**UML LAB INTERNAL - II**

**Aim:** To design and implement a lightweight symmetric-key encryption algorithm that incorporates elements of both Feistel and SPN structures, aiming for enhanced security and efficiency.

**Description:**

Cryptography is the practice and study of techniques for secure communication in the presence of adversaries. It enables us to protect sensitive information from unauthorized access and ensure its confidentiality, integrity, and authenticity. Symmetric-key cryptography, one of the fundamental branches of cryptography, utilizes a single secret key for both encryption and decryption. This shared key must be kept confidential, as anyone possessing it can both encrypt and decrypt messages.

This project delves into the design and implementation of a symmetric-key encryption algorithm, employing a blend of two widely recognized network structures: the Feistel network and the Substitution-Permutation Network (SPN). The Feistel network operates by splitting data into halves and applying a round function iteratively, while SPNs focus on confusion and diffusion through techniques like S-box substitutions and permutations. By combining these approaches, the project aims to create a robust and efficient encryption algorithm with enhanced security features.