NETWORK PROTOCOLS & SECURITY
23EC2210 R/A/E

Topic:

Data Encryption Standard (DES)

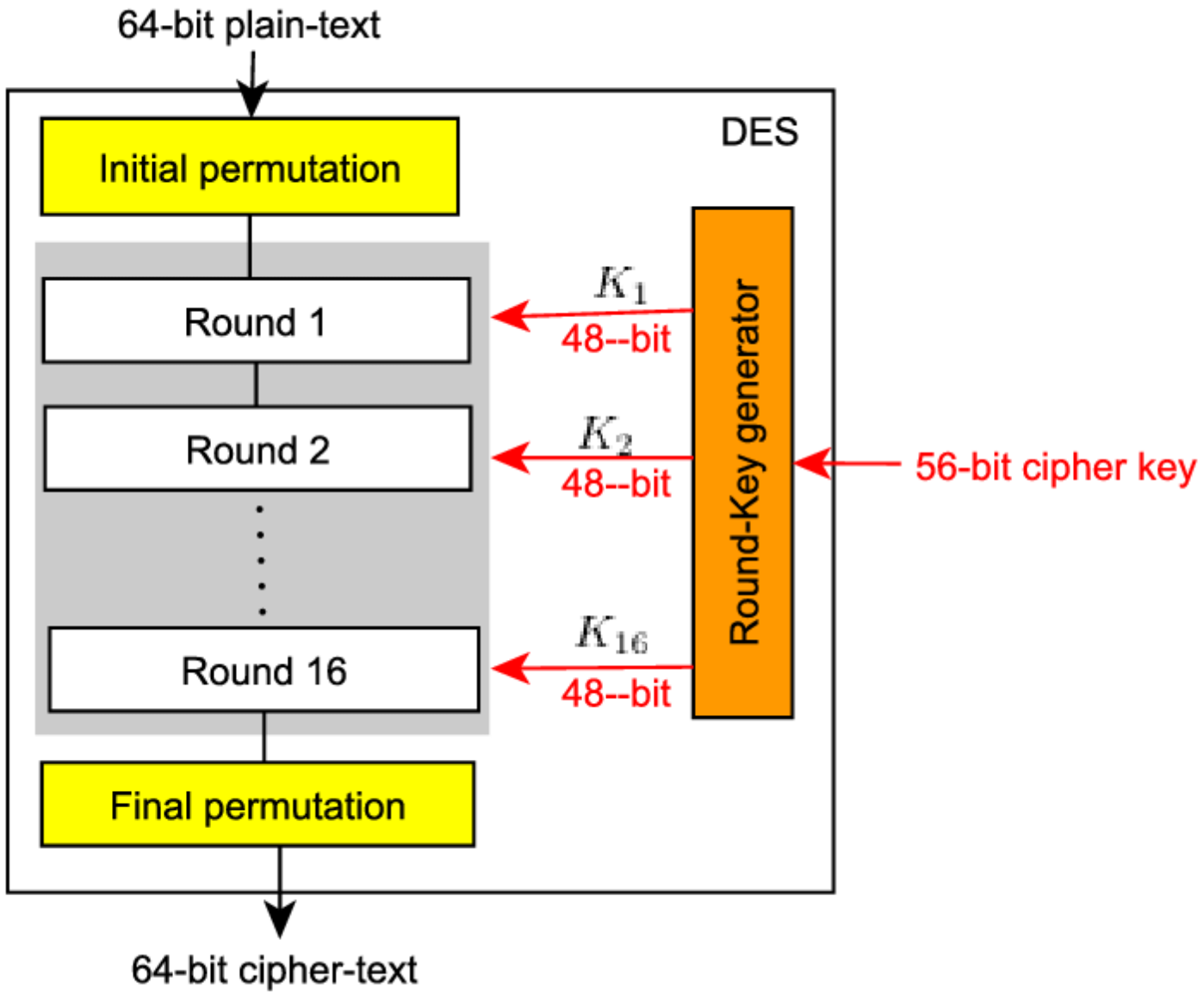
