Block and Stream Cipher

By: Dr. Upma Jain

- **Block Cipher** and **Stream Cipher** belongs to the symmetric key cipher. These two block ciphers and stream cipher are the methods used for converting the plain text into ciphertext.
- The main difference between a **Block cipher** and a **Stream cipher** is that a block cipher converts the plain text into cipher text by taking plain text's block at a time. While stream cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.

Difference between Block and Stream cipher

Block Cipher Converts the plain text into cipher text by taking plain text's block at a time.	Stream Cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.
Block cipher uses either 64 bits or more than 64 bits.	While stream cipher uses 8 bits.
The complexity of block cipher is simple.	While stream cipher is more complex.
Block cipher Uses confusion as well as diffusion.	While stream cipher uses only confusion.
In block cipher, reverse encrypted text is hard.	While in-stream cipher, reverse encrypted text is easy.
The algorithm modes which are used in block cipher are ECB (Electronic Code Book) and CBC (Cipher Block Chaining).	The algorithm modes which are used in stream cipher are CFB (Cipher Feedback) and OFB (Output Feedback).
Block cipher works on transposition techniques like rail-fence technique, columnar transposition technique, etc.	While stream cipher works on substitution techniques like Caesar cipher, polygram substitution cipher, etc.
Block cipher is slow as compared to a stream cipher.	While stream cipher is fast in comparison to block cipher.

The feistel Cipher

- In cryptography, a **Feistel cipher** (also known as **Luby–Rackoff block cipher**) is a symmetric structure used in the construction of block ciphers, named after the German-born physicist and cryptographer Horst Feistel.
- He proposed the use of cipher that alternates substituions and permutations.
- **This is the practical application of a proposal by claude Shannon to develop a product cipher that alternates confusion and diffusion functions.**

Confusion

- Confusion means that each binary digit (bit) of the ciphertext should depend on several parts of the key, obscuring the connections between the two.
- The property of confusion hides the relationship between the ciphertext and the key.
- This property makes it difficult to find the key from the ciphertext and if a single bit in a key is changed, the calculation of most or all of the bits in the ciphertext will be affected.
- Confusion increases the ambiguity of ciphertext and it is used by both block and stream ciphers.

