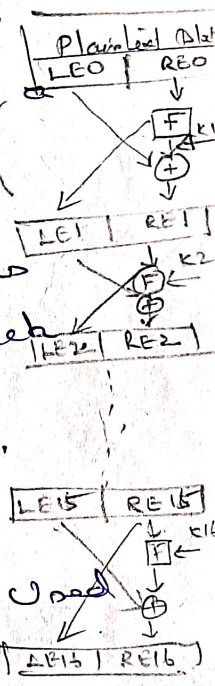


University Questions Forum (Qn:- Draw the general structure of DES and explain Encryption and Decryption?)

(\*) W.V.V. Reproduced Questions

# DES (Data Encryption Standard)

- The Data Encryption Standard (DES) is a Symmetric-Key block cipher.
- DES is published by the National Institute of Standards and Technology (NIST) in the year 1977
- It is based on the Feistel structure in which the plaintext is separated into two halves.
- It takes input as 64-bit plaintext and 56-bit key to produce 64-bit ciphertext.
- Before processing, the entire plain text is separated into two pieces of 32 bits each.
- Some operation is done on each portion.
- Each piece goes through 16 rounds of operation before the final permutation is obtained the 64-bit ciphertext.



## DES Algorithm steps:-

- 1) In the first step, the 64-bit plain text block is handled 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)

Initial Key

64-bit Key

Permutation Choice 1

8- Permutation choice 1  
 8- Permutation choice 2  
 8- Permutation choice 3  
 8- Permutation choice 4  
 8- Permutation choice 5  
 8- Permutation choice 6  
 8- Permutation choice 7  
 8- Permutation choice 8  
 8- Permutation choice 9  
 8- Permutation choice 10  
 8- Permutation choice 11  
 8- Permutation choice 12  
 8- Permutation choice 13  
 8- Permutation choice 14  
 8- Permutation choice 15  
 8- Permutation choice 16  
 8- Permutation choice 17  
 8- Permutation choice 18  
 8- Permutation choice 19  
 8- Permutation choice 20  
 8- Permutation choice 21  
 8- Permutation choice 22  
 8- Permutation choice 23  
 8- Permutation choice 24  
 8- Permutation choice 25  
 8- Permutation choice 26  
 8- Permutation choice 27  
 8- Permutation choice 28  
 8- Permutation choice 29  
 8- Permutation choice 30  
 8- Permutation choice 31  
 8- Permutation choice 32

8- Permutation choice 1  
 8- Permutation choice 2  
 8- Permutation choice 3  
 8- Permutation choice 4  
 8- Permutation choice 5  
 8- Permutation choice 6  
 8- Permutation choice 7  
 8- Permutation choice 8  
 8- Permutation choice 9  
 8- Permutation choice 10  
 8- Permutation choice 11  
 8- Permutation choice 12  
 8- Permutation choice 13  
 8- Permutation choice 14  
 8- Permutation choice 15  
 8- Permutation choice 16  
 8- Permutation choice 17  
 8- Permutation choice 18  
 8- Permutation choice 19  
 8- Permutation choice 20  
 8- Permutation choice 21  
 8- Permutation choice 22  
 8- Permutation choice 23  
 8- Permutation choice 24  
 8- Permutation choice 25  
 8- Permutation choice 26  
 8- Permutation choice 27  
 8- Permutation choice 28  
 8- Permutation choice 29  
 8- Permutation choice 30  
 8- Permutation choice 31  
 8- Permutation choice 32

64-bit Plain Text

Initial Permutation

32-bit RPT

32-bit LPT

Round 1

Round 2

48 bit

48 bit

Round 16

Final Permutation

64-bit Cipher Text

Left Circular Shift

Left Circular Shift

Permutation choice 2

Permutation choice 2

Permutation choice 2

Left Circular Shift

- 1) Now each LPT and RPT go through 16 rounds of encryption process.
- 2) In the end, LPT and RPT are rejoined and a final permutation (FP) is performed on the combined block.
- 3) The result of this process produces 64-bit Cipher Text.

