SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING(IoT and Cybersecurity Including BCT)

COURSE NAME : FUNDAMENTALS OF CRYPTOGRAPHY 19CS301

II YEAR / III SEMESTER

Unit II-

Topic : FIESTAL CIPHER STRUCTURE

FEISTAL CIPER STRUCTURE

The Feistel cipher structure is a widely used symmetric encryption structure in cryptography. It was introduced by Horst Feistel in the early 1970s and forms the basis for several well-known encryption algorithms, such as DES (Data Encryption Standard).

The Feistel cipher structure operates by dividing the input data into blocks and then subjecting these blocks to a series of rounds, each consisting of two main operations: the "F function" (also known as the "round function") and a permutation (usually swapping and mixing). Here's a high-level overview of how the Feistel cipher structure works:

Block Division: The plaintext (or input) block is divided into two equal-sized halves, often referred to as the left half (L0) and the right half (R0).

Round Operations: A fixed number of rounds are performed, each consisting of the following steps:

The right half of the previous round (Ri-1) becomes the left half for the current round (Li).

The F function is applied to the right half of the previous round (Ri-1) using a round-specific key (Ki) and the result is XORed with the left half of the previous round (Li-1). The output is the new right half (Ri).

The left half of the previous round (Li-1) remains unchanged.

Final Permutation: After all rounds are completed, the final step involves swapping the two halves and applying a final permutation to produce the ciphertext.

The Feistel cipher structure is designed to be reversible, ensuring that decryption is possible using the same algorithm but with the round keys applied in reverse order.

The strength of the Feistel cipher structure lies in its ability to create confusion and diffusion, two essential properties of secure encryption algorithms. The F function introduces confusion by incorporating nonlinear operations and the round keys, while the swapping and mixing in each round provide diffusion by spreading the influence of individual plaintext bits throughout the ciphertext.

It's important to note that while Feistel ciphers offer several advantages, they are not without limitations. For instance, they can be vulnerable to certain types of attacks, such as differential and linear cryptanalysis, if not designed properly.

Overall, the Feistel cipher structure forms the foundation for various encryption algorithms and has played a significant role in the development of modern cryptography.