Lecture Three

Stream Cipher and Shift Register

5. Advantages of Stream Cipher

The more common advantages of stream cipher or symmetric key are:

- Stream ciphers are generally faster than block ciphers in hardware, and have less complex hardware circuitry.
- They are also more appropriate, and in some cases mandatory (e.g., in some telecommunications applications), when buffering is limited or when characters must be individually processed as they are received.
- Because they have limited or no error propagation, stream ciphers may also be advantageous in situations where transmission errors are highly probable.
- The security of stream cipher is thus always measured relative to the complexity of exhaustive searching for the correct key. If the complexity of an attack is less than that of the exhaustive search, the cipher is said to be **broken**.
- Another advantage of stream ciphers in military cryptograph is that the cipher stream can be generated in a separate box that is subject to strict security measures and fed to other devices, e.g. a radio set, which will perform the XOR operation as part of their function. The latter device can then be designed and used in less stringent environment.

6. Shift Registers Importance

The Shift Register (SR) used and still be used in many fields, like computers, communications (radar, satellite equipments,…), information theory, coding theory, protocols …etc. It's an important part of many scientific devices design since its light, cheep, and has small size. The importance of SR raised when it's inter many modern and complex fields like communication and data security, so its inter in hardware or software of encryption devices specially the stream cipher system. These small devices are combined with each other and some Boolean functions to design an encryption algorithm to generate long binary sequences. These sequences have good randomness properties work as encryption key combined with plaintext binary digits to be encrypted before send to the receiver to be safe from intruders and attackers. The construction of the encryption algorithm must be designed with much careful. The designer must has good mathematical background before he designs the encryption algorithm to guarantee that the sequence not be estimated or calculated analytically even if the cryptanalyst has some information about the encryption algorithm or part of the encryption key.