FEISTEL STRUCTURE

What is the Design principle of Block cipher?

- Most of the block cipher technique will follow a common structure i.e., FEISTEL STRUCTURE
- **The Feistel structure**, also known as the Feistel network, is a symmetric structure used in the design of many block ciphers.
- Feistel designed a scheme for a block cipher that alternates between **permutation** (rearranging bits) and **substitution** (replacing bits).
- Feistel cipher structure encrypts plain text in several rounds, where it applies **substitution** and **permutation** to the data. Each round uses a different key for encryption, and that same key is used for the decryption process.

  Encryption Inputs:

  - Inputs include:
    - ✓ A plaintext block of length **2w bits**.
    - ✓ A key **K_i**.
  - The plaintext block is split into two halves:
    - ✓ **LE_0** (Left half)
    - ✓ **RE_0** (Right half)
- It was named after Horst Feistel, a cryptographer at IBM. Instead of encrypting the entire data block in one go, the Feistel structure divides the

block into two halves and processes them through multiple rounds. In each round, a round function is applied to one half, and the result is then XORed with the other half.

- The two halves are then swapped and the process repeats for a fixed number of rounds.

Here's a breakdown of the Feistel structure:

Encryption Process:

1. **Divide:** The plaintext block is divided into two equal halves, a left half (L0) and a right half (R0).
2. **Rounds:** For each round i from 1 to n (where n is the number of rounds):
    - A round function F takes the right half of the previous round (Ri−1) and a subkey Ki as input.
    - The output of the round function is XORed with the left half of the previous round (Li−1). This becomes the new right half (Ri).
    - The right half of the previous round (Ri−1) becomes the new left half (Li). Mathematically:

$$Li=Ri\text{-}1$$
$$Ri=Li\text{-}1\oplus F\ (Ri\text{-}1,\ Ki)$$

3. **Combine:** After the final round, the left half (Ln) and the right half (Rn) are concatenated to form the ciphertext.

Note that in some implementations, the halves are swapped after the last round.