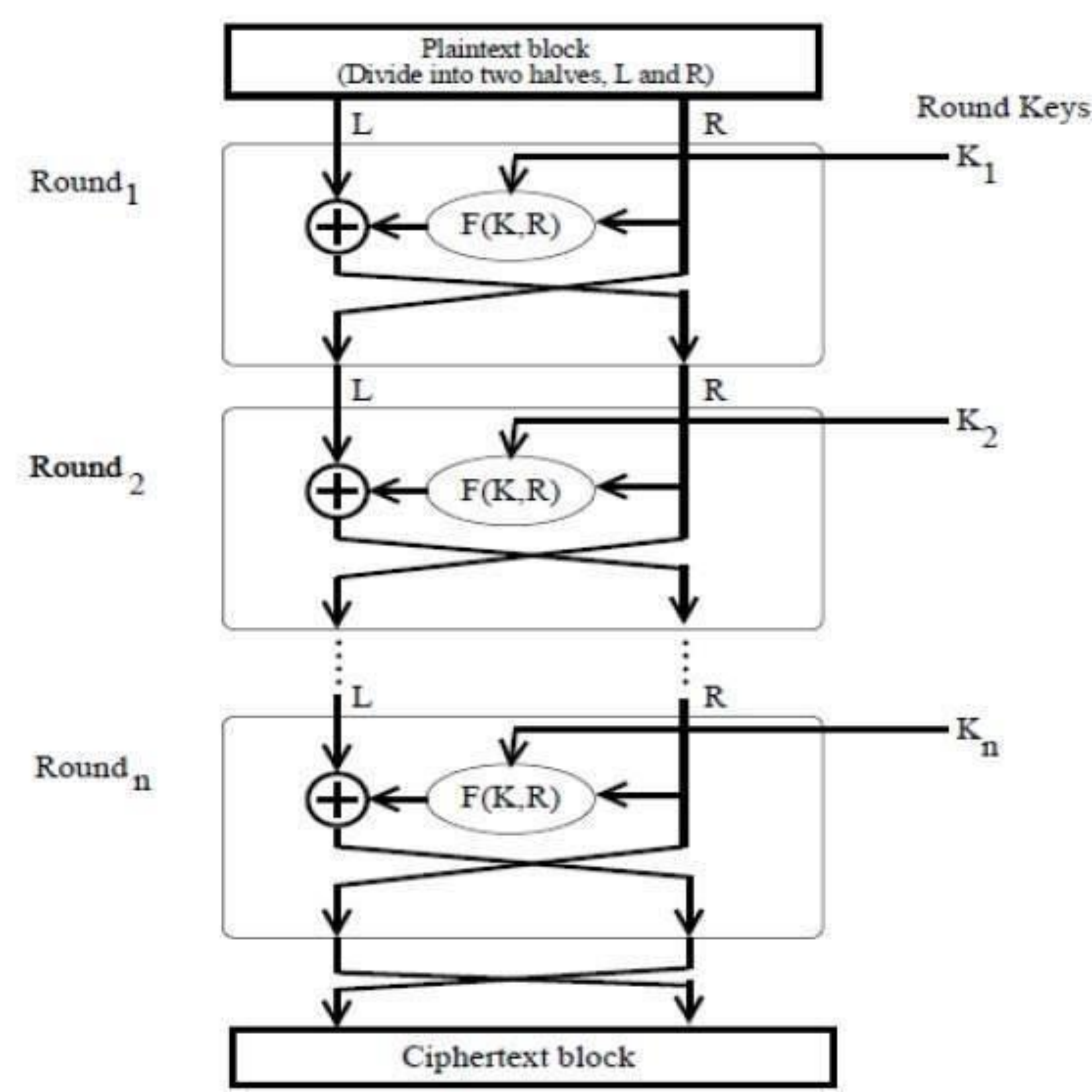
Diffusion

- Diffusion means that if we change a single bit of the plaintext, then about half of the bits in the ciphertext should change, and similarly, if we change one bit of the ciphertext, then about half of the plaintext bits should change.
- The purpose of diffusion is to hide the statistical relationship between the ciphertext and the plain text. For example, diffusion ensures that any patterns in the plaintext, such as redundant bits, are not apparent in the ciphertext.
- Block ciphers achieve this by "diffusing" the information about the plaintext's structure across the rows and columns of the cipher.

Feistel 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.**

- The **encryption process** uses the Feistel structure consisting multiple rounds of processing of the plaintext, each round consisting of a "substitution" step followed by a permutation step.



- 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.
- 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.

- In real implementation of the Feistel Cipher, such as DES, instead of using the whole encryption key during each round, a round-dependent key (a subkey) is derived from the encryption key. This means that each round uses a different key, although all these subkeys are related to the original key.
- The permutation step at the end of each round swaps the modified L and unmodified 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.
- Above substitution and permutation steps form a ‘round’. The number of rounds are specified by the algorithm design.
- Once the last round is completed then the two sub blocks, ‘R’ and ‘L’ are concatenated in this order to form the ciphertext block.

- **The difficult part** of designing a Feistel Cipher is selection of round function ‘f’. In order to be unbreakable scheme, this function needs to have several important properties that are beyond the scope of our discussion.

