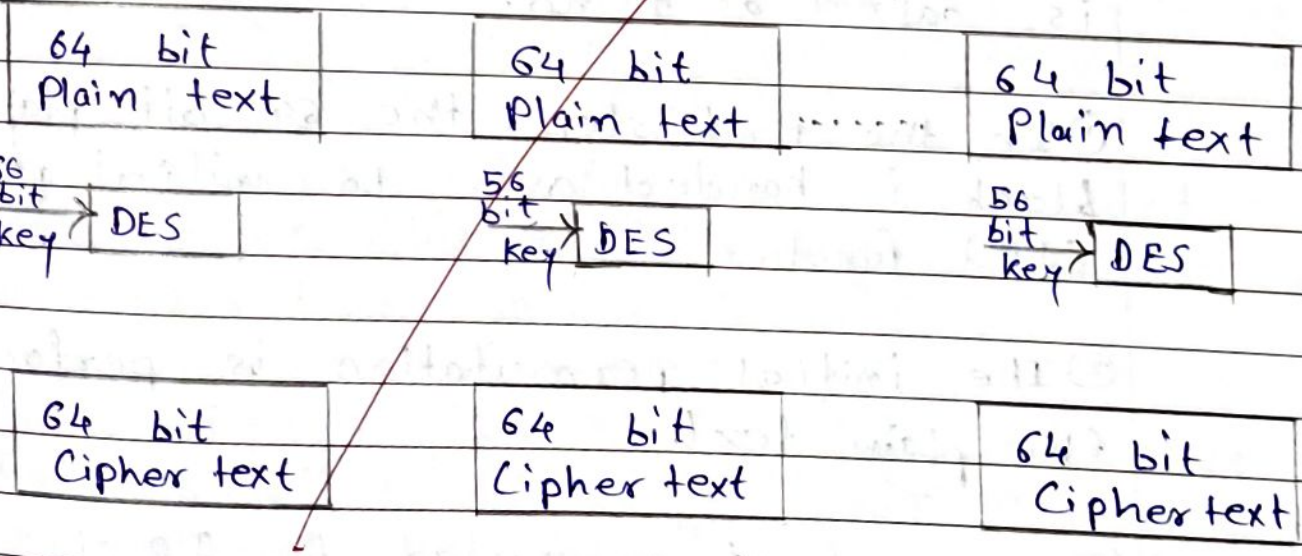
Experiment No. 05

Aim: Study of encryption of long messages using various modes of operation using DES.

Theory:

Data Encryption Standard (DES):-

* DES is block cipher. It encrypts data in blocks of 64 bit each. 64 bit plain text goes as an input to DES, which produces 64 bit cipher text. 56 bit key is used in DES.



* The initial key consists of 64 bits, however even before the actual DES process starts every 8^{th} bit of the key is discarded to produce a 56 bit key.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64

* Thus discarding the every 8th bit of the key produces a 56 bit key from the original 64 bit key.

* DES is based on the two fundamental attributes of cryptography - substitution and transposition.

* DES consists of 16 steps, each of which is called as round.

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

② The initial permutation is performed on the plain text.

③ The output generated by IP is divided into two blocks LPT and RPT.

④ Now each LPT and RPT go through 16 rounds of encryption process, each with its own key.

⑤ Finally LPT and RPT are rejoined and the final permutation (FP) is performed on the combined block.

⑥ The result of this process produces 64 bit Cipher text.

⇒ Initial Permutation :- Initial Permutation (IP) is performed only once and it happens before the first round.

IP Table

30	11	21	42	36	57	2	58	27	49	14	40	4	33	62	26
43	22	1	12	31	23	13	41	37	3	47	53	50	15	61	39
38	5	44	35	56	6	51	17	55	25	32	7	16	54	29	48
46	18	52	8	45	24	59	19	9	63	34	60	28	10	64	20

* The value 30 in the 1st cell indicates that the 1st bit of the original PT message is replaced by the 30th bit.