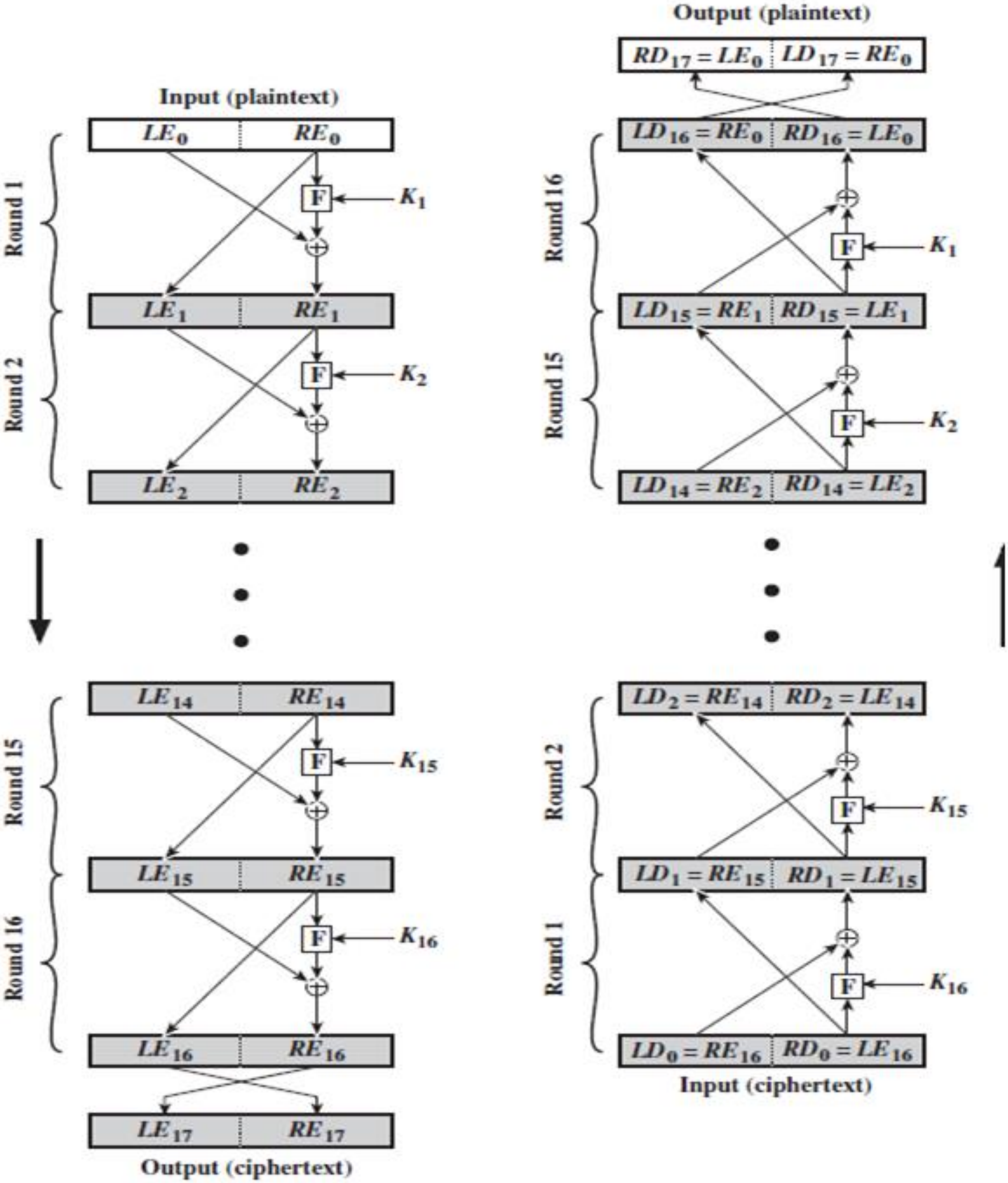
Working of Feistel Cipher Structure

- A ***substitution*** is performed on the left half of the data. This is done by applying a round function F to the right half of the data and then taking the exclusive-OR 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 subkey K_i.
- ***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 (SPN) proposed by Shannon.***

Decryption Process:

The decryption process in a Feistel cipher is remarkably similar to the encryption process. The same round function F is used, but the subkeys are applied in reverse order (Kn, Kn−1, ..., K1).

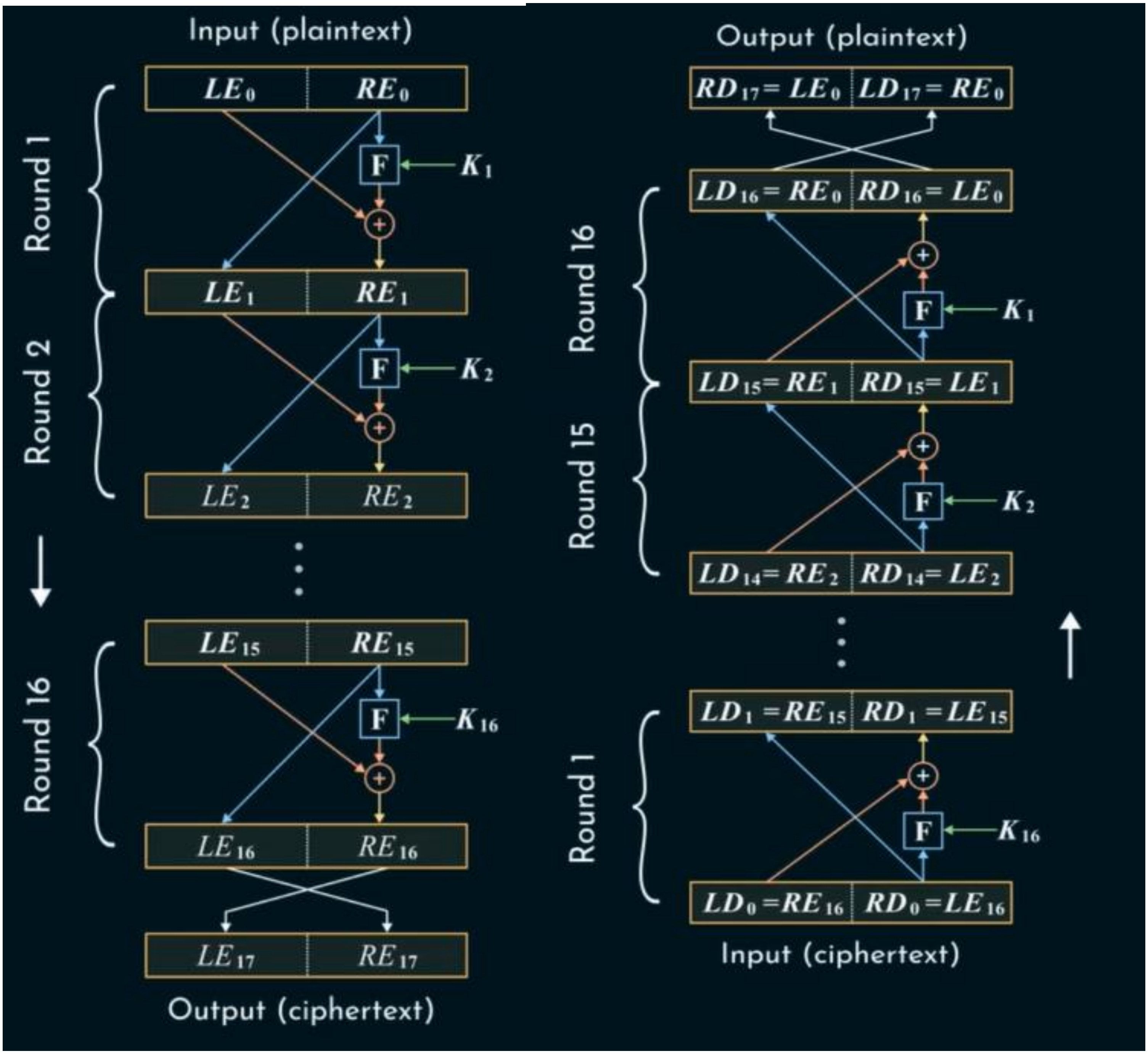
1. The ciphertext block is divided into two halves.
2. For each round i from 1 to n: Ri-1=Li, Li−1=Ri⊕F (Li, Kn−i+1)
3. After the final round, the original plaintext block is obtained (again, considering potential swapping in the last round of encryption).


