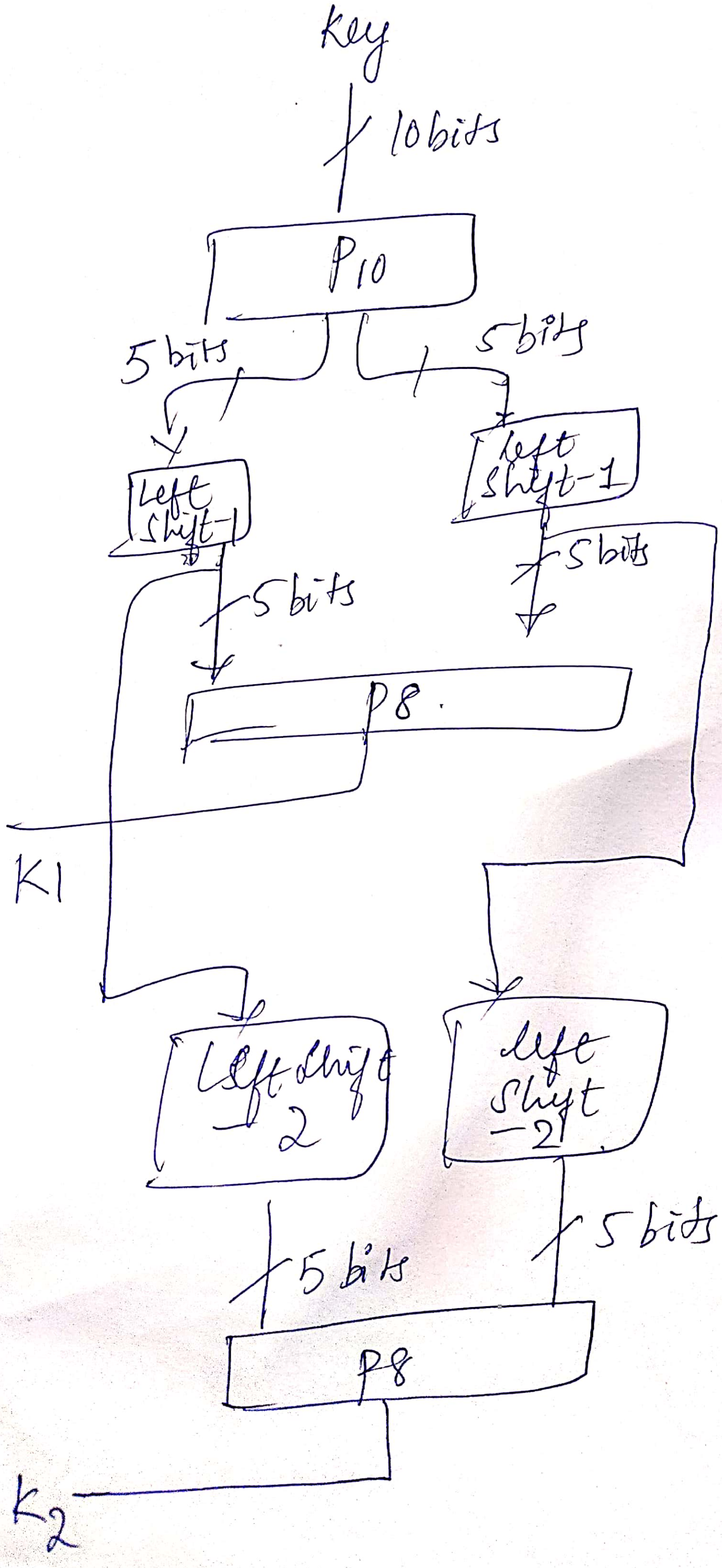
S-DES (Simplified DES)

Key generation Algorithm

Key → 1010000010
(10bits.)