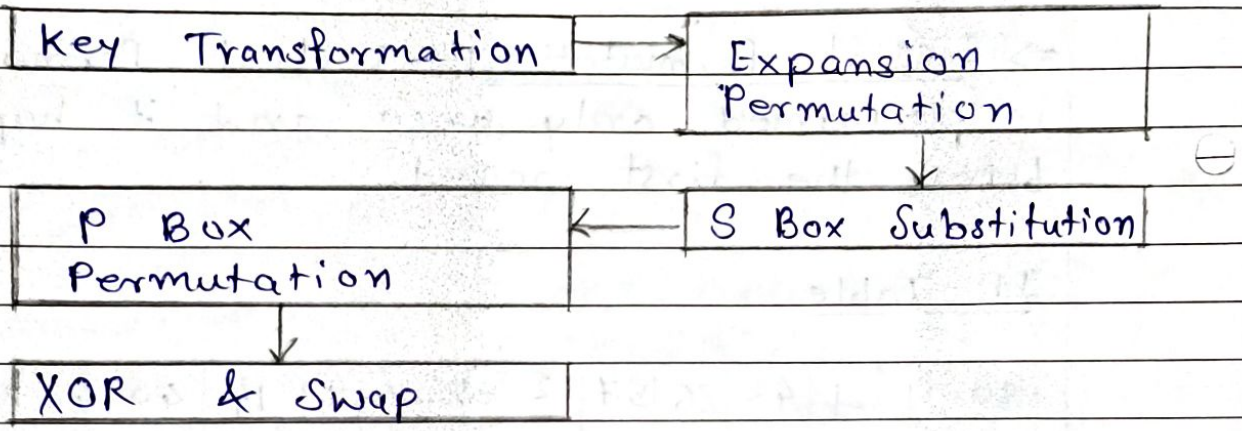
* The value 11 in the 2nd cell indicates that the 2nd bit of the original PT message is replaced by the 11th bit and so on.

* This is nothing but jugglery of bit positions of the original PT block.

* After the initial Permutation is performed the 64 bit permuted text block is divided

into two half blocks.

* Each half block consists of 32 bits. We call the left block as LPT and right block as RPT. 16 rounds are performed on these two blocks.



Steps -

(1) Key Transformation -

* The initial key was of size 64 bit which is already transformed into a 56 bit key by discarding every 8th bit.

* From this 56 bit key, a different 48 bit sub key is generated during each round using a process called key Transformation.

* This 56 bit key is divided into two halves each of 28 bits. These halves are circularly shifted left by one or two positions depending on the round.

Round No ⇒ 1, 2, 9 and 16 ⇒ Circular left shift by only one position

For all other Rounds ⇒ Circular left shift by two positions.

* After an appropriate shift, 48 bits are selected from these 56 bits. This is called as compression permutation.

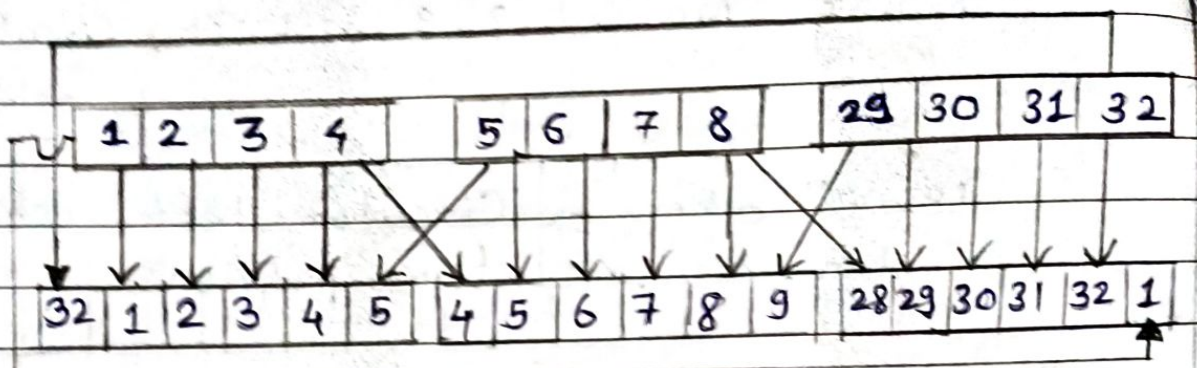
* Because of this compression permutation technique, a different subset of key bits is used in each round. That makes DES more difficult to crack.

② Expansion Permutation:-

* After the initial permutation we have divided the plaintext data into 2 halves each of 32 bit and called it as LPT and RPT. during this expansion permutation process RPT is expanded from 32 bit to 48 bits.

* The 32 bit RPT is divided into 8 blocks each block consisting of 4 bits.

* Now each of these 4 bits block is expanded into corresponding 6 bits block.



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

* So, the 56 bit key is compressed into 48 bit key and 32 bit RPT is expanded to 48 bit RPT.

