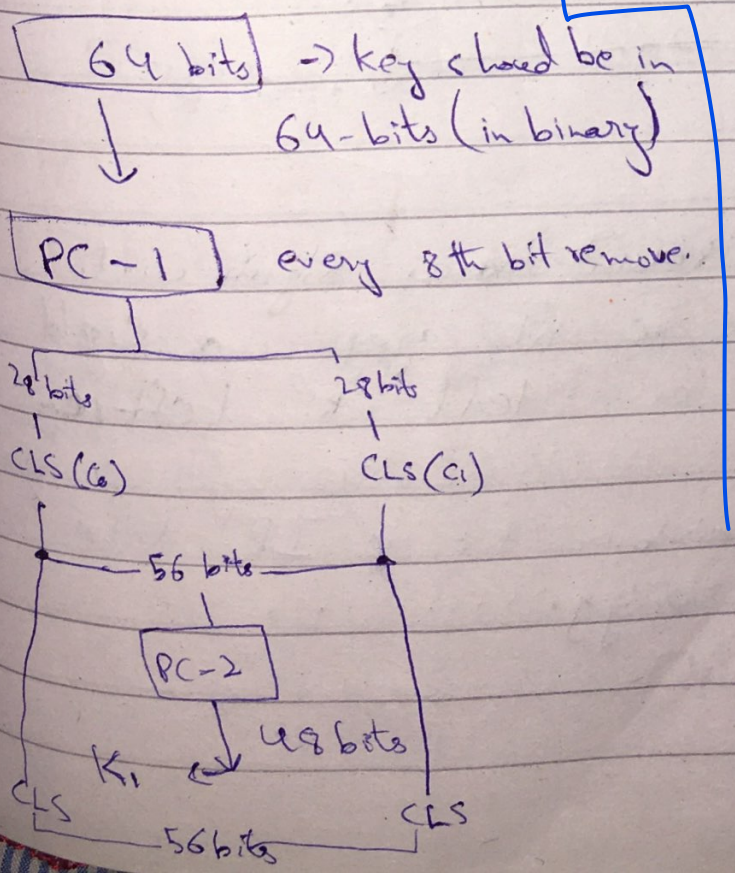
→ 16 rounds (initially 12, but repeatation occur)
→ every table is hard coded (using mathematically formula)
→ 1st, 2nd, 9th, 16th round (one bit shift)
→ rest 2 bits

DES (1976 – 2005)

