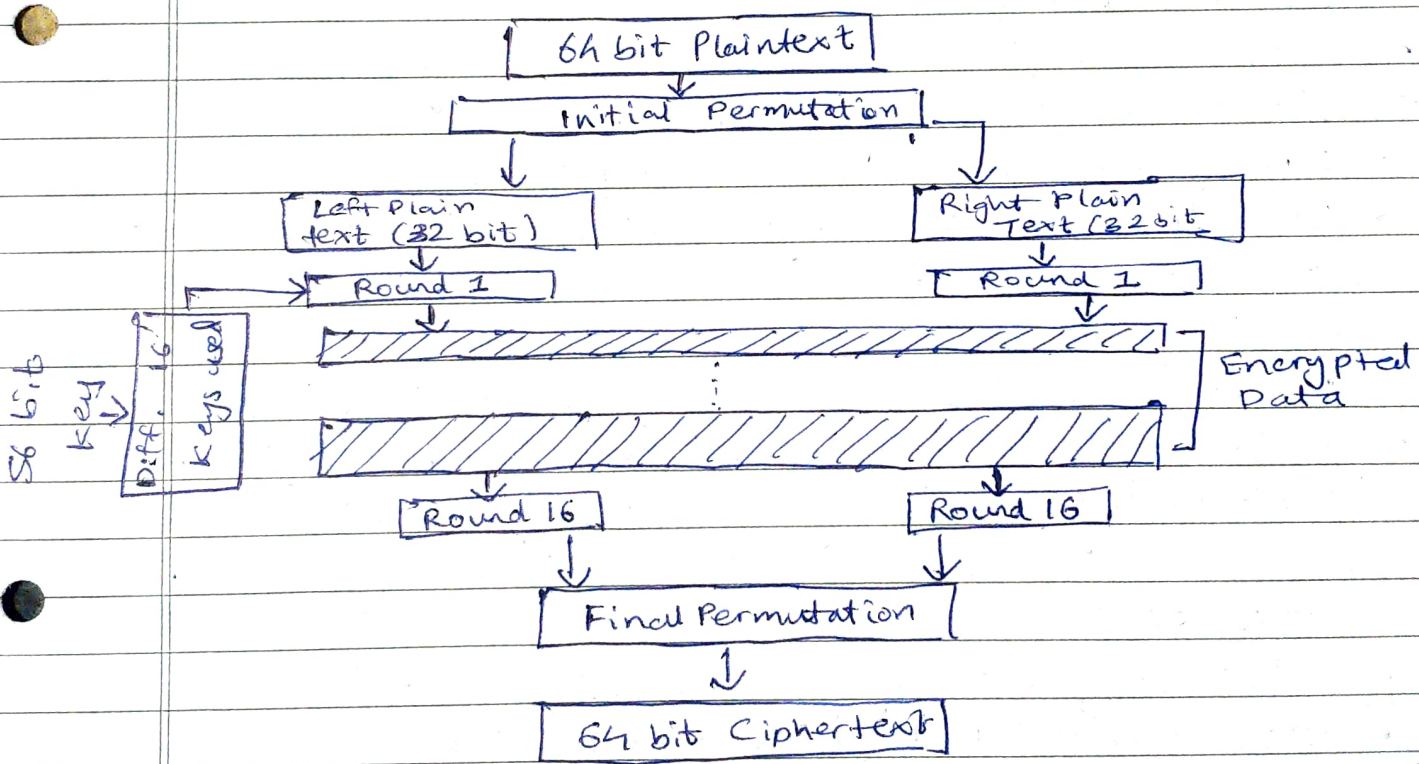
Sudesh Pawar
BE Comp A
F17111037

ICS A3

1) Explain working of DES in detail.

→ DES means Data Encryption Standard. It takes 64 bit plaintext as an input & creates 64bit ciphertext i.e. it encrypts data in block of size 64 bits per block. Divide plaintext message into 64bit block

- At the decryption side DES takes 64 bit ciphertext & creates 64bit plaintext using same 56 bit key. The principle of DES is very simple. Divide plaintext message into block of size 64 bits each which is initial permutation.



- After initial permutation on 64 bit block, the block is divided into 2 halves of 32 bit called left Plaintext & right plaintext
- The left plaintext & right plaintext goes through 16 rounds of encryption process along with 16 different keys for each round. After 16 rounds of encryptions process left plaintext & right plaintext gets combined & final permutation is performed on these combined blocks.

Q.2) Explain Triple DES.

A. Triple Data Encryption Standard (DES) is a type of computerized cryptography where block cipher algorithms are applied 3 times to each data block. The key size is increased in triple DES to ensure additional security through encryption capabilities

- Each block contains 64 bits of data.
- 3 keys are referred to as bundle keys with 56 bits per key.
- There are 3 keying options in data encryption standards:

1) All 3 keys being independent.
2) Key 1 & Key 2 being independent keys.
3) All three keys being identical.

- Key option #3 is known as triple DES.
- The triple DES key length contains 168 bits but the key security falls to 112 bits

Q.3) What is weak key in DES algorithm? Explain with example

Ans. Weak keys are the keys that cause the encryption mode of DES to act identically to the decryption mode of DES.

- DES weak keys produce 16 identical subkeys. This occurs when the key is:
- Alternating ones + zeroes (0x0101010101)
- Alternating 'F' + 'E' (0xFEFEFEFEFE)

→ Using weak keys, the outcome of the Permitted Choice-1 (PC-1) in the DES key schedule leads to round keys being either all 0's, all 1's or alternating 0-1 patterns.