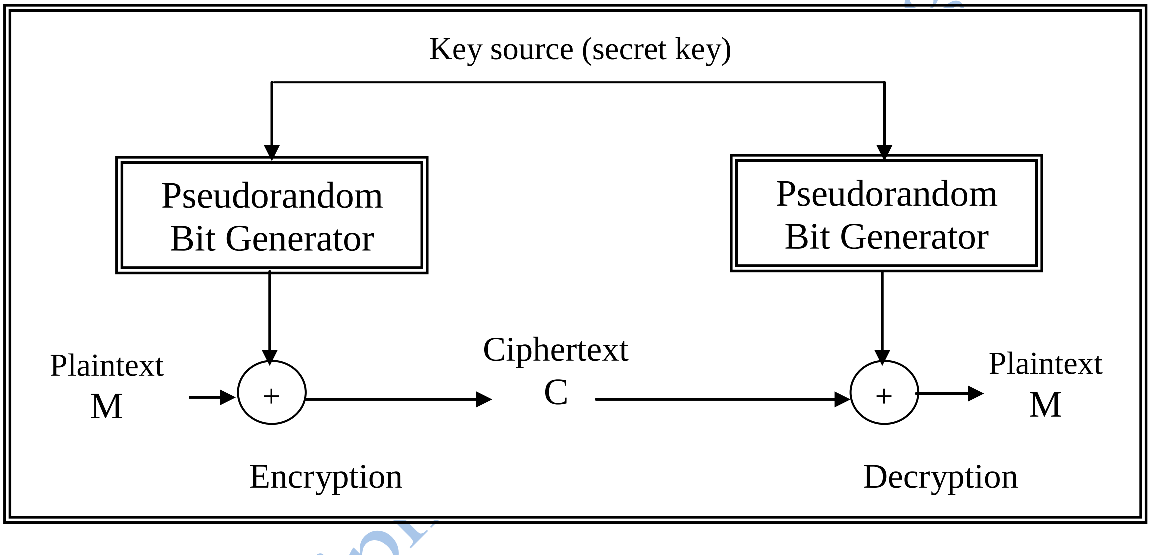

Figure (3) Stream Cipher System.

The key is fed into random bit generator to create a long sequence of binary signals. This "key-stream" k is then mixed with plaintext m, usually by a bit wise XOR (Exclusive-OR modulo 2 addition) to produce the ciphertext stream, using the same random bit generator and seed.