Block Cipher and Data Encryption Standard

CSS 325

Block Cipher

- **Is an encryption/decryption** scheme in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.
- Many block ciphers have a **Feistel structure**. Such a structure consists of a number of **identical rounds of processing**. In each round, a **substitution** is performed on one half of the data being processed, followed by a **permutation** that interchanges the two halves.
- The original key is expanded so that **a different** key is used for each round.

Feistel Cipher Structure

- Cipher that alternates **substitutions** and **permutations**,
- **Substitution:** Each plaintext element or group of elements **is uniquely replaced by a corresponding ciphertext element or group** of elements.
- **Permutation**: plaintext elements is replaced by a permutation of that sequence. **no elements are added or deleted or replaced** in the sequence, rather the order in which the elements appear in the sequence is changed.

Block cipher principles (Feistel Cipher Structure)

- Virtually all conventional block encryption algorithms, including DES have a structure first described by **Horst Feistel of IBM** in 1973
- Such structure consists of a number of identical rounds of processing. In each round a **substitution** is performed on one half of the data being processed, followed by **permutation** that interchanges the two halves.
- The original key is **expanded** so that different key is used in each round.

Encryption Process in Each Round

- Plaintext P is split into left and right halves

  $P = (L_0, R_0)$

- For each round

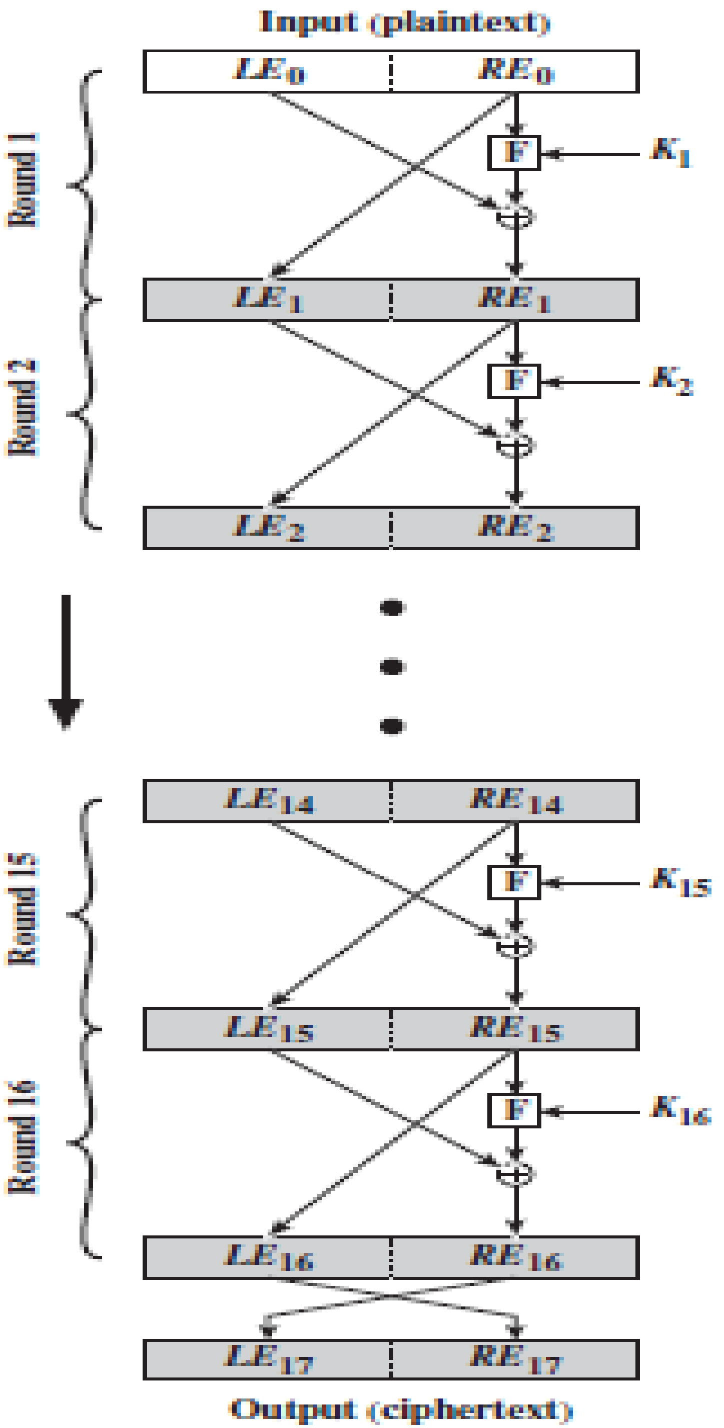
  i = 1,2,3,4,…..n

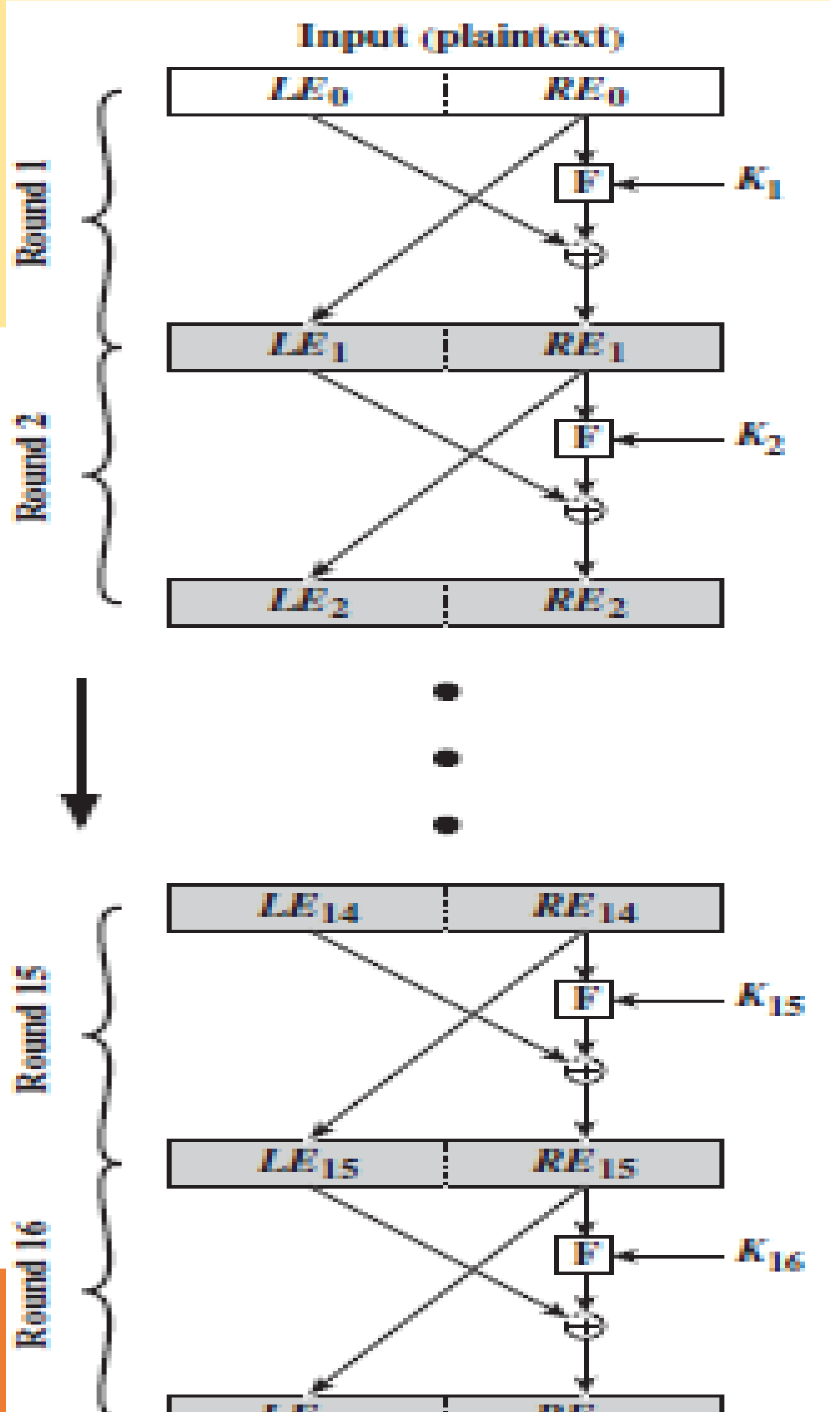
  $L_i = R_{i-1}$ ………………(1)

  $R_i = L_{i-1} \oplus F\ (R_{i-1}, K_i)$….(2)

- Ciphertext ***C*** is the output of final round ***n***

  $C = (L_n, R_n)$





Input (plaintext)
LE_0
RE_0
Round 1
F
K_1
LE_1
RE_1
Round 2
F
K_2
LE_2
RE_2
LE_{14}
RE_{14}
Round 15
F
K_{15}
LE_{15}
RE_{15}
Round 16
F
K_{16}

