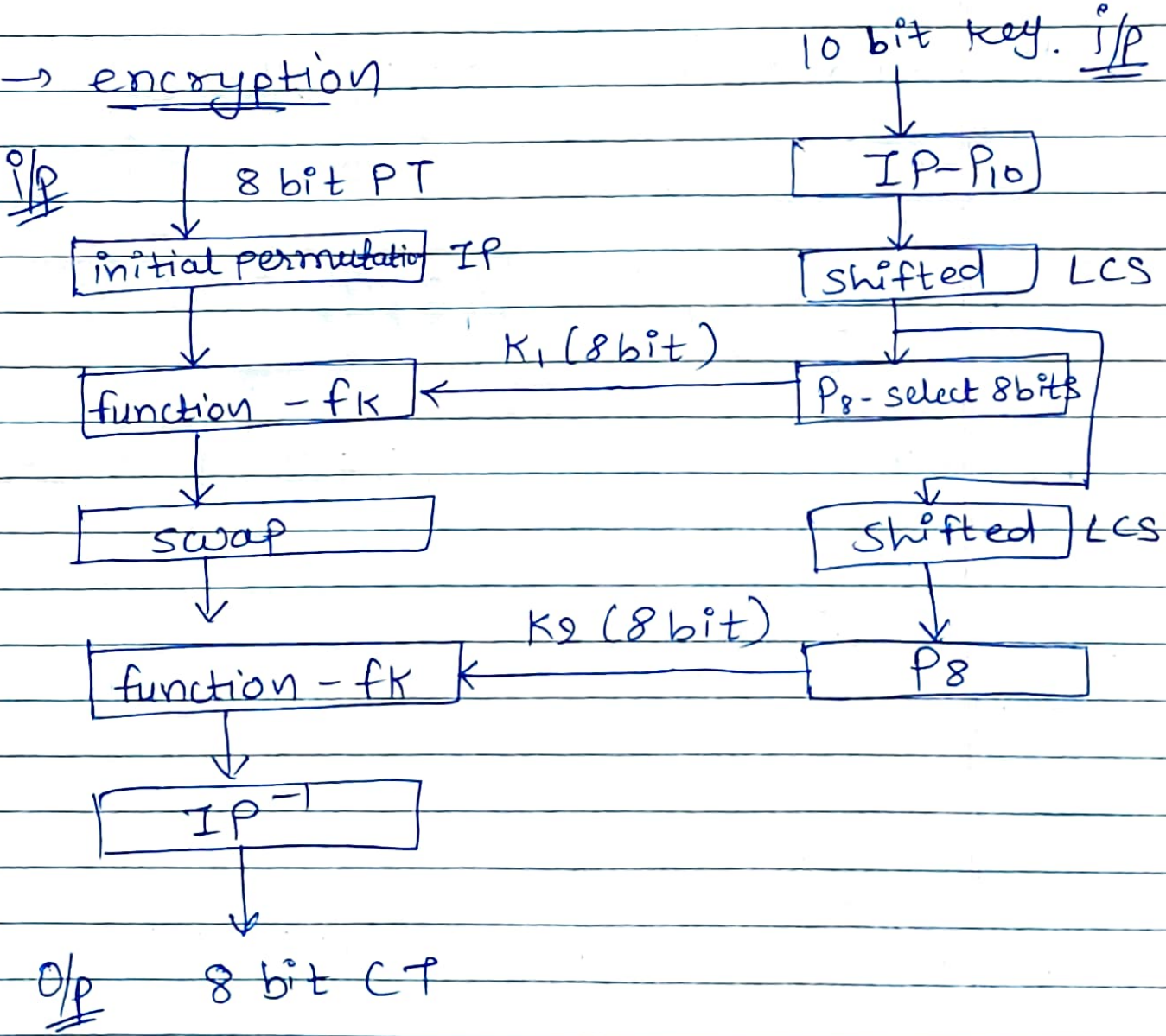
S-DES Simplified DES

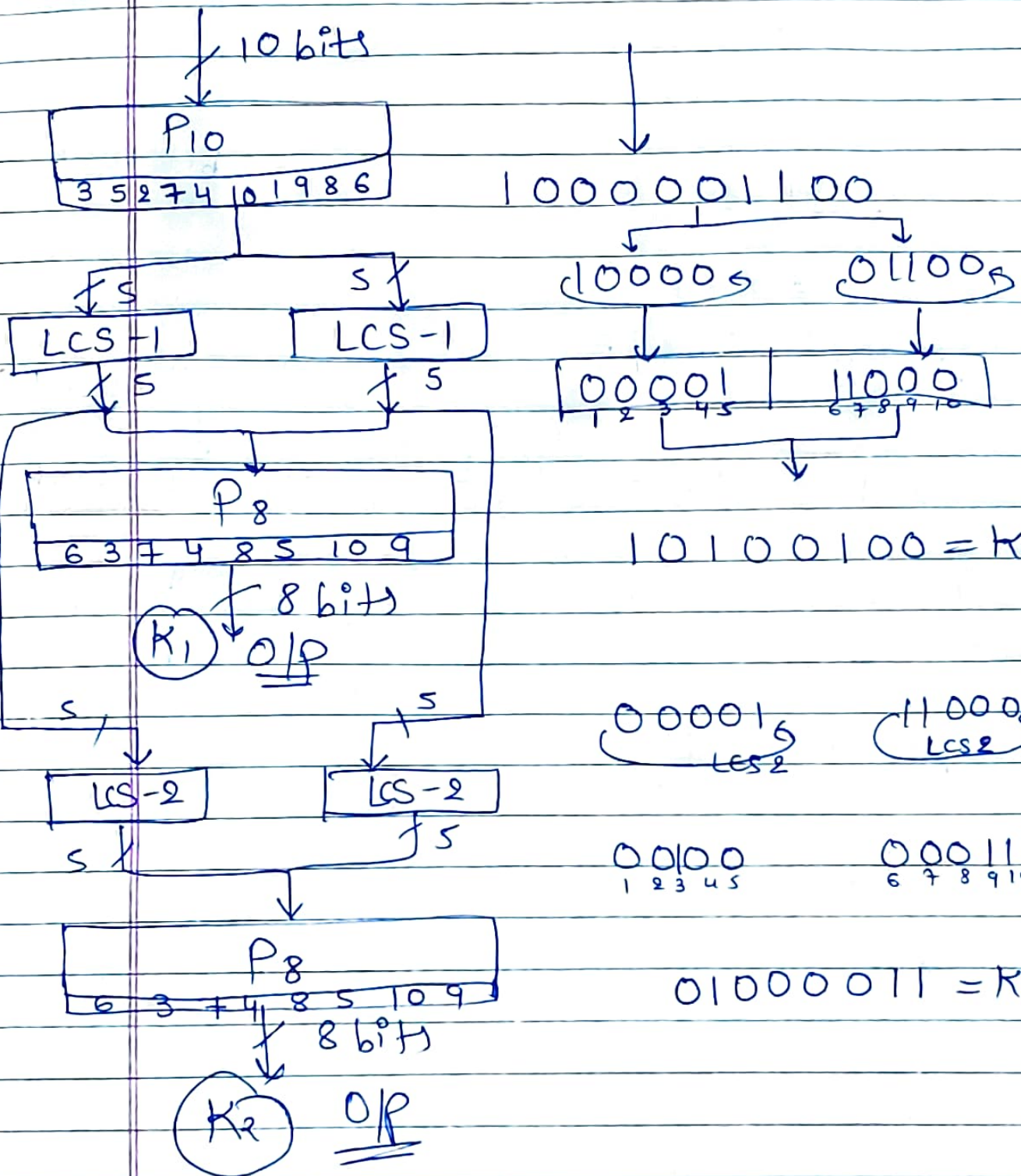
→ 8 bit PT 10 bit key.
8 bit CT

→ encryption



⇒ For decryption keys are used in reverse order i.e. first K2 will be used at 1st stage and for 2nd stage K1 key will be used.