Session – 37

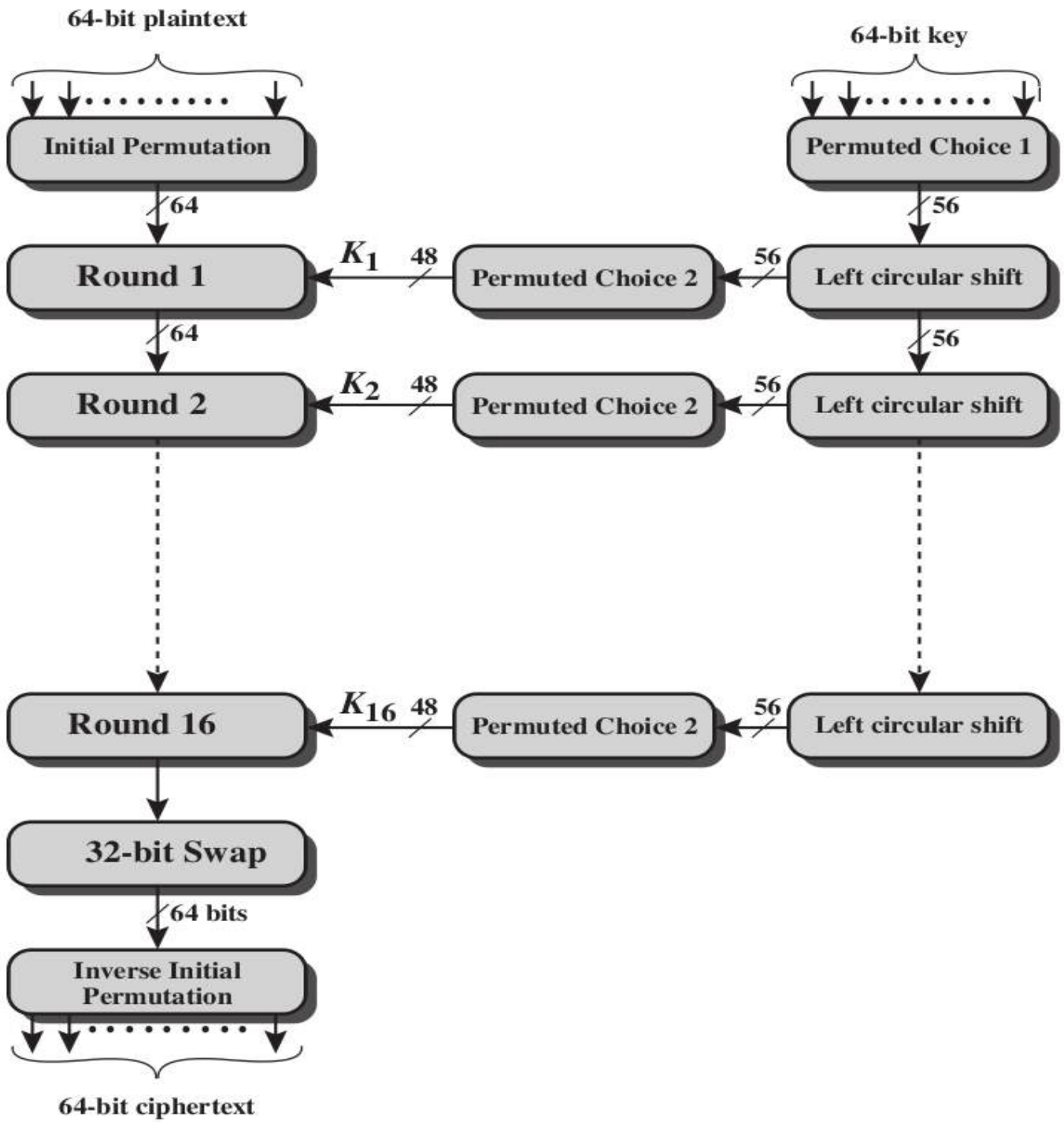
Data Encryption Standard(DES)
Block Cipher