Decryption Process in Each Round

- Ciphertext **C** is the output of final round **n**

$$C = (L_n, R_n)$$

- For each round

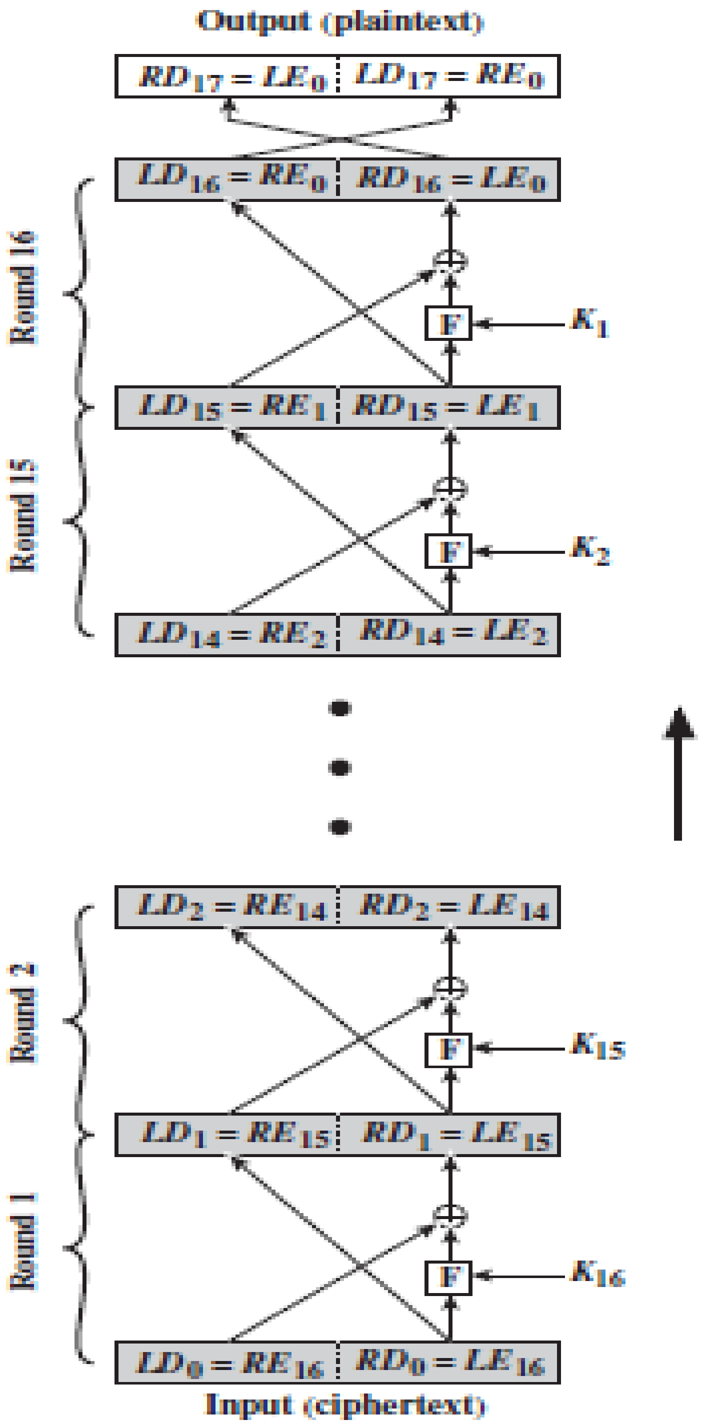
  i = 1,2,3,4,…..n

$$R_{i-1} = L_i \quad \ldots\ldots\ldots\ldots\ldots\ldots(3)$$

$$L_{i-1} = R_i \oplus F(R_{i-1}, K_i)\ldots.(4)$$

- Final result is Plaintext P

$$P = (L_0, R_0)$$



XOR Properties

$$(A \oplus B) \oplus C = A \oplus (B \oplus C)$$

$$A \oplus A = 0$$

$$A \oplus 0 = A$$

Example

- Consider a Feistel Cipher with four rounds where $\mathbf{P=(L_0,R_0)}$ and the corresponding $\mathbf{C=(L_4,R_4)}$. What is the ciphertext **C** interms of $\mathbf{L_0}$, $\mathbf{R_0}$ and the subkey for the given function

$$F(R_{i-1}, K_i) = 0$$

Example 2

- Consider a Feistel Cipher with four rounds where **$P=(L_0,R_0)$** and the corresponding **$C=(L_4,R_4)$.** What is the ciphertext **C** interms of **L_0, R_0** and the subkey for the given function

$$F(R_{i-1},K_i) = R_{i-1} \oplus K_i$$

Feistel Network Parameters

- **Block Size:** Large block size means greater security {64bits, AES use 128 bits}
- **Key Size:** Larger key size means greater security but may decrease encryption/decryption speed
- **Number of Rounds:** multiple rounds offers increasing security
- **Subkey generation algorithm**: greater complexity in this algorithm lead to greater difficulty of cryptanalysis
- **Round function F**: Greater complexity generally means greater resistance

Individual Assignment

- Explain the Structure of Data Encryption Standard (DES) and explain the difference between DES, double DES and Triple DES