(X) V.V.I Repeated Question

Q:- Draw the general structure of DES and explain Encryption and Decryption? University Question June

DES (Data Encryption Standard)

→ The Data Encryption standard (DES) is a Symmetric-Key block cipher.

→ DES is published by the National Institute of Standard and Technology (NIST) in the year 1977

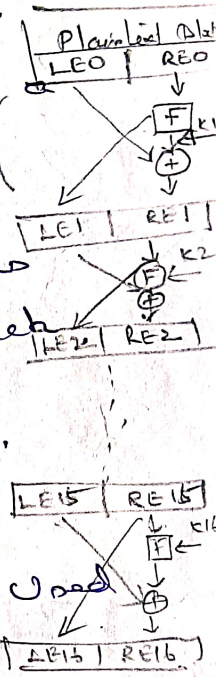
→ It is the based on the Feistel multiple rounds of processing of plain text each round structure in which the plaintext is seperated into two halves.

→ It takes input as 64-bit plaintext and 56-bit key to produce 64-bit ciphertext.

→ Before proceeding, the entire plain text is seperated into two pieces of 32 bits each

→ Some operation is done on each portion.

→ Each pieces goes through 16 rounds of operation before the final permutation is used to obtain the 64-bit ciphertext.



DES Algorithm steps:-

1) In the first step, the 64-bit plain text block is handed over to an initial Permutation (IP) function.

2) The initial permutation is performed on Plain text.

3) Next, the initial Permutation (IP) produces two halves of the permuted block.

Say: Left plain Text (LPT 32 bit)

Right plain Text (RPT 32 bit)

4) Now each LPT and RPT go through 16 rounds of encryption process.

5) In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the Combined block.

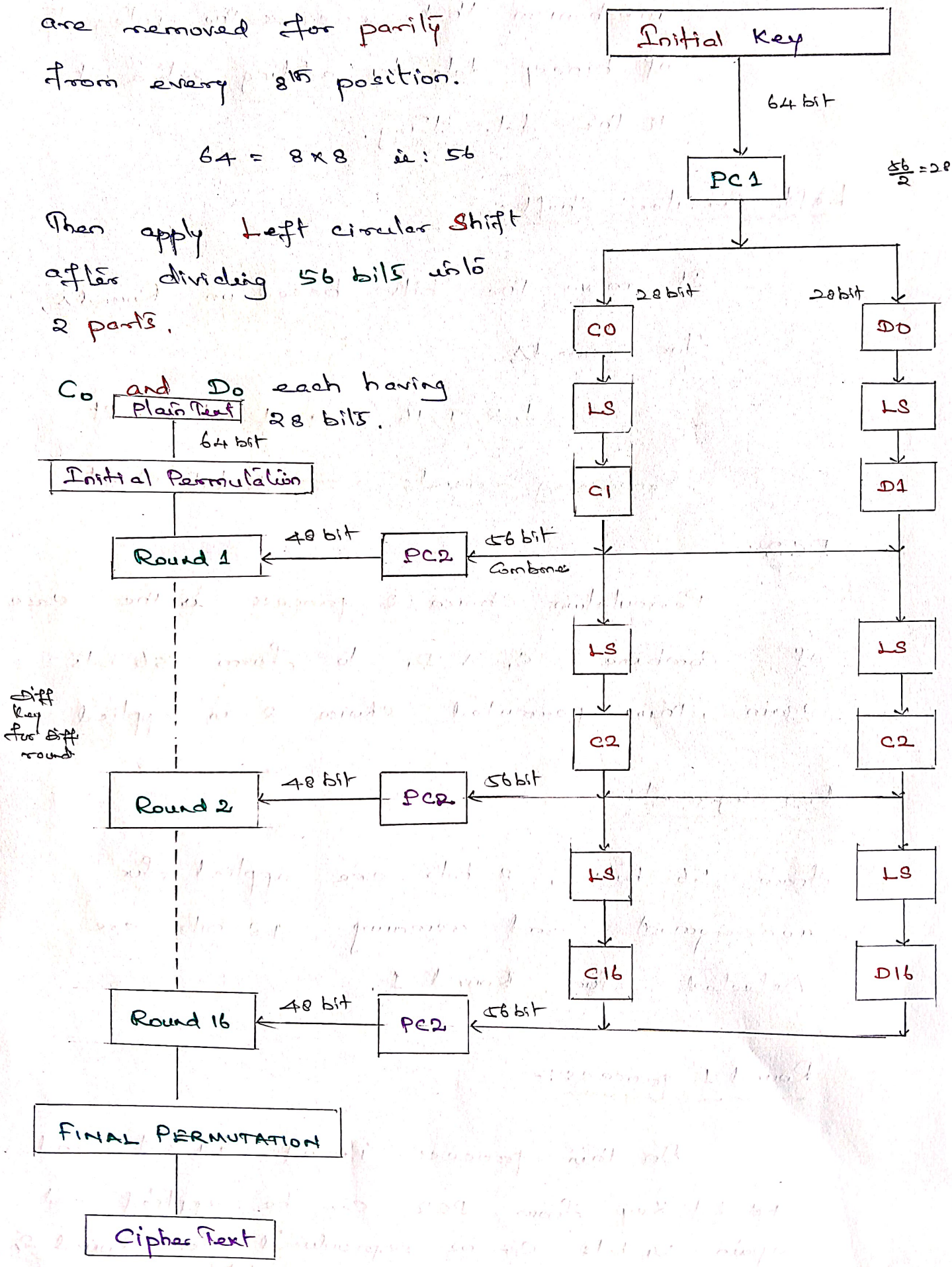
6) The result of this process produces 64-bit Ciphertext.

Initially, 64 bits, 8 bits are removed for parity from every 8th position.

$64 = 8 \times 8$ i.e. 56

Then apply Left circular shift after dividing 56 bits into 2 parts.

C_0 and D_0 each having 28 bits.



Parity :- Parity refers to an error-detection mechanism that ensures the integrity of binary data by adding extra bit to the data string.

Left Circular shift :

It move the bits based on Rounds,

For rounds,

1, 2, 9, 16 —— 1 bit shift

Remaining rounds —— 2 bit shift

PC2 :

Permutation Choice 2 process is the case of Combine C_1 & D_1 to form 56 bits again, this permuted choice 2 is applied.

Rearrangement :-

From 56 bits, 8 bits are applied for rearrangement and remaing 48 bits are selected for Round 1.

Round 1 process :-

On this process i/p of 64 bit and 48 bit Key from PC2 can be applied and again 64 bits can be reproduced for Round 2.

ie:- i/p - 64 bit + 48 bit key