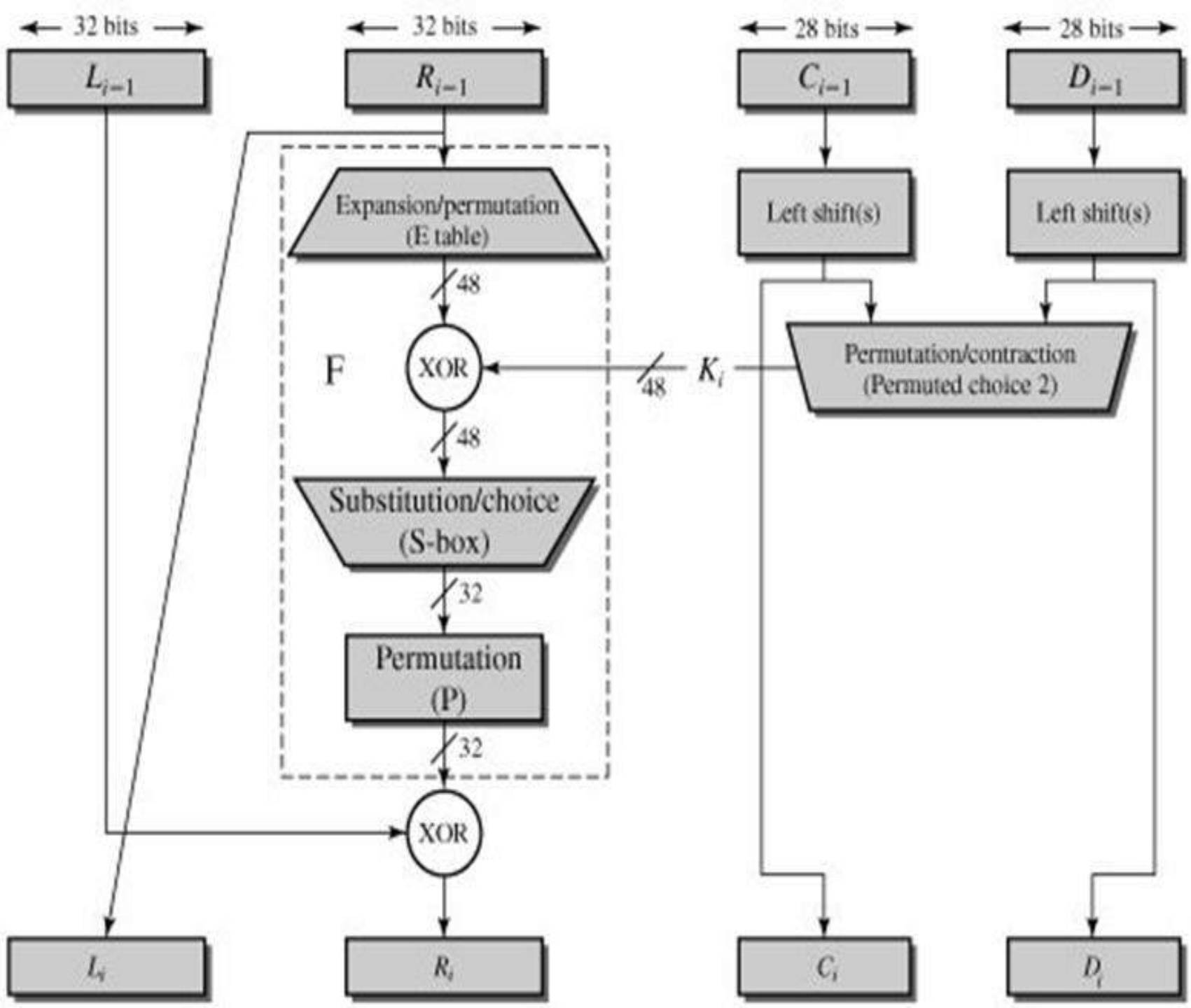
Data Encryption Standard(DES)

- **Data Encryption Standard (DES)** is the **symmetric block** cipher which encrypts a **64-bit plain text** in a **64-bit ciphertext**.
- Introduced by the National Institute of Standard and Technology (NIST) in the 1970s.
- Initially, DES was only used in financial applications but later it was accepted as the cryptographic algorithm by other organizations too.