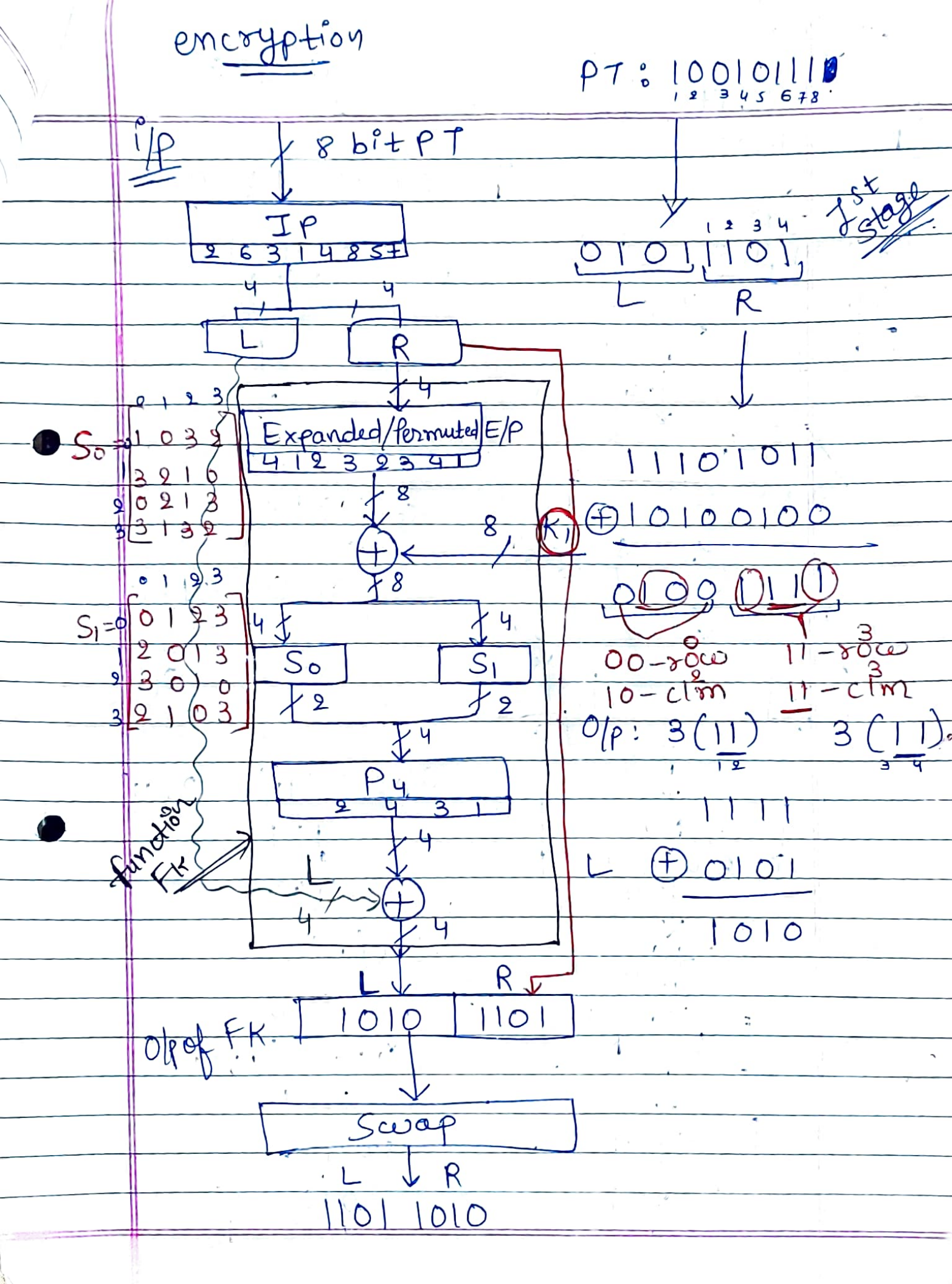
eg. key = 1010000010
(1 2 3 4 5 6 7 8 9 10)



answer ⟹ $K_1 = 10100100$

$K_2 = 01000011$

encryption


PT: 10010111
1 2 3 4 5 6 7 8
i/p
8 bit PT
IP
2 6 3 1 4 8 5 7
4
4
L
R
1st stage
1 2 3 4
0 1 0 1 | 1 1 0 1
L
R
1 1 1 0 1 0 1 1
⊕ 1 0 1 0 0 1 0 0
0 1 0 0 | 1 1 1
00 - row
10 - clm
11 - row
11 - clm
o/p: 3 (11) 3 (11)
1 2 3 4
1 1 1 1
L ⊕ 0 1 0 1
1 0 1 0
S0 =
0 1 2 3
1 0 3 2
3 2 1 0
0 2 1 3
3 1 3 2
Expanded/Permuted E/P
4 1 2 3 2 3 4 1
8
8
K1
S1 =
0 1 2 3
0 1 2 3
2 0 1 3
3 0 0 0
2 1 0 3
4
4
S0
S1
2
2
4
P4
2 4 3 1
4
Function FK
L
4
4
4
L
R
1010
1101
O/p of FK
Swap
L
R
1101 1010

encryption

2nd stage

L R

1101 1010

1 2 3 4

0101 0101

⊕ 01000011

K2 0001 0110

S_0 S_1

01 - ① row 00 - ⓪ row

00 - ⓪ clm 11 - ③ clm

O/P: 3 (11) 3 (11)

1 2 3 4

1111

L ⊕ 1101

0010

L R

0010 1010 → O/P of fk

1 2 3 4 5 6 7 8

0011 1000

8 bit CT O/P.

