Segment-2

August 19, 2023 5:45 PM

[This note is made After SZK's lectures. For details must follow SZK'z Lectures]

Syllabus of segment 2:

Symmetric Ciphers: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Steganography, Block Ciphers and the Data Encryption.

➢ Basic Concepts Must to know :

- **Cryptography** : The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form .
  [Intelligible message means the message that is understandable by both sender and receiver]
- **Plaintext:** The original intelligible message
- **Cipher text:** The transformed message
- **Cipher:** An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods
- **Key:** Some critical information used by the cipher, known only to the sender& receiver
- **Encipher (encode)/Encryption:** The process of converting plaintext to cipher text using a cipher and a key
- **Decipher (decode)/Decryption:** the process of converting cipher text back into plaintext using a cipher and a key.
- **Cryptanalysis:** The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. Also called code breaking .
- **Cryptology:** Both cryptography and cryptanalysis
- **Code:** An algorithm for transforming an intelligible message into an unintelligible one using a code-book

➢ Cryptography:

- Cryptographic systems are generally classified along 3 independent dimensions:
  1. **Type of operations used for transforming plain text to cipher text.**
     All the encryption algorithms are based on two general principles:
     i) **Substitution:** In which each element in the plaintext is mapped into another element.
     ii) **Transposition:** In which elements in the plaintext are rearranged.
  2. **The number of keys used:**
     i) **symmetric key (or) single key (or) conventional encryption:**

If the sender and receiver uses same key

ii) **Public key encryption/Asymmetric key:**

If the sender and receiver use different keys

3. **The way in which the plain text is processed:**

i) **block cipher:**

A block cipher processes the input and block of elements at a time, producing output block for each input block. [Block by block]

ii) **stream cipher:**

A stream cipher processes the input elements continuously, producing output element one at a time, as it goes along. [Bit by Bit]

➢ Symmetric / CONVENTIONAL ENCRYPTION:

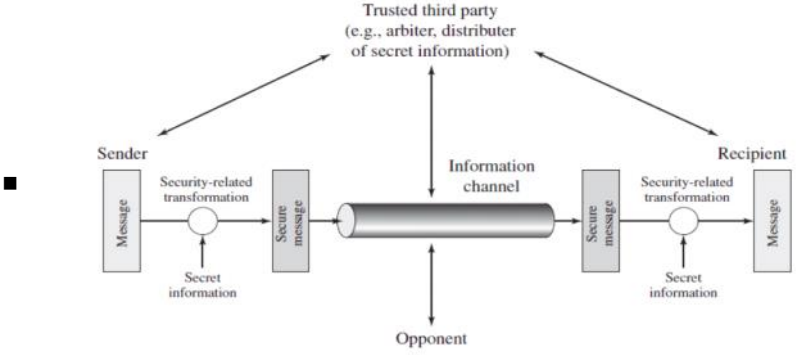
- Sender and recipient share a common key
- Some basic terminologies used:
  - cipher text - the coded message
  - Cipher - algorithm for transforming plaintext to cipher text
  - Key - info used in cipher known only to sender/receiver • encipher (encrypt) - converting plaintext to cipher text
  - decipher (decrypt) - recovering cipher text from plaintext
  - Cryptography - study of encryption principles/methods

- In symmetric key algorithms, the encryption and decryption keys are known both to sender and receiver. The encryption key is shared and the decryption key is easily calculated from it. In many cases, the encryption and decryption keys are the same.

- **Cryptanalysis (code breaking)** - the study of principles/ methods of deciphering cipher text without knowing key

  - Cryptology - the field of both cryptography and cryptanalysis

- A MODEL FOR NETWORK SECURITY:



- Simplified Model of Symmetric Encryption:

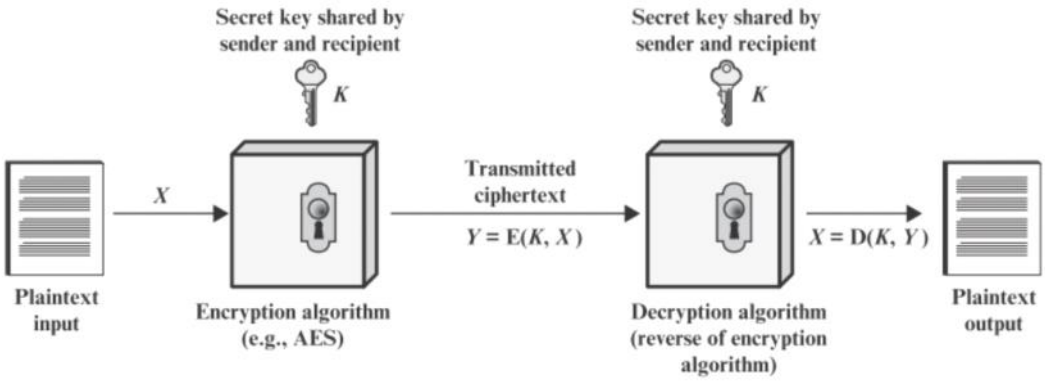


Figure 3.1 Simplified Model of Symmetric Encryption

  - Here the original message, referred to as plaintext, is converted into apparently random nonsense, referred to as cipher text. The encryption process consists of an algorithm and a key. The key is a value independent of the plaintext. Changing the key changes the output of the algorithm. Once the cipher text is produced, it may be transmitted. Upon reception, the cipher text can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption. **The security depends on several factors. First, the encryption algorithm must be powerful enough that it is impractical to decrypt a message on the basis of cipher text alone. Beyond that, the security depends on the secrecy of the key, not the secrecy of the algorithm.**

  - **Two requirements for secure use of Conventional / Symmetric encryption:**
    - A strong encryption algorithm
    - A secret key known only to sender / receiver

- Model of Symmetric Cryptosystem:

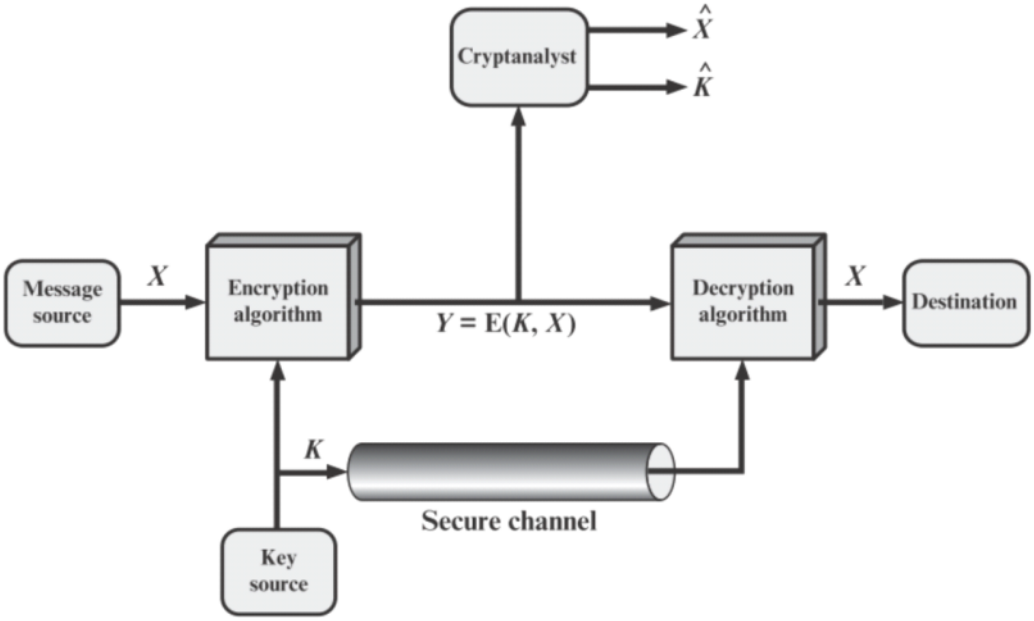


Figure 3.2 Model of Symmetric Cryptosystem

- Y = E(K, X)
  E = encryption algorithm function
  X = Plain text
  K = key
- X = D(K, Y)
  D = Decryption algorithm function
- **assume encryption algorithm is known**
- **implies a secure channel to distribute key**

- A source produces a message in plaintext, X = [X1, X2… XM] where M are the number of letters in the message. A key of the form K = [K1, K2… KJ] is generated. If the key is generated at the source, then it must be provided to the destination by means of some secure channel.

