FEISTEL STRUCTURE FOR BLOCK CIPHERS

(A cryptographic system based on Feistel structure uses the same basic algorithm for both encryption and decryption.)

Feistel Block Cipher

- Feistel Cipher is not a specific scheme of block cipher. It is a design model from which many different block ciphers are derived.
- DES is just one example of a Feistel Cipher.
- A cryptographic system based on Feistel cipher structure uses the same algorithm for both encryption and decryption.
- Feistel cipher proposed a structure which implements **substitution** and **permutation** alternately to obtain cipher text from the pain text and vice-versa.
- In the Feistel block cipher, each block has to undergo many rounds where each round has the same function.

- As shown in Figure (In next slide), the Feistel structure consists of multiple rounds of processing of the plaintext, with each round consisting of a substitution step followed by a permutation step. ˆ

- The input block to each round is divided into two halves that I have denoted L and R for the left half and the right half.

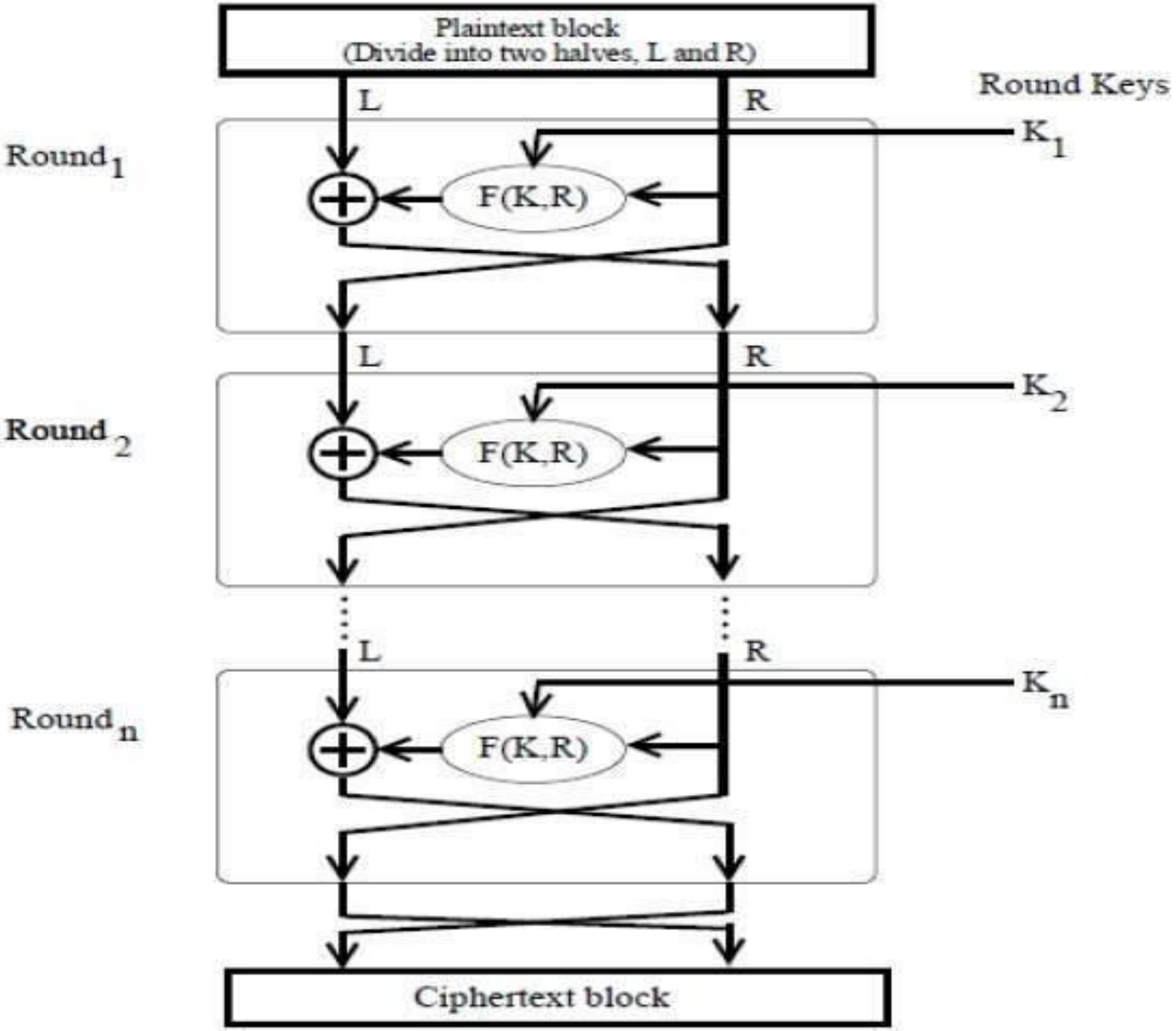

Fig: The Feistel Structure for symmetric key cryptography

Step 1: The plain text is divided into the blocks of a fixed size and only one block is processed at a time. So, the input to encryption algorithm is a plain text block and a key K.

Step 2: The input block to each round is divided into two halves that can be denoted as **L and R** for the left half and the right half.

Step 3: In each round, the right half of the block, R, goes through unchanged. But the left half, L, goes through an operation that depends on R and the encryption key. First, we apply an encrypting function 'f' that takes two input – the key K and R. The function produces the output f(R,K). Then, we XOR the output of the mathematical function with L.

Step 4: Each round executes the same function.(Each round has the same function and after the fixed number of rounds, the plain text block is obtained.)

- **i.e The permutation step at the end of each round consists of swapping the modified L and R. Therefore, the L for the next round would be R of the current round. And R for the next round be the output L of the current round.**

Note: Besides DES, there exist several block ciphers today — the most popular of these being Blowfish that are also based on the Feistel structure.

NOTE:

- Feistel cipher structure has alternate application **substitution** and **permutation** on plain text block to obtain cipher text block.

- Feistel block cipher operates on each block independently.

- The encryption and decryption algorithm in Feistel cipher is the same.

- The **key** used for encryption and decryption is the **same** but the sequence of application of subkey is reversed.

- During encryption a plain text block undergoes multiple rounds. But the function performed in each round is same.

- Generally, 16 rounds are performed in Feistel cipher.

- Typical block size of Feistel cipher is 64-bit but modern block cipher uses 128-bit block.

.