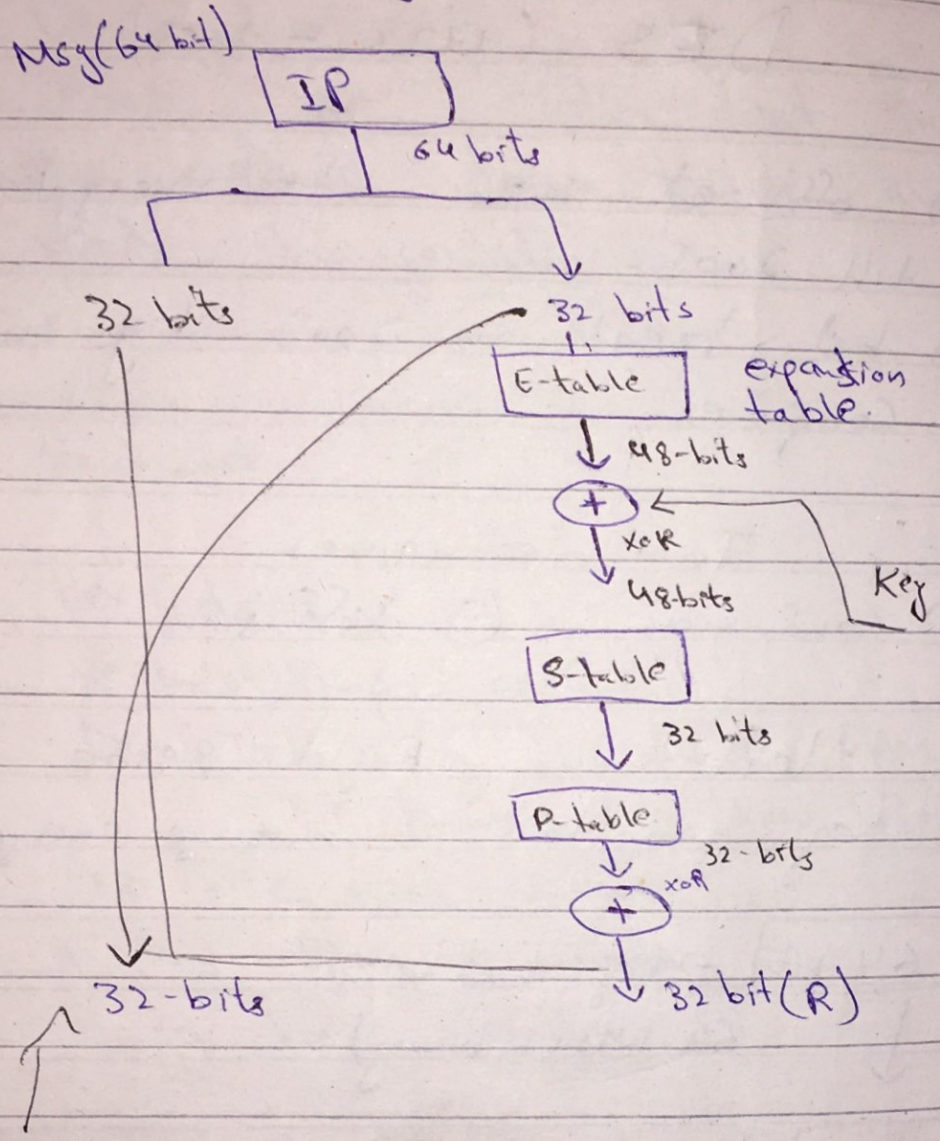
→ offrial use for encryption till 2005.
→ but break in 2005 by super computer.

Two techniques.
① Confusion ② diffusion.

Left → Key generation
Right side. → message encryption



Right.



→ Last round wali Right wali 32 bits left pe nhi ayegi wo Right pe rahegi or left ki left pe-

~~end~~ mai Dono ko Combine kr k IP^{-1} table se pass karenge!

2 2
1 2

E-table

-1 ↩ ↪ +1

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

1 2 3 4 5 6 7 8

→ 1 0 1 0 1 0 1 1

E-table ans

S-table :- (total 8 sbox S1, S2, S3 ... S8)

pair 6-6 bits give one output

every pair goes to different sub table of S

sequencially

S1 ← Pair 1

S2 ← Pair 2

→ kaunsi raw mai jana hai

1 0 1 0 1 1

columns

1 1 → 3 (4th rows)

$2^n \rightarrow 2^2 = 4$ rows

$2^n \rightarrow 2^4 = 16$ columns. (hongi)

↳ Zero se start

(row/column) kr k aage wale ko dekhenge

1 3 3 4 5 7 7 9 9 B B C D F F 1

0 0 0 1 0 0 1 1 0 0 1 1 0 1 0 0 0 1 0 1 0 1 1 1 0 1 1 1

1 1 0 0 1 1 0 0 1 1 0 1 0 1 1 1 0 0 1 1 0 1 1 1 1 1 1 1 0 0 0 1

0 0 0 1 0 0 1 0 0 1 1 0 1 0 0 1 0

1 1 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1 0 1 1 1 1

C L S

1 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1 0 1 1 1 1 1

2nd C L S

1 0 1 0 1 0 1 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0 0 1 1 1 1 0

PC-2

0 0 0 1 1 0 1 1 0 0 0 0 0 0 0 1 0 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 0 0 0 1

1 1 0 0 0 0 0 1 0 1 1 1 0 0 1 0

0123456789ABCDEF

binary :-

0000 0001 0010 0011 0100 0101 0110 0111 1000

1001 1010 1011 1100 1101 1110 1111

32 bit (R)

1 0001 0011 0101 0111 1001

11001100000 0000011