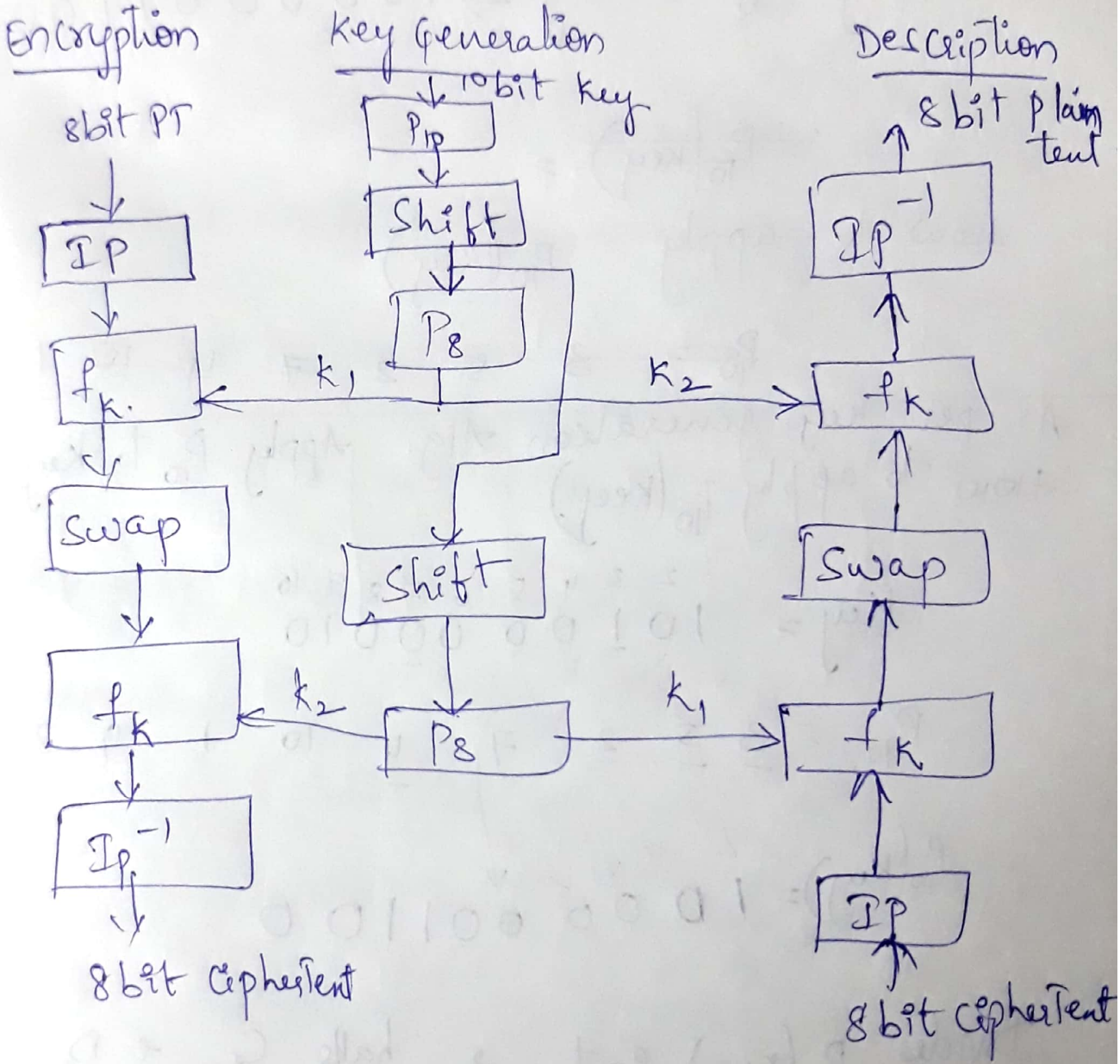
S-DES

S-DES Diagram.



$. Key generation Algorithm

key = 1 2 3 4 5 6 7 8 9 10
1 0 1 0 0 0 0 0 1 0

P_{10} = 3 5 2 7 4 10 1 9 8 6

P_8 = 6 3 7 4 8 5 10 9

As per key generation Alg. Apply P_{10} to key
How to apply P_{10}(key)

	1	2	3	4	5	6	7	8	9	10
Key =	1	0	1	0	0	0	0	0	1	0

P_{10} = 3 5 2 7 4 10 1 9 8

P_{10}(Key) = 1 0 0 0 0 0 1 1 0 0

Divide P_{10}(key) into 2 halves C_{i-1} + D_{i-1}

⇒ 1 0 0 0 0 | 0 1 1 0 0

C_{i-1} D_{i-1}

Left circular shift to C_{i-1} + D_{i-1}

$LCS(C_{i-1}) = 00001$ $LCS(D_{i-1}) = 11000$

→ $LCS(C_{i-1})$ and $LCS(D_{i-1})$ used for next Round

used

Apply P_8 to generate this round key.

$\therefore LCS(C_{i-1}) + LCS(D_{i-1}) = 00001\ 11000$

Apply P_8 to above

$P_8 = 6\ 3\ 7\ 4\ 8\ 5\ 10\ 9$

$\therefore K_1 = P_8(LCS(C_{i-1}, D_{i-1})) = 10100100$

To generate K_2

Take $LCS(C_{i-1}) + LCS(D_{i-1})$ as i/p.

$C_i = LCS(C_{i-1})$ $D_i = LCS(D_{i-1})$

$\therefore C_i = 00001$ $D_i = 11000$

Apply $LCS_2(C_i + D_i)$

1 2 3 4 5 6 7 8 9 10

⇒ 00100 00011

Apply P_8 to above

$K_2 = P_8(LCS_2(C_i, D_i)) = 01000011$

Encryption

Plaintext (PT) = 1 1 1 1 0 0 1 1.

