Name : Tejas Redkar
PRN : 10322 10937
Panel - C
Roll No : PC-44

ICS Lab A2

A 1/12/23

* FAQ's

Q1) 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 & applies a series of rounds where one half is modified based on the other half & a round key. This process is repeated multiple times & the two halves are eventually swapped or combined to produce the cipher text.

Q2) Draw & describe DES algorithm

Step 1 Plain text (64 bits)

Step 2 Initial Permutation (IP)

Step 3 LPT RPT

Step 4 Key → 16 rounds 16 rounds ← Key

Step 5 Final Permutation (FP)

Step 6 Cipher text (64 bits)

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

Q3) List & state bread-level operations used internally in the DES algorithm.

Ans Permutations (IP & FP)
Substitution (S-box)
Expansion (key expansion)
XOR operations (between data & round keys)

Q4) Compare various block ciphers such as DES, 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 & widely adopted.

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

Q5) What are the Block cipher design guidelines

Ans
- The block size should be large enough to prevent attacks that exploit statistical patterns in the plaintext.
- The S-box used in the cipher should be non-linear to provide confusion
- Key sizes should be larger because it resists bruteforce attacks.
- More rounds increase complexity & security.