Step 4 Details of one round

Key transformation

↓

Expansion permutation

↓

S-box substitution

↓

P-box permutation

↓

xor and swap

Key transformation

Left shift ⟹

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
No. of key bits shifted	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

For example

C_0 = 1111000011001100101010101111

C_1 = 1110000110011001010101011111

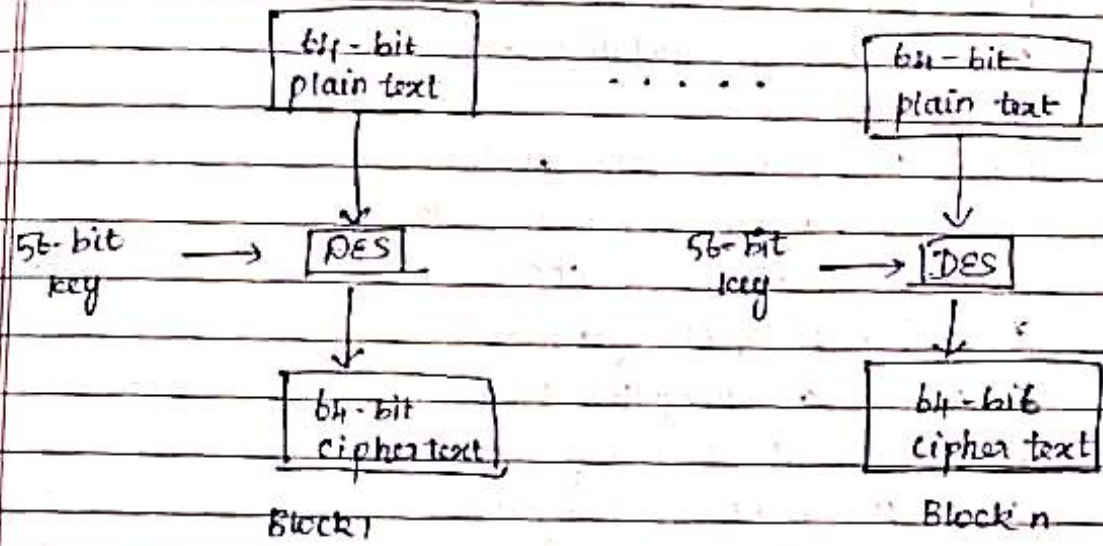
Compression permutation

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

CNS

1) Data Encryption Standard (DES)

Basic working principle

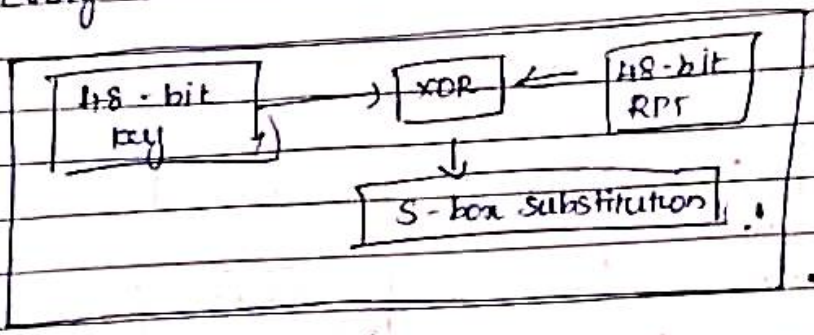


1. Discarding 8th bit of original key

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

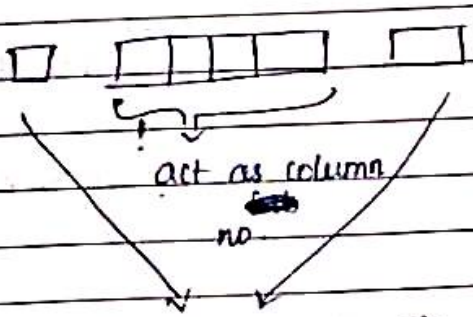
64-bit original key
↓
key discarding process
↓
56-bit key.