Now apply

P10 permutation

P10 →										
I/P :-	1	2	3	4	5	6	7	8	9	10
O/P :-	3	5	2	7	4	10	1	9	8	6

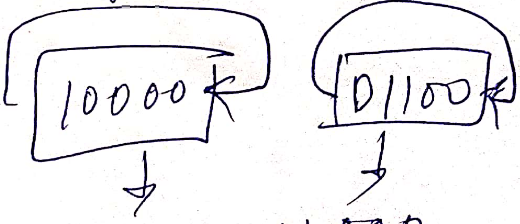
After P10. →

1000001100

now divide into 5 bits each

10000 01100

perform left shift-1



00001 11000

Then apply P8 permutation.

P8 →

I/p	1	2	3	4	5	6	7	8	9	10
o/p	6	3	7	4	8	5	10	9		

Aftee P8. → 10100100 → K_1

Now apply left shift - 2 on left shift 1 bits

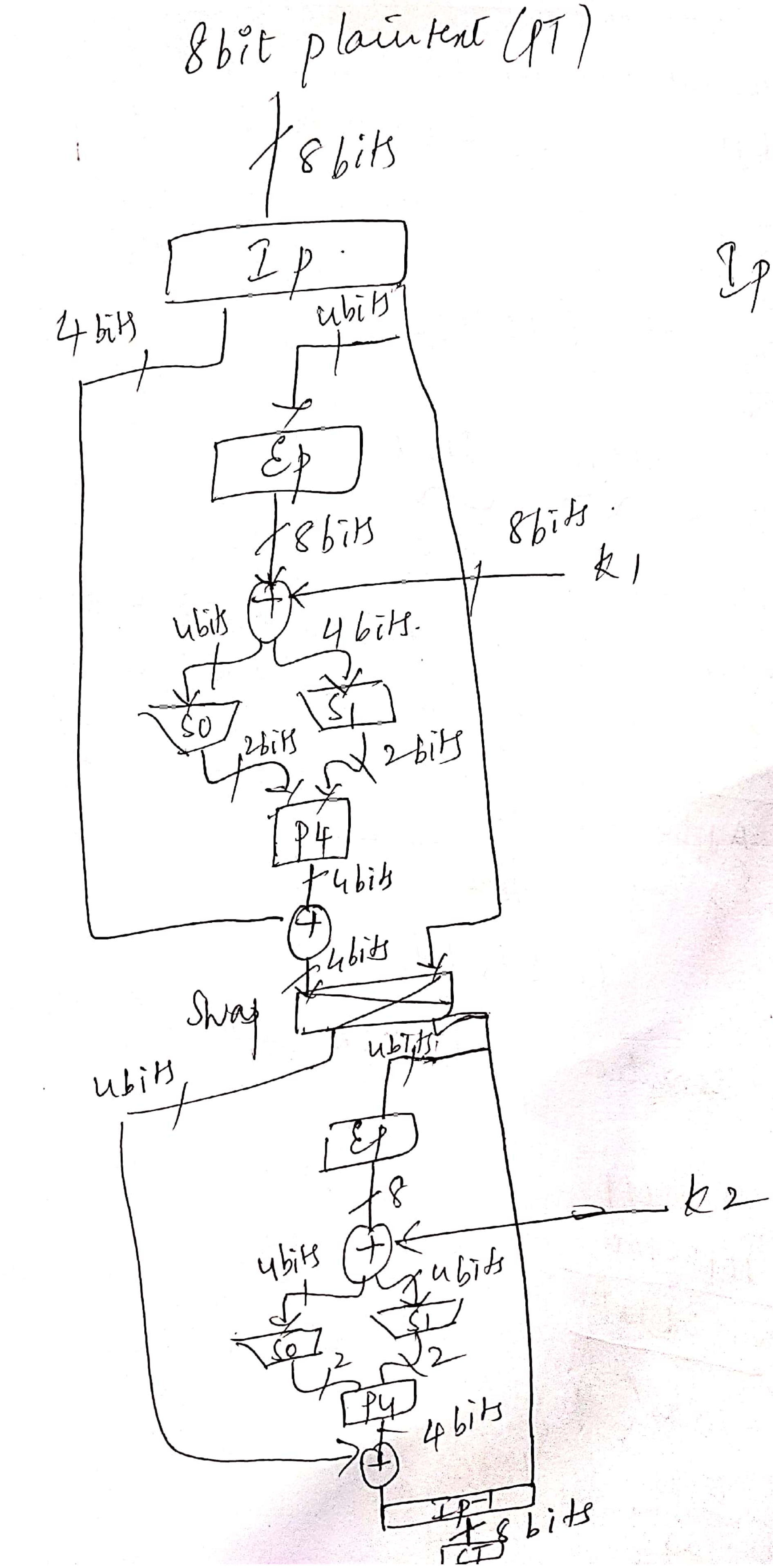
00001 11000

Aftee left shift-2 → 00100 00011 ~~→ K_2~~ . .

Now Apply P8.

Aftee P8 = 01000011 → K_2

Encryption Algorithm



Ip → Initial permutation

Ip^{-1} → Inverse Initial permutation

Ep → Expanded Permutation

P4 – permutation 4

S0, S1 → Substitution boxes.

CT – Cipher Text

PT – plaintext.

PT = 10010111

Initial peemutarion (IP)

I/p	1	2	3	4	5	6	7	8
O/p	2	6	3	1	4	8	5	7

After Ip → 01011101

$$\underbrace{0101}_{Lo} \quad \underbrace{1101}_{Ro}$$

Expanded peemutation (Ep) →

I/p →	1	2	3	4	5	6	7	8
O/p →	4	1	2	3	2	3	4	1

Apply Ep on 1101

After Ep →

11101011

Now consider K1 & XOR with Ep o/p.

$$\begin{array}{r} 11101011 \\ \oplus\ 10100100 \\ \hline 01001111 \\ \hline \end{array}$$

Divide into 4 bits

$$\underbrace{0100}_{\hookrightarrow S0} \quad \underbrace{1111}_{\hookrightarrow S1}$$