- DES is a block cipher.
- Encrypts blocks of 64-bits.
- Uses a key of 56-bit.
- Same key is used in encryption and decryption process of DES.
- No. of Rounds: 16




64-bit plaintext
64-bit key
Initial Permutation
Permuted Choice 1
64
56
Round 1
K_1
48
Permuted Choice 2
56
Left circular shift
64
56
Round 2
K_2
48
Permuted Choice 2
56
Left circular shift
Round 16
K_{16}
48
Permuted Choice 2
56
Left circular shift
32-bit Swap
64 bits
Inverse Initial Permutation
64-bit ciphertext


32 bits
32 bits
28 bits
28 bits
L_{i-1}
R_{i-1}
C_{i-1}
D_{i-1}
Expansion/permutation
(E table)
Left shift(s)
Left shift(s)
48
F
XOR
48
K_i
Permutation/contraction
(Permuted choice 2)
48
Substitution/choice
(S-box)
32
Permutation
(P)
32
XOR
L_i
R_i
C_i
D_i

S-DES (Simplified DES)

- Used for better understanding of DES.
- Plaintext size: 8-bit
- Key : 10-bit
- No. of rounds: 2
- Ciphertext : 8-bit

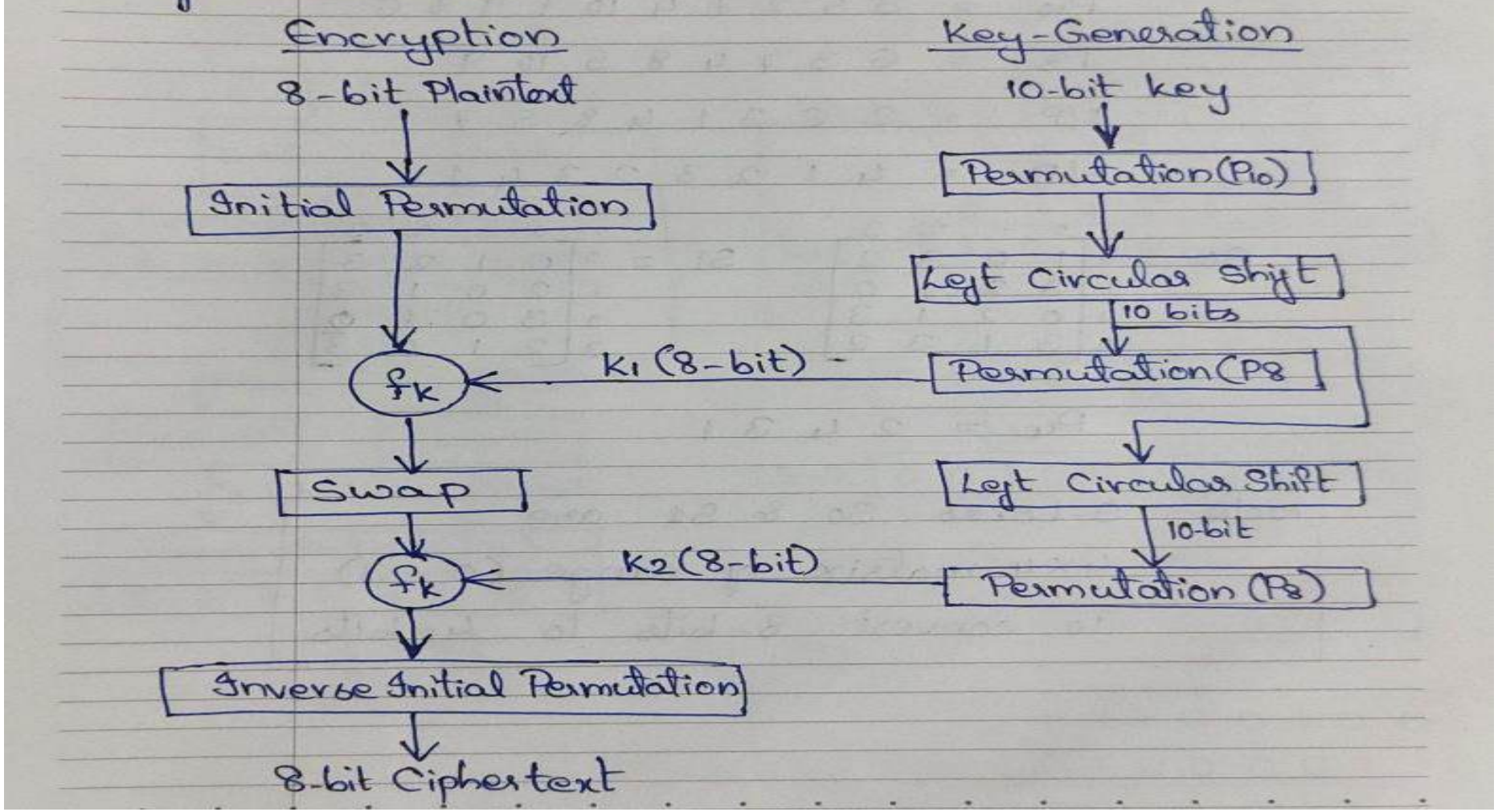
S-DES example

S-DES example

S-DES(Simplified DES)

I/p - Plaintext → 8-bit
key → 10-bit

O/p - Ciphertext → 8-bit
No. of Rounds → 2



S-DES Example:

Given PT = 1 0 0 1 0 1 1 1

Key = 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

I/P = 2 6 3 1 4 8 5 7

E/P = 4 1 2 3 2 3 4 1

S0 =

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

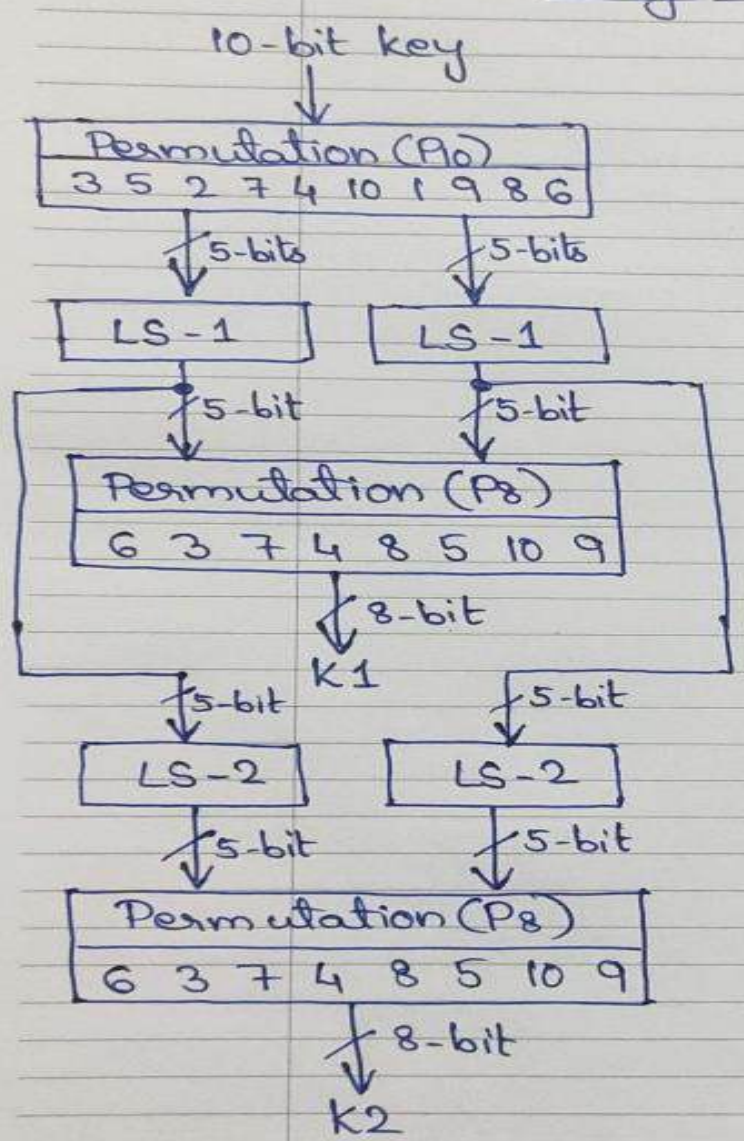
S1 =

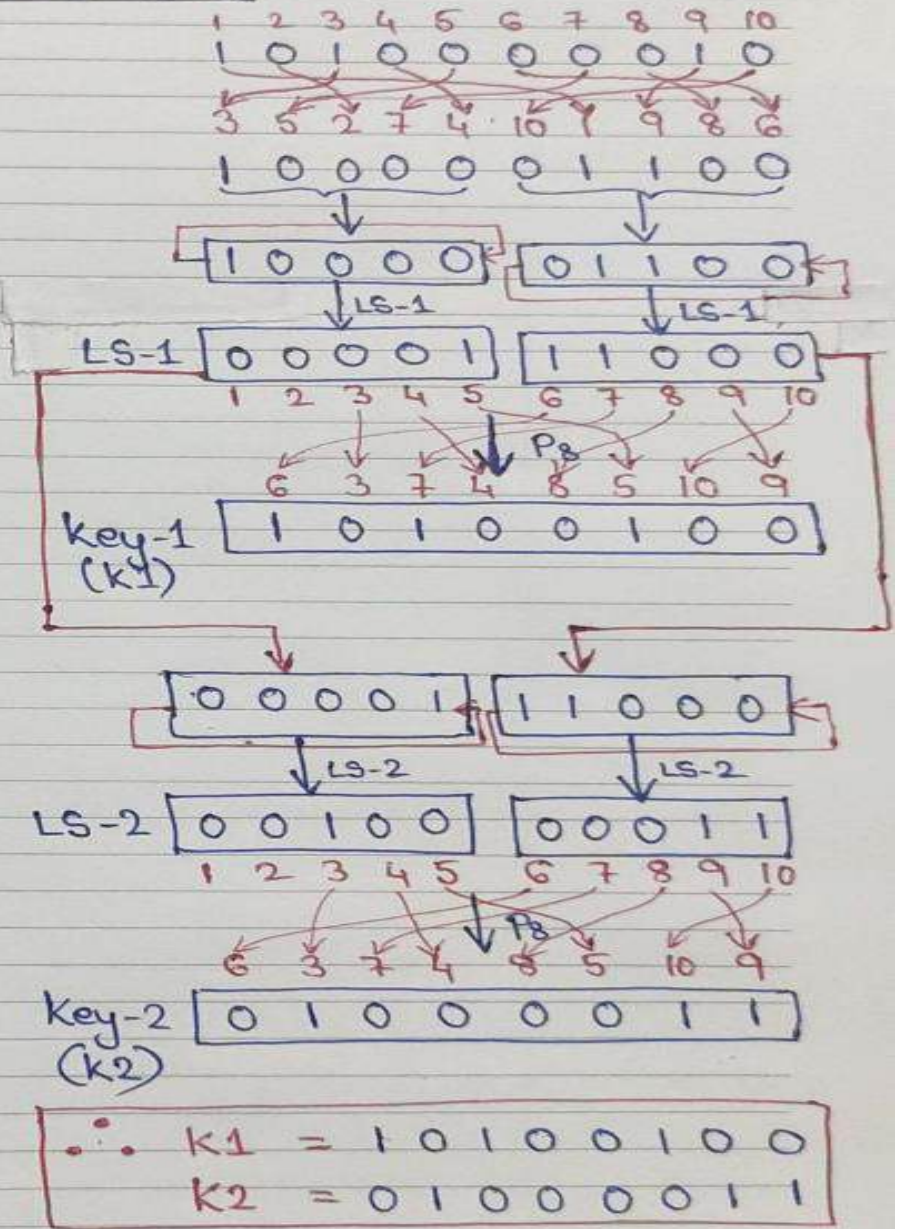
	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