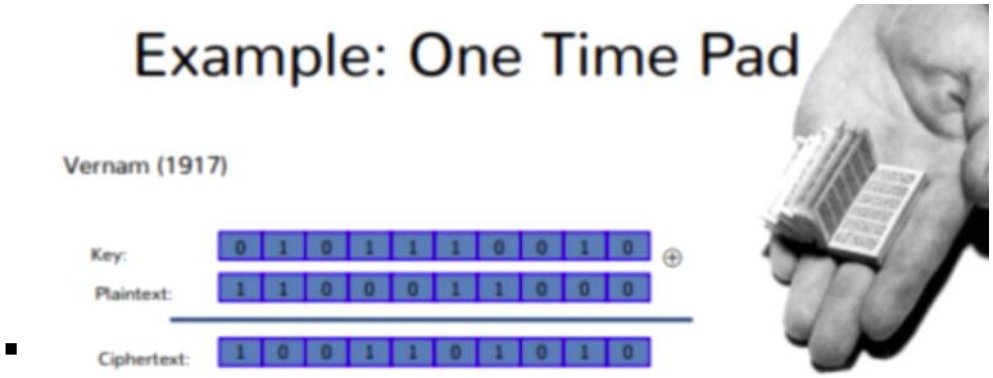
  With the message X and the encryption key K as input, the encryption algorithm forms the cipher text Y = [Y1, Y2, YN]. This can be expressed as Y = EK(X)

  The intended receiver, in possession of the k e y , is able to invert the transformation: X = DK(Y)

  An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both. It is assumed that the opponent knows the encryption and decryption algorithms.

  If the opponent is interested in only this particular message, then the focus of effort is to recover X by generating a plaintext estimate. Often if 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.



- **Encryption:** $c = E_k(m) = m \oplus k$
- **Decryption:** $D_k(c) = c \oplus k = (m \oplus k) \oplus k = m$

➢ CLASSICAL ENCRYPTION TECHNIQUES :

There are two basic building blocks of all encryption techniques: **substitution and transposition**

- **SUBSTITUTION TECHNIQUES**
  A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

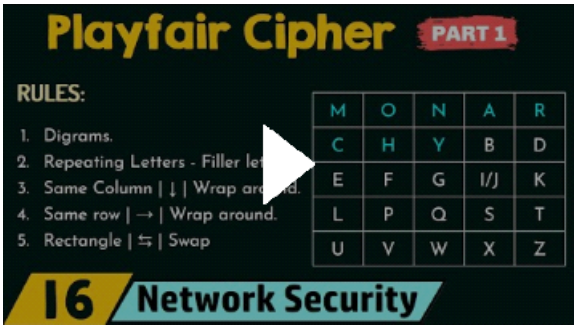
  → Caesar cipher (or) shift cipher :
  - The earliest known use of a substitution cipher and the simplest was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet.
  - e.g., plain text : pay more money
    Cipher text: SDB PRUH PRQHB
    Note that the alphabet is wrapped around, so that letter following „z" is „a".
  - For each plaintext letter p, substitute the cipher text letter c such that
    $C = E(p) = (p+3) \bmod 26$
  - A shift may be any amount, so that general Caesar algorithm is
    $C = E(p) = (p+k) \bmod 26$
  - Where k takes on a value in the range 1 to 25. The decryption algorithm is simply

P = D(C) = (C-k) mod 26

→ Playfair cipher :

- □ Learn from Neso academy

  Playfair Cipher (Part 1)



→ Hill cipher:

- □ Learn from Neso academy

→ Polyalphabetic cipher:

- □ Learn from Neso academy

→ One time pad:

- □ Learn from Neso academy

○ **TRANSPOSITION TECHNIQUES:**

A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

→ Rail fence:

- □ Neso academy

→ Row Transposition Ciphers:

- □ SZK + Neso academy

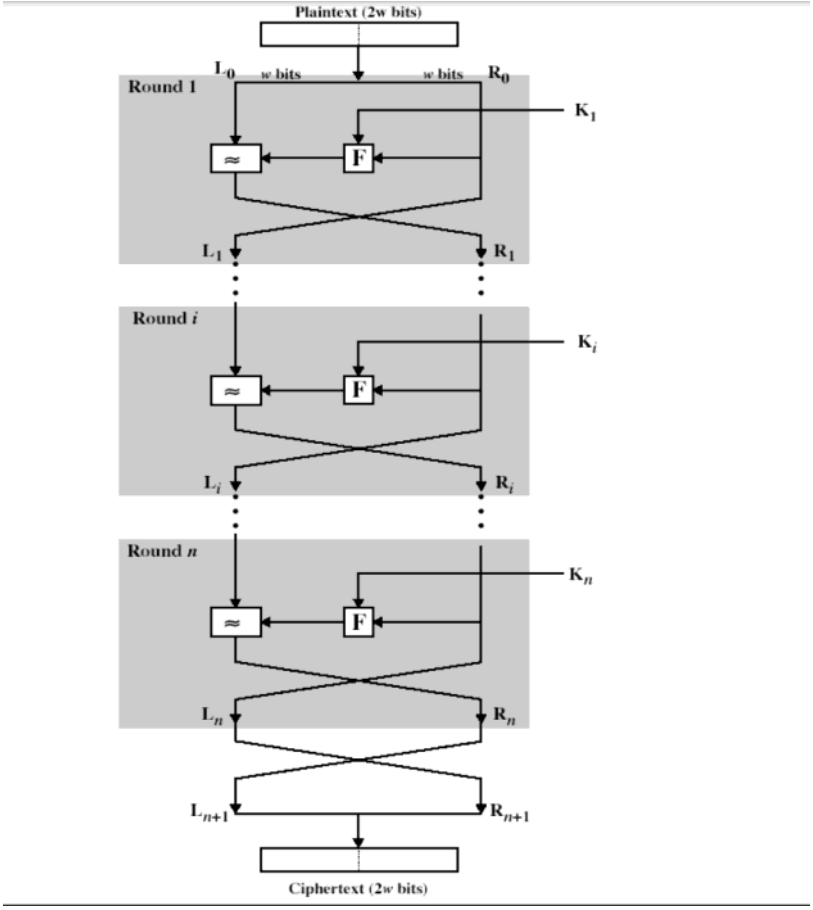
○ **Feistel cipher structure:****[Important cause SZK took a lecture on it]**

The input to the encryption algorithm are a plaintext block of length 2w bits and a key K. the plaintext block is divided into two halves L0 and R0. The two halves of the data pass through „n" rounds of processing and then combine to produce the ciphertext block. Each round „i" has inputs Li-1 and Ri-1, derived from the previous round, as well as the subkey Ki, derived from the overall key K. in general, the subkeys Ki are different from K and from each other.

All rounds have the same structure. A substitution is performed on the left half of the data (as similar to S-DES). This is done by applying a round function F to the

right half of the data and then taking the XOR of the output of that function and the left half of the data. The round function has the same general structure for each round but is parameterized by the round sub key ki. Following this substitution, a permutation is performed that consists of the interchange of the two halves of the data. This structure is a particular form of the substitution-permutation network. The exact realization of a Feistel network depends on the choice of the following parameters and design features:

- **Block size** - Increasing size improves security, but slows cipher
- **Key size -** Increasing size improves security, makes exhaustive key searching harder, but may slow cipher
- **Number of rounds -** Increasing number improves security, but slows cipher
- **Subkey generation -** Greater complexity can make analysis harder, but slows cipher
- **Round function** -- Greater complexity can make analysis harder, but slows cipher
- **Fast software en/decryption & ease of analysis** - are more recent concerns for practical use and testing