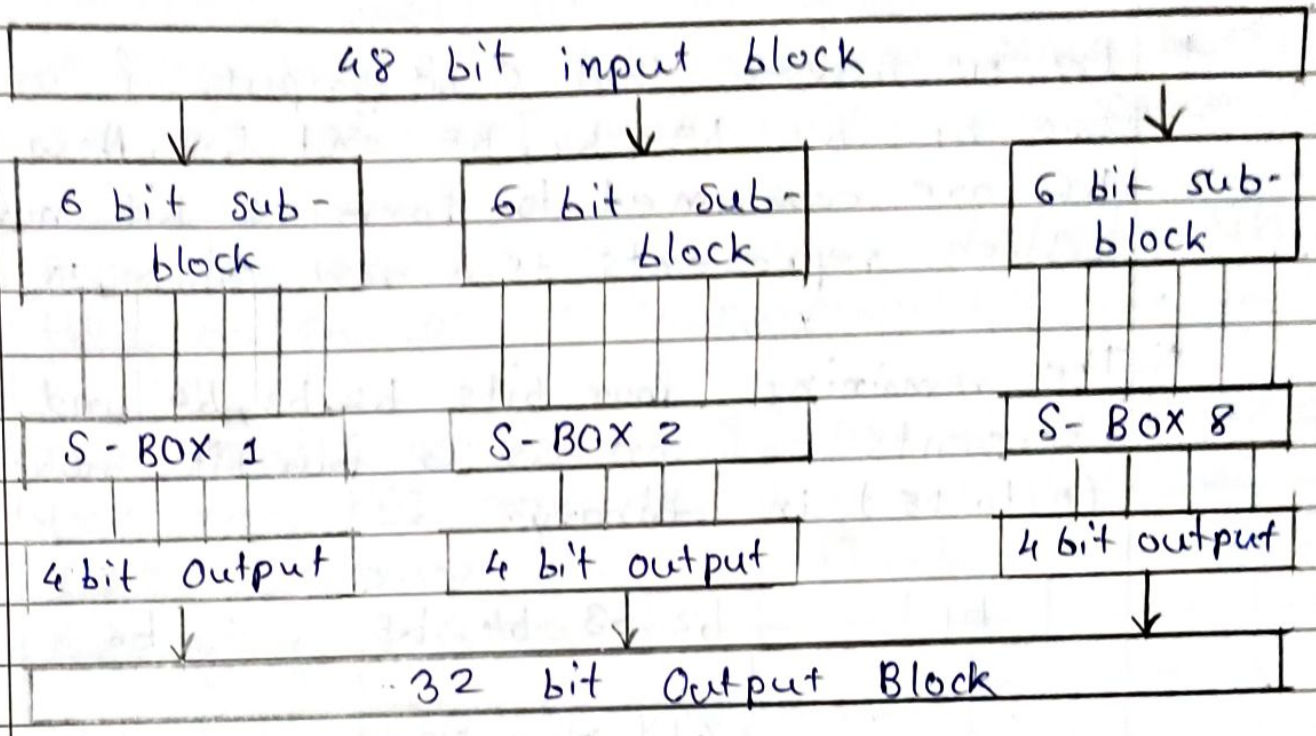
* Now these two 48 bit data (key & RPT) are XOR'ed and the resulting output is given to the next step.

③ S Box Substitution:-

* This process takes 48 bit input and produces a 32 bit output using substitution technique. This substitution is performed by 8 substitution boxes called as S boxes.

* Each of these 8 S-boxes has a 6 bit input and a 4 bit output.

* The 48 bit input block is divided into 8 sub blocks (each of size 6 bits) and each such subblock is given to an S-box.



* What is the logic used by S-box for selecting only four bits out of six bits?

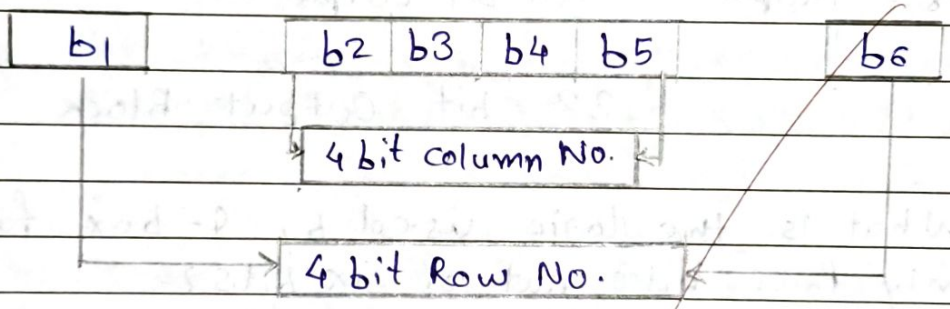
* We can conceptually think of every S box as a table that has 4 rows (numbered from 0 to 3) and 16 columns (numbered from 0 to 15) at the intersection of every row and column, there is a 4 bit number which will be the output for that S box.

11	5	13	1	10	2	0	11	7	3	15	10	3	6	12	8
0	12	9	13	15	1	1	4	11	14	6	3	8	7	9	9
14	5	4	6	15	4	9	0	7	0	12	6	5	3	15	8
13	2	10	2	11	2	8	12	7	13	1	5	9	14	10	14

* The 6 bit input indicates which row and column, and ∴ which intersection is to be selected.