P_4 = 2 4 3 1

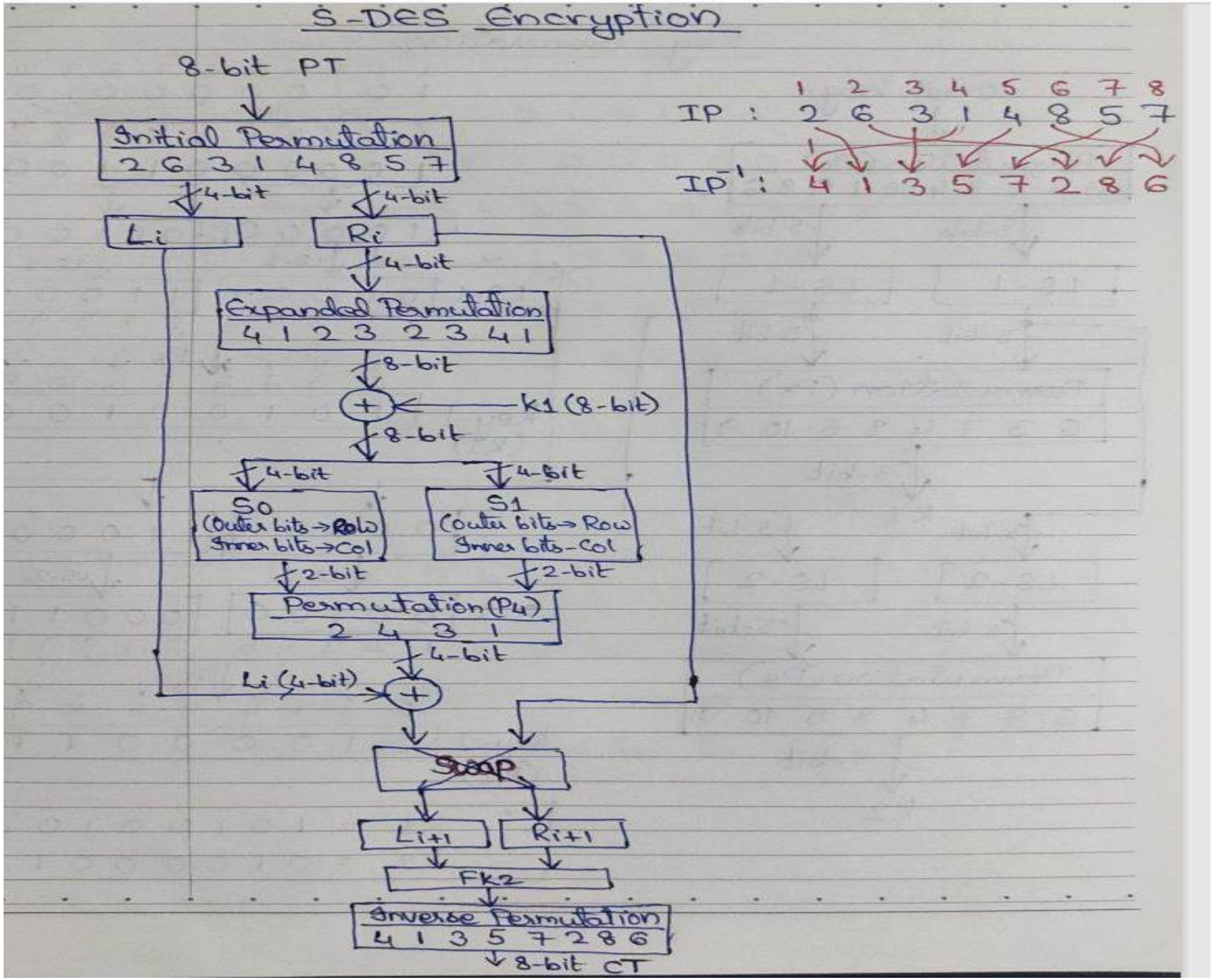
Note: S-boxes S0 & S1 are 4×4 matrix of range (0-3)
To convert 8-bits to 4-bits