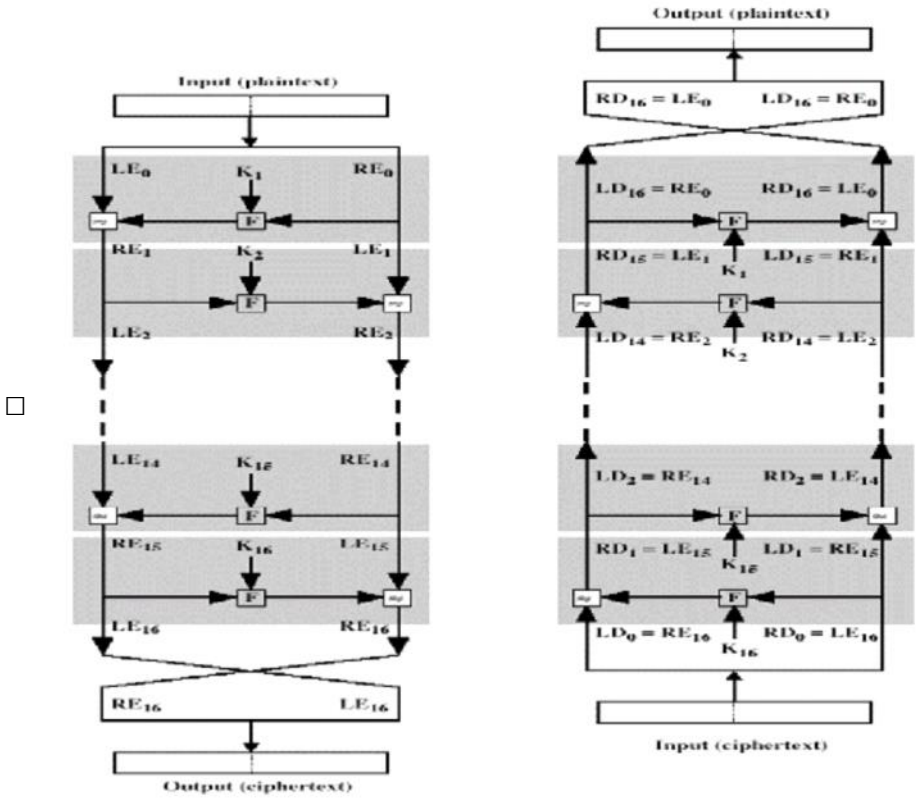


Fig: Feistel encryption and decryption

- Learn the process from online..

○ BLOCK CIPHER PRINCIPLES:

→ Review

[Virtually, all symmetric block encryption algorithms in current use are based on a structure referred to as Fiestel block cipher. For that reason, it is important to examine the design principles of the Fiestel cipher. We begin with a comparison of stream cipher with block cipher

• **A stream cipher** is one that encrypts a digital data stream one bit or one byte at a time. E.g, vigenere cipher. **A block cipher** is one in which a block of plaintext is treated as a whole and used to produce a cipher text block of equal length. Typically a block size of 64 or 128 bits is used.**]**

→ most symmetric block ciphers are based on a Feistel Cipher Structure needed since must be able to decrypt ciphertext to recover messages efficiently. block ciphers look like an extremely large substitution
→ would need table of 264 entries for a 64-bit block
→ Instead create from smaller building blocks
→ using idea of a product cipher in 1949 Claude Shannon introduced idea of substitution-permutation (S-P) networks called modern substitution-transposition product cipher these form the basis of modern block ciphers
→ **S-P networks** are based on the two primitive cryptographic operations we have

seen before:

- □ substitution (S-box)
- □ permutation (P-box)
- □ provide confusion and diffusion of message
- □ **diffusion** – dissipates statistical structure of plaintext over bulk of ciphertext
- □ **confusion** – makes relationship between ciphertext and key as complex as possible

- **DATA ENCRYPTION STANDARD (DES) :**
  - Follow Lecture Video of SZK given in google classroom
- **DES Modes of Use:**
  - Block Modes:
    - → Electronic Codebook Book (ECB)
    - → Cipher Block Chaining (CBC)
  - Stream Modes:
    - → Cipher Feedback (CFB)
    - → Output Feedback (OFB)
- **DES Design Principles:**
  - Learn from online