Inside every s-box the 48-bits transformed key and 48-bits expanded RPT undergo X-OR operation and the final output enters S-box substitution. Every block has its own S-box, nearly 8 S-box.



(Draw 4x16 S-boxes of count 8)

How substitution takes place:



Eg: (1) 0110(1).

0000 0001 0010 0011 0100 0101 0110 ... 1111

00
01
10
11

(value in binary)

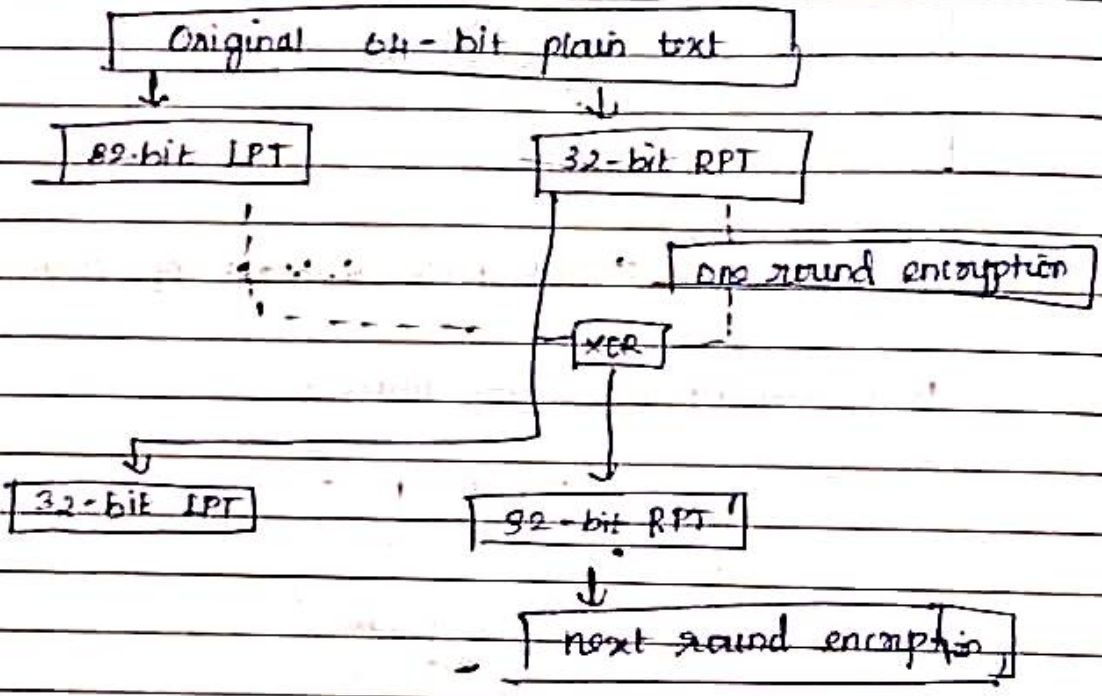
Thus every block gives a 4-bit o/p, collectively it gives 32-bit o/p value

P-Box permutation

The resultant 32-bits are permutated

(put 8x16 box with nos filled in random order)

XOR and swap



Step 5:

Final permutation

(Draw 8x16 box with nos in random order)

Strength of DES

1) 56-bit key have $2^{56} = 7.2 \times 10^{16}$ values
2) Avalanche effect in DES

2. Steps in DES.

Step1: Initial 64-bit plain text is handed over to initial permutation IP function