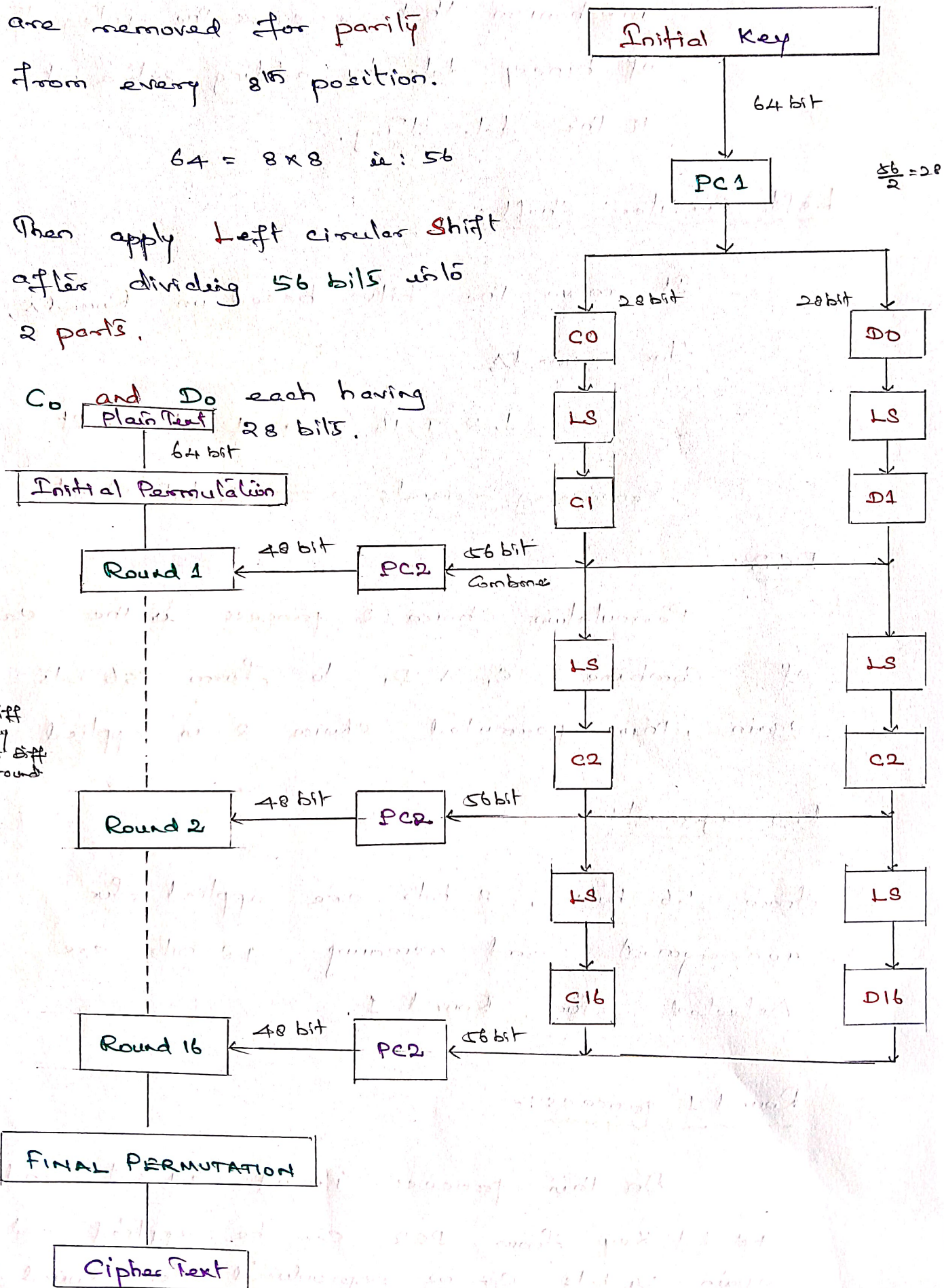
Data Encryption Standard (DES)

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

$$64 = 8 \times 8 \quad \therefore 56$$

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

$C_0$  and  $D_0$  each having Plain Text 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 moves 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, 4 D, to form 56 bits again, this permuted choice 2 is applied.

Rearrangement :-

From 56 bits, 8 bits are applied for rearrangement and remaining 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.  
i.e. :- i/p - 64 bit + 48 bit key