Page No.
Date

Devanshu Surana
PC-23, Panel C
1032210755

ICS Lab A2.

(A) 4
30/11/25

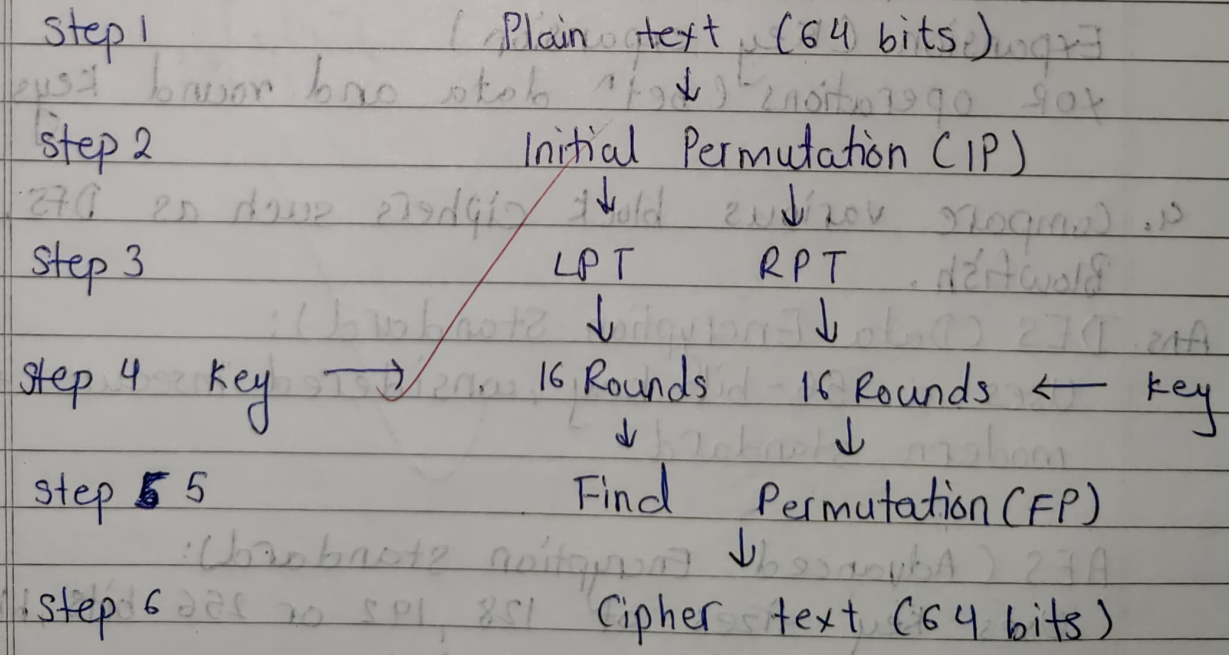
FAQ's

1. What is the concept of Feistel cipher?

Ans. It is a symmetric-key block cipher structure used in modern encryption algorithms. It divides the input data into two halves and applies a series of rounds where one half is modified based on the other half and a round key. This process is repeated multiple times, and the two halves are eventually swapped or combined to produce the ciphertext.

2. Draw and describe DES algorithm.

Ans.



1. IP: the 64-bit plaintext block undergoes an initial permutation that rearranges the bits acc. to table.
2. 16 Rounds of Processing:
   - Expansion, substitution and permutation of 32 bit data.
   - XOR with Round key - combines data with the round subkey.
3. Final Permutation: After the 16 rounds, a final permutation is applied of the data which is the inverse of initial permutation.
4. Ciphertext output: The final output of the final permutation is the ciphertext.

3. List and state broad-level operations used internally in the DFS algorithm.

Ans. Permutations (IP and FP)
Substitution (S-box)
Expansion (Key expansion)
XOR operations (bet^ data and round keys)

4. Compare various block ciphers such as DFS, AES, Blowfish.

Ans. DES (Data Encryption Standard):
Uses a 56-bit key, considered insecure for modern standard

AES (Advanced Encryption standard):
Uses key sizes of 128, 192 or 256 bits, highly secure, and widely adopted.

Page No.
Date

Blowfish:
Uses variable-length key (32 to 448 bits), known for its speed but not widely used in practice.

5. What are the Block, cipher design guidelines.

Ans. The block size should be large enough to prevent attacks that ~~ep~~ exploit statistical pattern in the plaintext.
The s-box used in the cipher should be non-linear to provide confusion
Key sizes should be larger because it resist brute-force attacks.
More rounds increase complexity and security.