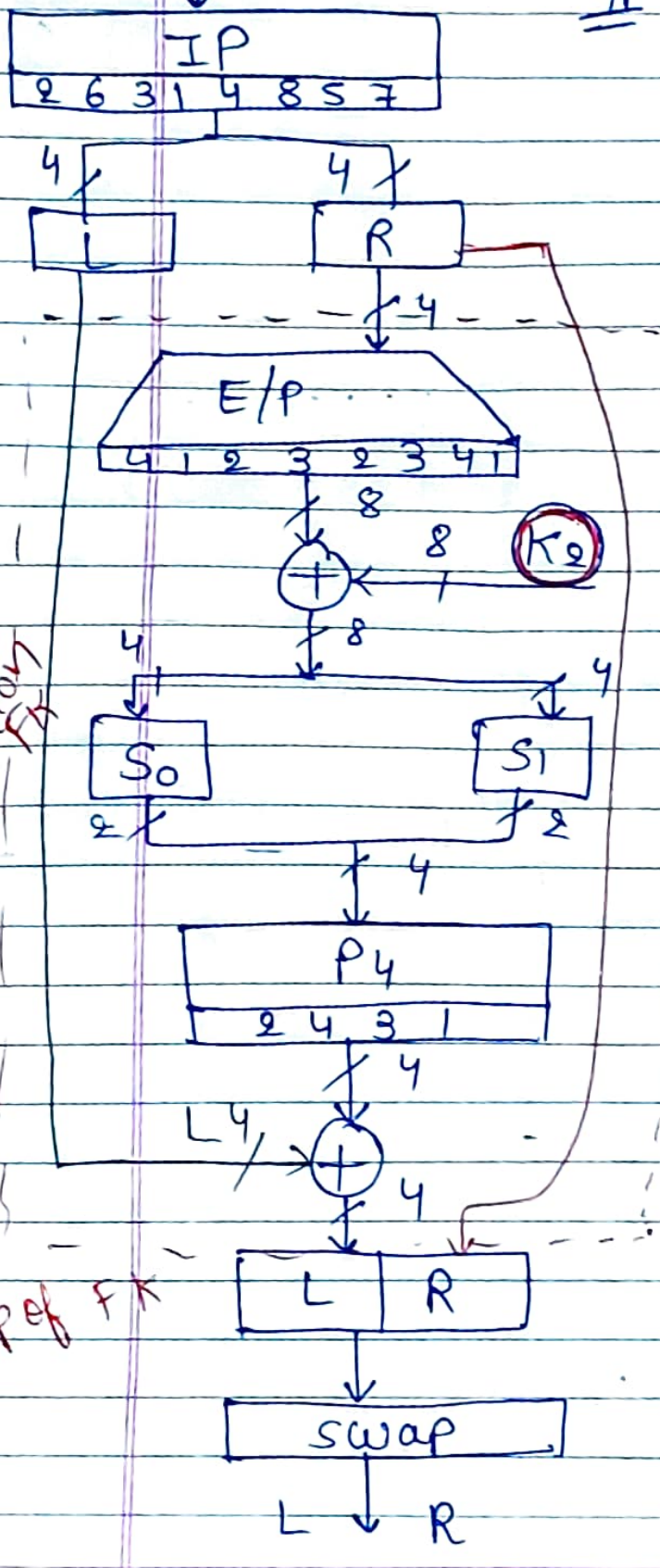
decryption

$K_1 = 10100100$

$K_2 = 01000011$

i/p 8 bit = 00111000

CT



1st stage

i/p 0011 1000

1 2 3 4 5 6 7 8

0010 1010

1 2 3 4

L R

4 1 2 3 2 3 4 1

0 1 0 1 0 1 0 1

K_2 ⊕ 0 1 0 0 0 0 1 1

0001 0110

S_0 S_1

01 - 1 row 00 row

00 - 0 clm 11 - 3 clm

o/p : 3 (11) 3 (11)

1 1 1 1

1 2 3 4

2 4 3 1

1 1 1 1

L ⊕ 0010

1101

1101 1010

L R

swap

1010 1101

L R

decryption 2nd stage

L R

1010 1101

1 2 3 4

↓

4 1 2 3 2 3 4 1

1 1 1 0 1 0 1 1

K_1 ⊕ 1 0 1 0 0 1 0 0

0 1 0 0 1 1 1 1

↓ ↓

S_0 S_1

00 - 0 row 11 - 3 row

10 - 2 row 11 - 3 clm

O/p: 3 (11) 3 (11)

1 1 1 1

1 2 3 4

2 4 3 1

1 1 1 1

L ⊕ 1010

0 1 0 1

L | 0101 | 1101 | R

1 2 3 4 5 6 7 8

O/p of F_K

↓

IP^{-1}

4 1 3 5 7 2 8 6

↓

1 0 0 1 0 1 1 1

8 bit PT O/p