I_p = 2 6 3 1 4 8 5 7

E/p = 4 1 2 3 2 3 4 1

(To convert 4bits to 8bits)

P_4 = 2 4 3 1

$$S_0 = \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \quad S_1 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 2 \\ 2 & 1 & 0 & 3 \end{bmatrix}$$

S_0 & S_1 are S-boxes - used to convert 8 bits to 4 bits

Apply Ip to plain text

I_p = 2 6 3 1 4 8 5 7

1 2 3 4 5 6 7 8

PT = 1 1 1 1 0 0 1 1

I_p(PT) $\Rightarrow$ 1 0 1 1 1 1 0 1

divide above into 2 halfs.

L_{i-1} = 1011 $\quad$ R_{i-1} = 1101

Round, starts.

Round 1

Apply E/p on R_{i-1} = 1101

E/p = 4 1 2 3 2 3 4 1

$\therefore$ E/p(R_{i-1}) = 11101011

To do ⊕ with key - K_1

We need E/p.

R_{i-1} = 4 bits K_1 = 8 bits

- To Do XOR both must have Equal no. of bits.

$\therefore$ we expanded R_{i-1} using Expanded permutation (E/P).

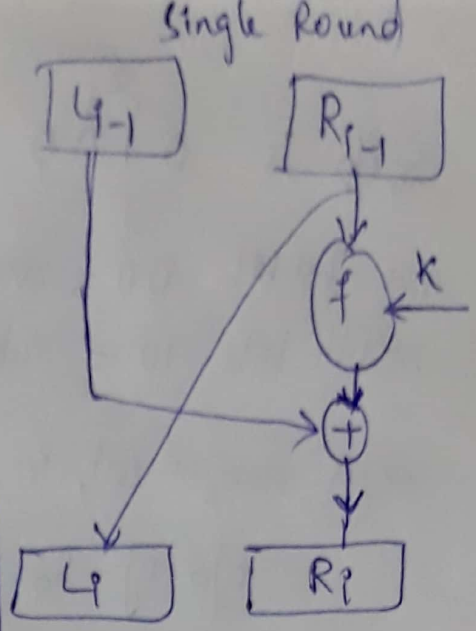
E/p (R_{i-1}) ⊕ K_1

$\Rightarrow$ 1 1 1 0 1 0 1 1

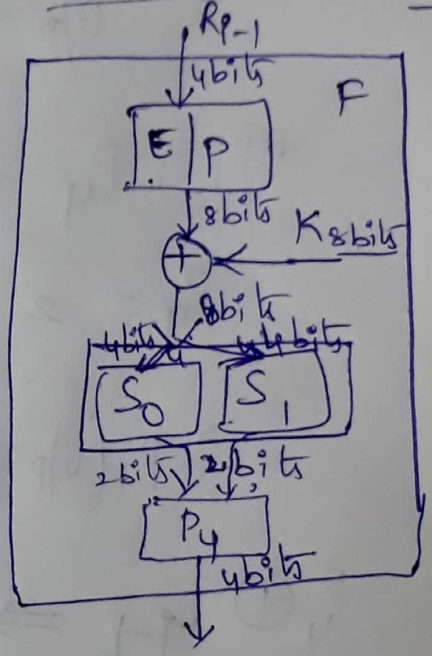
⊕ 1 0 1 0 0 1 0 0

0 1 0 0 1 1 1 1 (8 bits

- Divide above into 2 halfs give first half(4bits) to S_0 as i/p to get 2 bits as o/p and second half (4 bits) to S_1 as i/p to S_1 to get 2 bits as o/p.



In Each Round function



S_0 i/p is 0100 (column)

First & last bit 00 = row_0

Middle bits 10 = $column_2$

refer row_0 & col, in S_0 = 03

∴ o/p of S_0 = 11

S_1 i/p is 1111 (col, row)

11 – row_3

11 – $column_3$

In S_1 3rd row & col = 3

∴ o/p of S_1 = 11

∴ o/p of S_0 & S_1 = 1111 (1 2 3 4)

Apply P_4 to o/p of S_0 & S_1

P_4 = 2 4 3 1

⇒ P_4(o/p of S_0 & S_1) = 1 1 1 1

$P_4 \oplus L_{4-1}$ ⇒

1	1	1	1	P_4(o/p of S_0 & S_1)
1	0	1	1	L_{4-1}
0	1	0	0	

∴ $L_4 = R_{4-1}$ $R_4 = (L_{4-1} \oplus f(R_{4-1}, K_4))$

∴ L_4 = 1101 R_4 = 0100.

Round 2 $R_1 = 0100$ E/p = 4 1 2 3 2 3 4 1

E/p(R_1) = 00101000

E/p(R_1) ⊕ k_2 ⇒ 00101000
⊕ 01000011
01101011
S_0 S_1

S_0 = 0110 (row 00, col 11)

S_0 − 0 row, 3 col = 2

S_0 = 10

S_1 = 1011

11 − 3 row
01 − 1 col = 1

S_1 = 01

∴ o/p of S_0S_1 = 1001

P_4(o/p of S_0S_1) = 0101

P_4(o/p of S_0S_1) ⊕ L_1 ⇒ 0101
⊕ 1101
1000

∴ $L_{i+1} = R_i$ $R_{i+1} = (L_i \oplus f(R_i, k_2))$

∴ R_{i+1} = 0100 R_{i+1} = 1000

Apply I_p^{-1} to $L_{i+1} + R_{i+1}$ ⇒ $I_p^{-1}(L_{i+1}, R_{i+1})$ = Cipher Text

I_p = 2 6 3 1 4 8 5 7

I_p^{-1} = 4 1 3 5 7 2 8 6

= 00010100
⇓
Cipher Text