Lecture NS2 2018

Chapter 4

1. Describe the model of **Symmetric cryptosystem** (Figs 3.1, 3.2 and pages 86— 87)

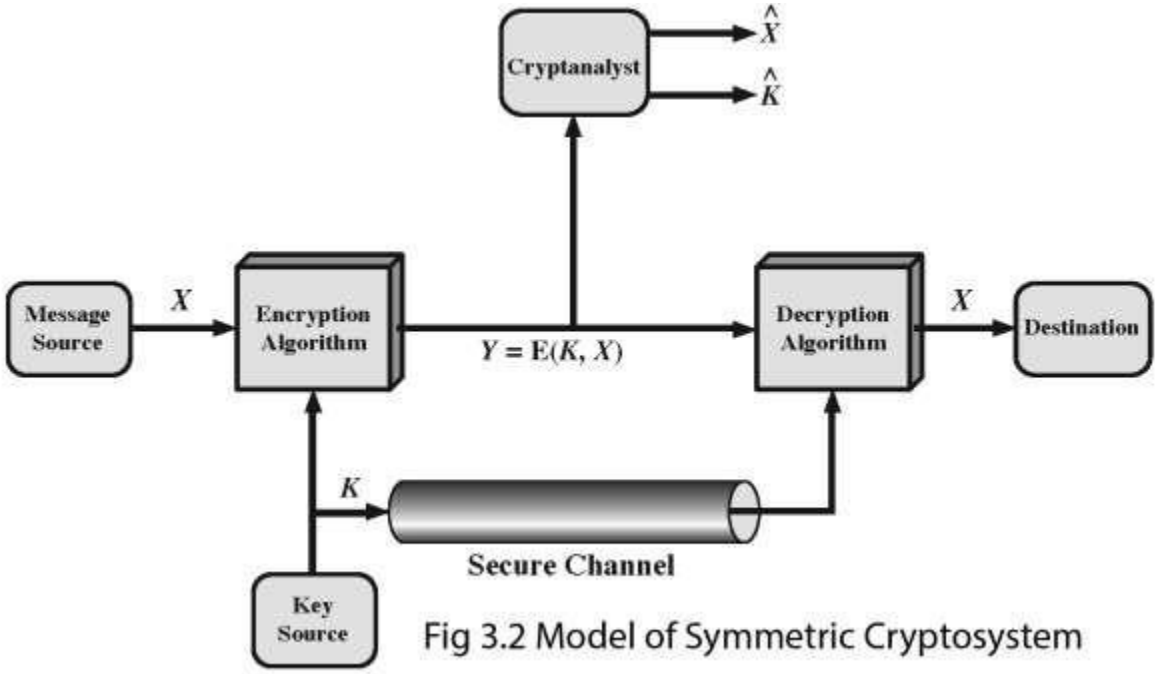

Fig 3.2 Model of Symmetric Cryptosystem

A **message source** produces a message in **plaintext** $X = [X_1, X_2, \ldots X_M]$ consisting of M characters is some finite alphabet.

Traditionally, the alphabet usually consisted of the 26 capital letters. Nowadays, the binary alphabet {0, 1} is typically used.

For **encryption**, an encryption key of the form $K = [K_1, K_2, \ldots, k_J]$ is generated.
If the key is generated at the message source, then it must also be provided to the destination by means of some secure channel. Alternatively, a third party could generate the key and securely deliver it to both source and destination.

With the message *X* and the encryption key *K* as input, the encryption algorithm forms the **ciphertext** $Y = [Y_1, Y_2, \ldots, Y_N]$. We can describe this process as

$$Y = E(K, X)$$

This notation indicates that *Y* is produced by using encryption algorithm E as a function of the plaintext *X*, with the specific function determined by the value of the encryption key *K*.

The intended receiver, in possession of the key, is able to invert the transformation and **decrypt** the cipher text into the plaintext:

$$X = D(K, Y)$$

Note that the **same key** is used for encryption and decryption

An opponent, observing *Y* but not having access to *K* or *X*, may attempt to recover *X* or *K* or both *X* and *K*. It is assumed that the opponent knows the encryption (E) and decryption (D) algorithms. If the opponent is interested in only this particular message, then the focus of the effort is to recover *X* by generating a plaintext estimate X^E . Often, however, the opponent is interested in being able to read future messages as well, in which case an attempt is made to recover *K* by generating an estimate K^E.

Chapter 4

1. Explain how the Feistel cipher works Figure 4.3, 4.4. pages 123 - 129
   Lecture Notes NS2_2_LN, Slides 5, 6, 7, 8,

2. Explain how the Data Encryption Standard works.
   Figure 4.5, Lecture Notes NS2_2_LN, Slides 9, 10, 11,12 13, 14

Chapter 6

3. Advanced Encryption Standard

   Describe the structure of the AES Encryption and Decryption process
   Figure 6.3 and page 177—180
   Lecture Notes NS2_3_LN, Slides 7, 8, 9, 10, 11, 12, 13 , 14
   Lecture Notes NS2_4_LN, Slides 2, 3, 4
   Tutorial Notes NS2_3 and NS2_4