Chapter – X

Key Generation

Chapter – X

Key Generation

It is evident that the length of key increases the security and the maximum length may be equal to that of the message. Then the suitable method is to generate the random number which may be used as key each time a message requires to be encrypted and transmitted to the receiver. The receiver with the same key, to be transmitted by the sender, recovers the message from cipher text. The generation of the purely random number is not a very easy task. A good number of literatures are available on the random number generation. These are basically a generation of pseudo-random number.

For any message security we can use anyone of the six encoders to encrypt it by selecting the block length and the number of operations. The algorithms are such that we can extend the block length even equal to the message, though the study of each block length has been restricted to 256 bit. This will give the maximum security. But the computation time will increase at a very high rate and will make impracticable.

Under the condition a proposition is made here to generate the key to be used for the encryption of a message. These three parameters (the selection of encoder, the length of block and the number of operation) are to be sent by the sender through a secured channel and the encrypted message will be sent through insecure channel which can be accessed by the eavesdroppers. This is shown in the following figure 10.

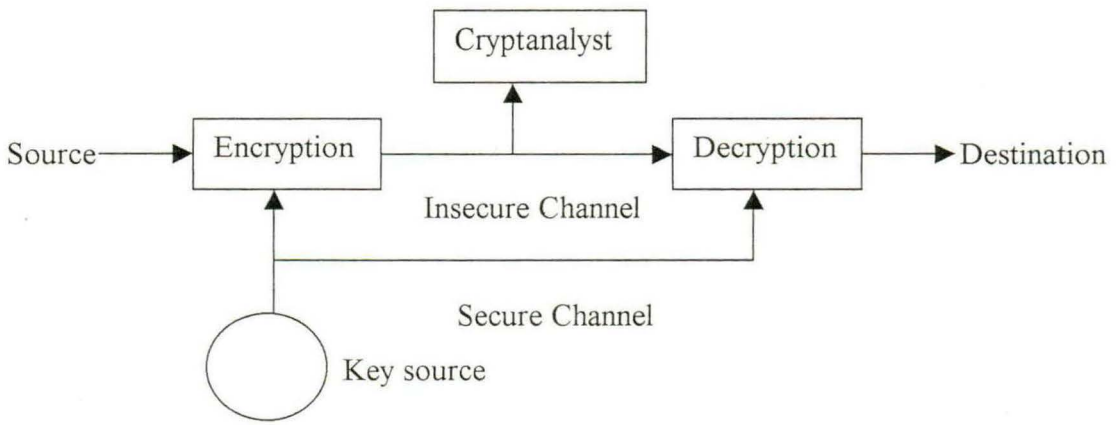

Fig10 : Model of Symmetric Cryptosystem

It is considering that X is the message and Y, the ciphertext generated by the encryption algorithm and key, K. At the receiving end the message is generated from the ciphertext and the securely transmitted key, K. The ciphertext is accessible to the cryptanalysts who can estimate the message and the key.

Here three parameters are variable: **variable technique, variable block length** and **variable operation** made at the time of encryption. The selection of block length and operation are the numbers only chosen at the sending end each time separately in pseudo-random fashion. But the selection of technique is described in the following.

Out of 6 encoders, two are substitution type and four are of transposition type. Each time the technique selected, two encoders in cascade are selected, one from substitution type and the other from transposition type. The message is subjected to the first encoder and then to the second one. There will be 16 possible techniques.

These three variable components of the key will add sufficient security to the message to be transmitted to the receiver. The receiver will receive the ciphertext through the insecure channel and the key, the components of the key is encrypted in 256 bit length block using any of the substitution encoder, through the secure channel. At the receiving end the key components will be recovered from the key and the ciphertext will be decrypted generating the message. This kind of key, different in each session of transmission, is called the session key.

In brute-force attack, it will be a difficult task to the cryptanalysts to find the clue of attack in the variable parameter key of 256 bit length or higher.