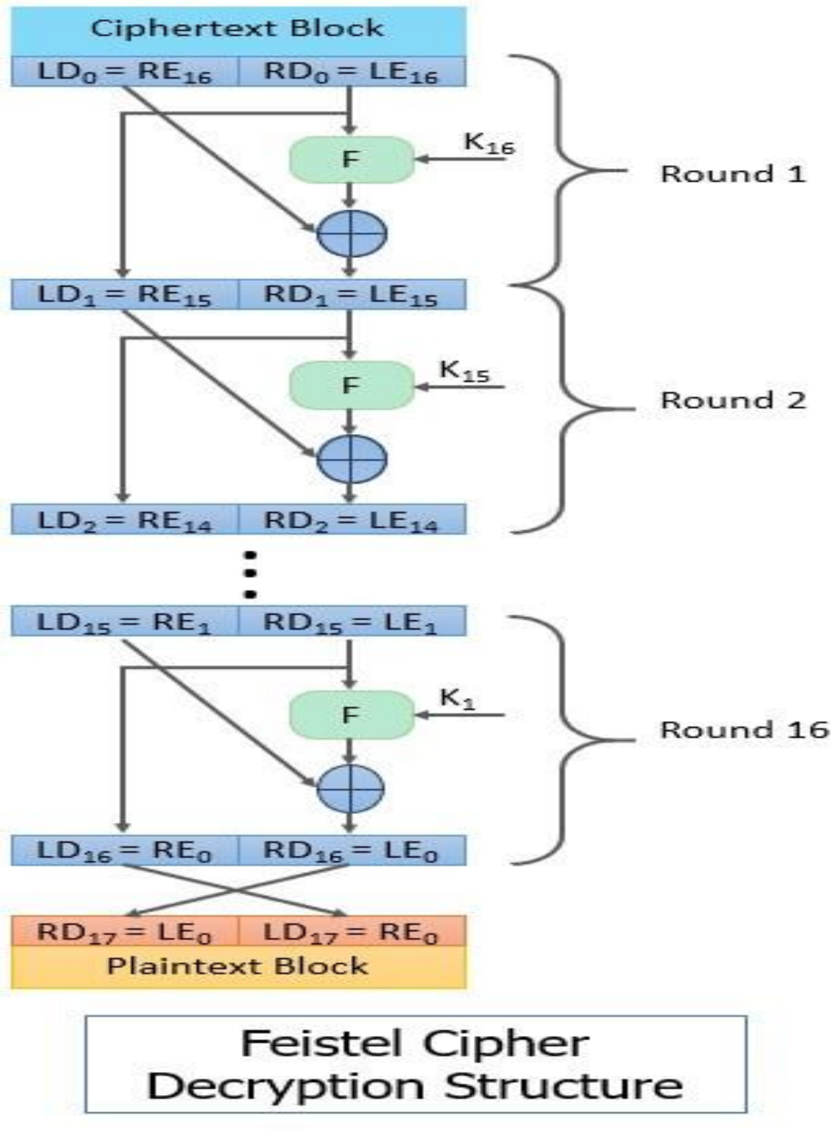
The design features of Feistel cipher that are considered while implementing any block cipher are as follow:

- **Block Size**
  The block cipher is considered more secure if the block size is larger. But the larger block size can reduce the execution speed of encryption and decryption. Generally, the block size of a block cipher is of 64-bit. But, the modern-day block cipher such as AES has 128-bit block size.
- **Key Size**
  The security of block cipher increases with the increasing key size. But the large key size may decrease the speed of encryption and decryption. Earlier the key of 64-bit was considered to adequate. But the modern cipher uses a key of size 128-bit.
- **Number of rounds**
  The number of rounds also increases the security of the block cipher. More are the number of rounds more complex is the cipher.
- **Subkey generation function**
  More the subkey generation function is complex, difficult it is for a cryptanalyst to crack it.
- **Round Function**
  Complex round function enhances the security of the block cipher.
- **Fast Software Encryption/Decryption**
  The block cipher is implemented in a software application to achieve better execution speed.
- **Easy Analysis**
  The block cipher algorithm should be easy to analyze because it would ease in analyzing the cryptanalytic weakness and develop more strength in the algorithm.

Feistel Cipher Decryption

- Feistel Cipher structure does not have a different algorithm for decryption. The encryption and decryption function proposed by Feistel cipher are same with some rules which are as follows:
- The input to the decryption algorithm is a cipher text block produced by the encryption algorithm.
- The sequence of subkeys used in encryption are reversed. The key K_n is used in the first round of decryption, key K_{n-1} in the second round of decryption and so on, until the last round occurs where key K_1 is used.

To understand the structure of decryption, look at the figure below:



Feistel Cipher Decryption Structure

- As you can observe in the figure above the cipher text block has two halves left half (LD_0) and the right half (RD_0). Where $LD_0 = RE_{16}$ and $RD_0 = LE_{16.}$
- Now as in encryption algorithm, the round function is performed on the right half of cipher block with the key K_{16} and the result of the round function is XORed with the left half of the cipher text block.

- Thank You