* Let us assume that 6 bit input of an S box are b_1, b_2, b_3, b_4, b_5 and b_6. Now b_1 and b_6 are combined to form 2 bit number which represents the row (00, 01, 10 and 11)

* The remaining four bits b_2, b_3, b_4 and b_5 represents column as a four bit number (0 to 15) in binary.



* E.g. Let the 6 bit input to S-box be 101101
∴ row number = 11 = 03 (decimal)
Column number = 0110 = 06 (decimal)
∴ Intersection of row 03 & column 06 is considered as the output of the S Box.

(4) P Box Permutation :-

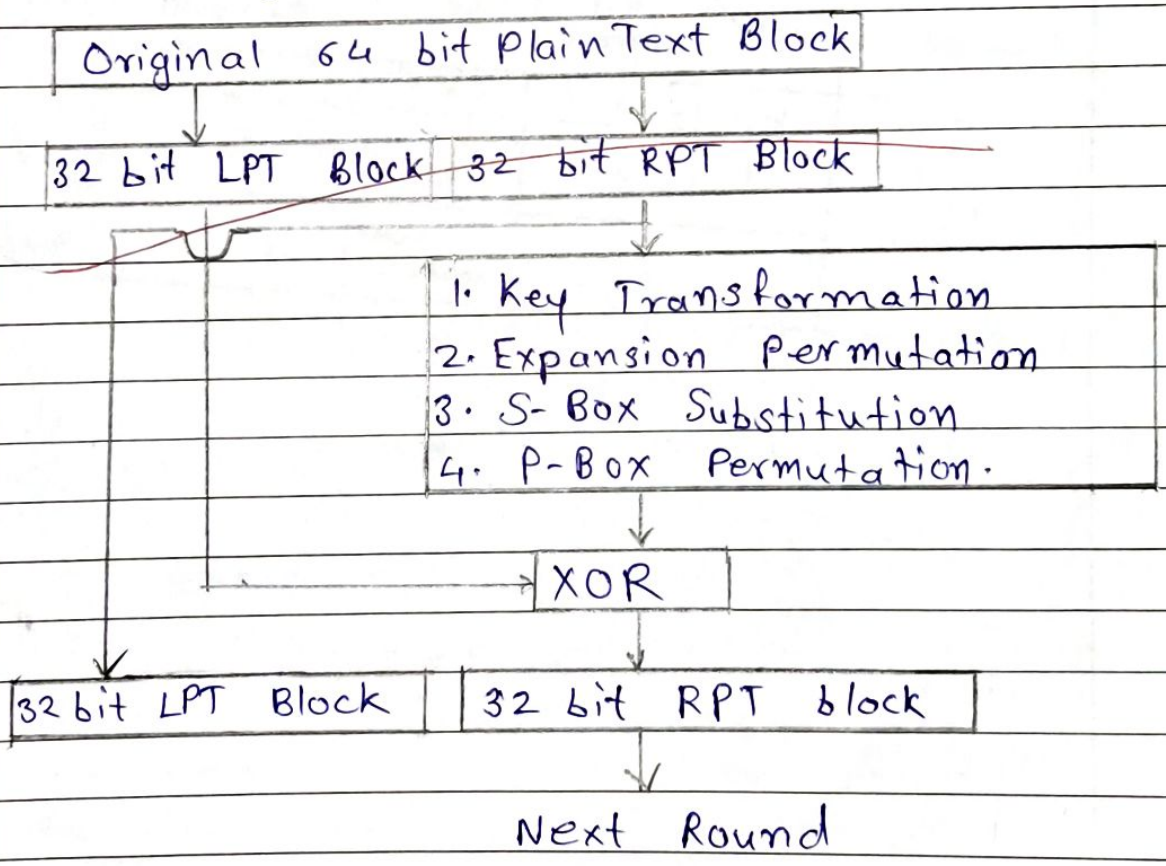
* The output of the S Box consists of 32 bits. This 32 bits are permuted using a P Box.

(5) XOR and Swap :-

* Uptill now we have performed all the operations only on the 32 bit RPT out of the total 64 bit original plain text. 32 bit of LPT was untouched so far.

* Now the 32 bit LPT will be XORed with the output of PBOX Permutation.

* The result of the XOR operation becomes the new RPT and the original previous RPT becomes the new LPT in the swapping process.



⑥ Final Permutation :-

At the end of 16 rounds the final permutation is performed (only once).

Conclusion:

Hence we successfully studied encryption of long message using various modes of operation using DES.