Output (plaintext)
$RD_{17} = LE_0$
$LD_{17} = RE_0$
Input (plaintext)
LE_0
RE_0
Round 1
F
K_1
LE_1
RE_1
Round 2
F
K_2
LE_2
RE_2
$LD_{16} = RE_0$
$RD_{16} = LE_0$
Round 16
F
K_1
$LD_{15} = RE_1$
$RD_{15} = LE_1$
Round 15
F
K_2
$LD_{14} = RE_2$
$RD_{14} = LE_2$
LE_{14}
RE_{14}
Round 15
F
K_{15}
LE_{15}
RE_{15}
Round 16
F
K_{16}
LE_{16}
RE_{16}
LE_{17}
RE_{17}
Output (ciphertext)
$LD_2 = RE_{14}$
$RD_2 = LE_{14}$
Round 2
F
K_{15}
$LD_1 = RE_{15}$
$RD_1 = LE_{15}$
Round 1
F
K_{16}
$LD_0 = RE_{16}$
$RD_0 = LE_{16}$
Input (ciphertext)

Examples of Ciphers Using Feistel Structure:

Many well-known and widely used block ciphers are based on the Feistel structure, including:

- **DES (Data Encryption Standard):** One of the earliest and most influential block ciphers.
- **Triple DES (3DES):** An enhancement of DES that applies the DES algorithm three times.
- **Blowfish:** A popular and efficient block cipher designed by Bruce Schneier.
- **Twofish:** Another strong block cipher designed as a candidate for AES.
- **FEAL (Fast Data Encipherment Algorithm):** An earlier cipher that used a Feistel structure.


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_{15}
RE_{15}
Round 16
F
K_{16}
LE_{16}
RE_{16}
LE_{17}
RE_{17}
Output (ciphertext)
Output (plaintext)
$RD_{17} = LE_0$
$LD_{17} = RE_0$
$LD_{16} = RE_0$
$RD_{16} = LE_0$
Round 16
F
K_1
$LD_{15} = RE_1$
$RD_{15} = LE_1$
Round 15
F
K_2
$LD_{14} = RE_2$
$RD_{14} = LE_2$
$LD_1 = RE_{15}$
$RD_1 = LE_{15}$
Round 1
F
K_{16}
$LD_0 = RE_{16}$
$RD_0 = LE_{16}$
Input (ciphertext)