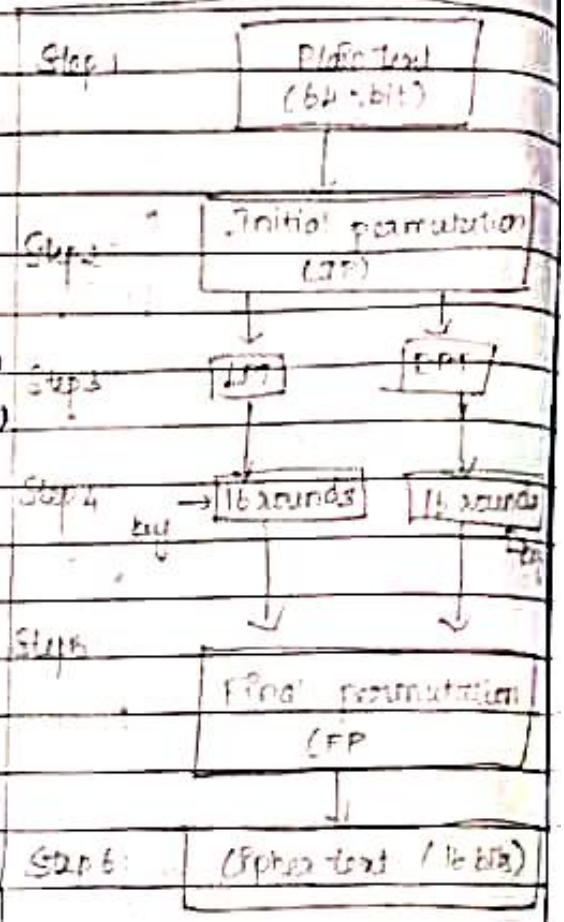
Step2: Initial permutation on plain text

Step3: Initial permutation produces two halves : left plain text (LPT) and right plain text (RPT)

Step4: Each LPT & RPT go through 16 rounds of encryption process each with its own key

Step5: LPT & RPT are rejoined and final permutation is performed

Step6: Result of 64-bit cipher text.



Step2: Initial permutation

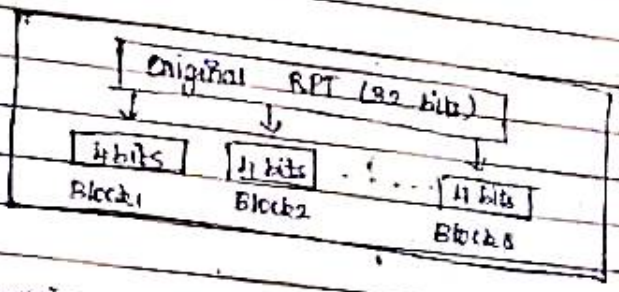
58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Initial permutation table

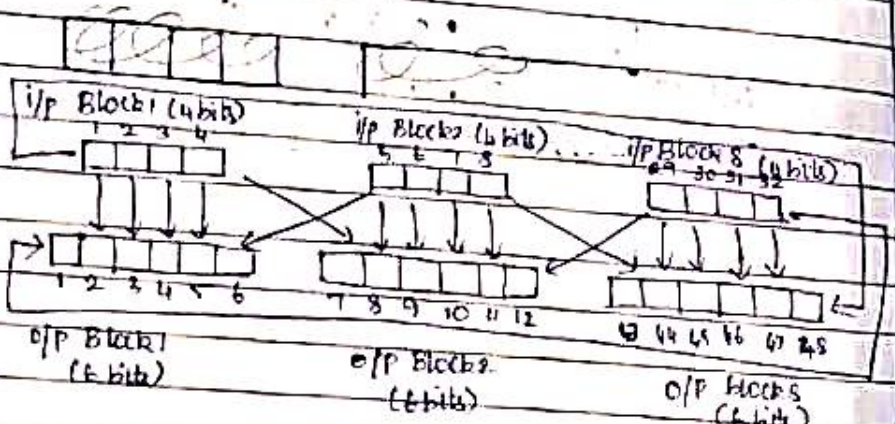
ASHITHA S6
CNS
Cryptography and Network Security
Jeluvaraj

Expansion permutation

At first original RPT (32) is taken and divided into 8 blocks each of 4-bits and expansion permutation takes place such that 4-bits of each block are converted to 6-bits forming a total of 48-bits



Expansion



S-box Substitution