NOTE:

- **Block cipher** is an encryption and decryption method which operates on the **blocks** of plain text, instead of operating on each bit of plain text separately. Each block is of equal size and has fixed no of bits.

- The generated ciphertext has blocks equal to the number of blocks in plaintext and also has the same number of bits in each block as of plain text.

- Block cipher uses the same key for encryption and decryption.

Block Cipher Design Principles

The design of the block cipher is based on the three principles, which are

- **Number of rounds**
- **Design of function F**
- **Key schedule algorithm**

1. Number of Rounds :

The number of Rounds is regularly considered in design criteria, it just reflects the number of rounds to be suitable for an algorithm to make it more complex, **in DES we have 16 rounds ensuring it to be more secure while in AES we have 10 rounds which makes it more secure.**

2. Design of function F :

The core part of the Feistel Block cipher structure is the Round Function. The complexity of cryptanalysis can be derived from the Round function i.e. the increasing level of complexity for the round function would be greatly contributing to an increase in complexity.

3. Key schedule algorithm :

In Feistel Block cipher structure, each round would generate a sub-key for increasing the complexity of cryptanalysis. The Avalanche effect makes it more complex in deriving sub-key. Decryption must be done very carefully to get the actual output as the avalanche effect is present in it.