0100 → S0

00 → 0 → row

10 → 2 → colum

Ily. 1111 → S1

11 → 3 - row

11 → 3 - col

$$S_0 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 1 & 0 & 3 & 2 \\ 1 & 3 & 2 & 1 & 0 \\ 2 & 0 & 2 & 1 & 3 \\ 3 & 3 & 1 & 3 & 2 \end{array}$$

$$S_1 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 1 & 3 \\ 2 & 3 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 3 \end{array}$$

So $S_0 = 3 = 11$

$S_1 = 3 = 11$

Now. Send $\overset{1111}{\text{it}}$ to $\boxed{P4 \rightarrow 2431}$

O/P of P4 → 1111

P4 ⊕ left hand side 4 bits

$$\begin{array}{r} 1111 \\ 0101 \\ \hline 1010 \end{array}$$

1010 1101

1101 1010

After round 1

1101 1010

Now $\underbrace{1101}_{L1}$ $\underbrace{1010}_{R1}$

consider R_1 send to Ep

After Ep → 01010101

Then XOR with K2.

$$\begin{array}{r} \oplus\ 01010101 \\ 0\cancel{1}000011 \\ \hline 00010110 \end{array}$$

$\underline{0001} \to S0$ $\quad$ $\underbrace{0110} \to S1$

o/p of S0 → 11 $\quad$ o/p of S1 → 11

So 1111 send to P4 → 2431)

o/p of P4 → 1111

Now XOR with L1

$$\begin{array}{r} 1111 \\ \oplus\ 1101 \\ \hline 0010 \end{array}$$

(00101010)

$\underline{0010 \ \& \ R_1}$ gone to IP^{-1}

IP^{-1} → 41357286

so $\boxed{CT = 00111000}$