Key - Generation

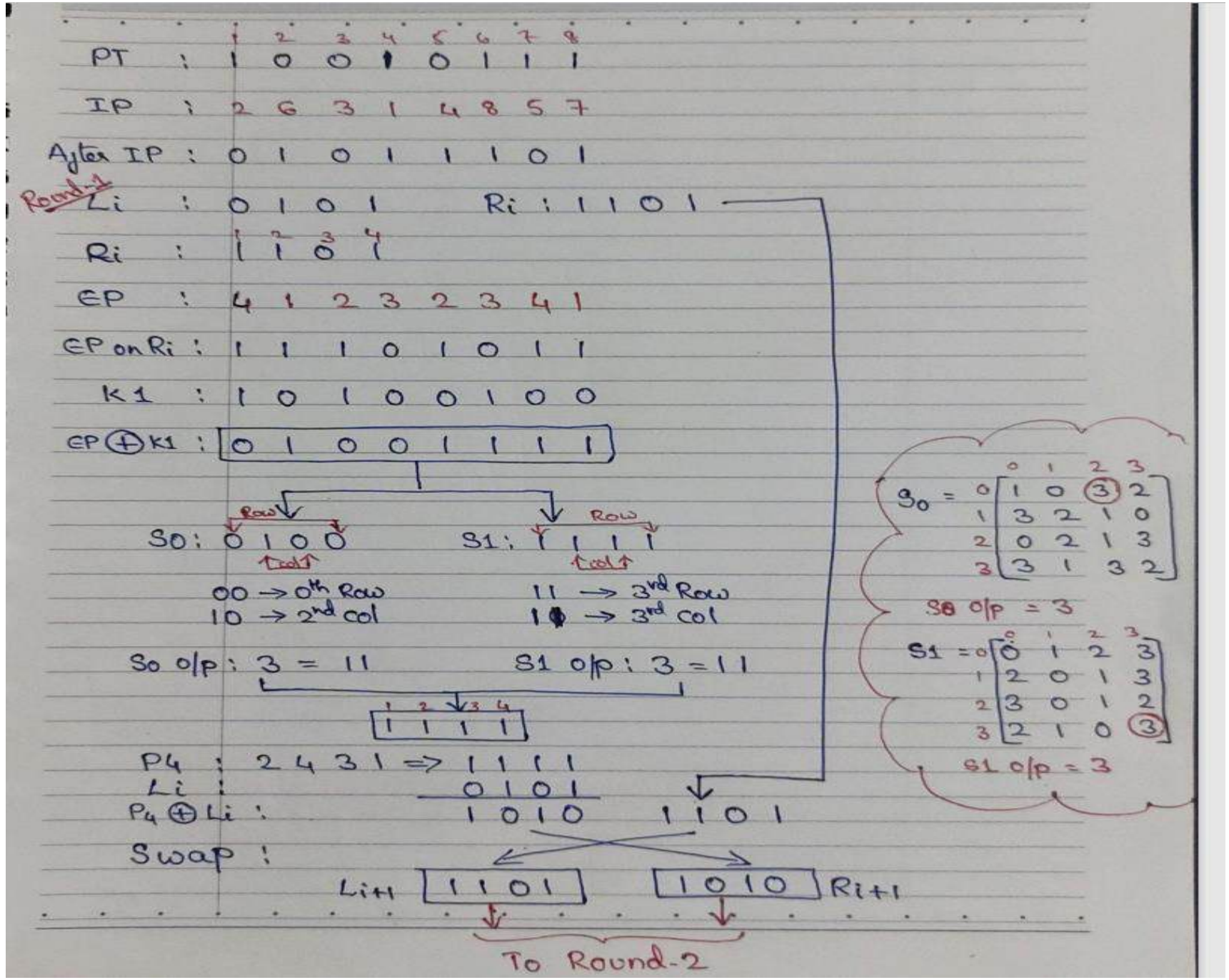


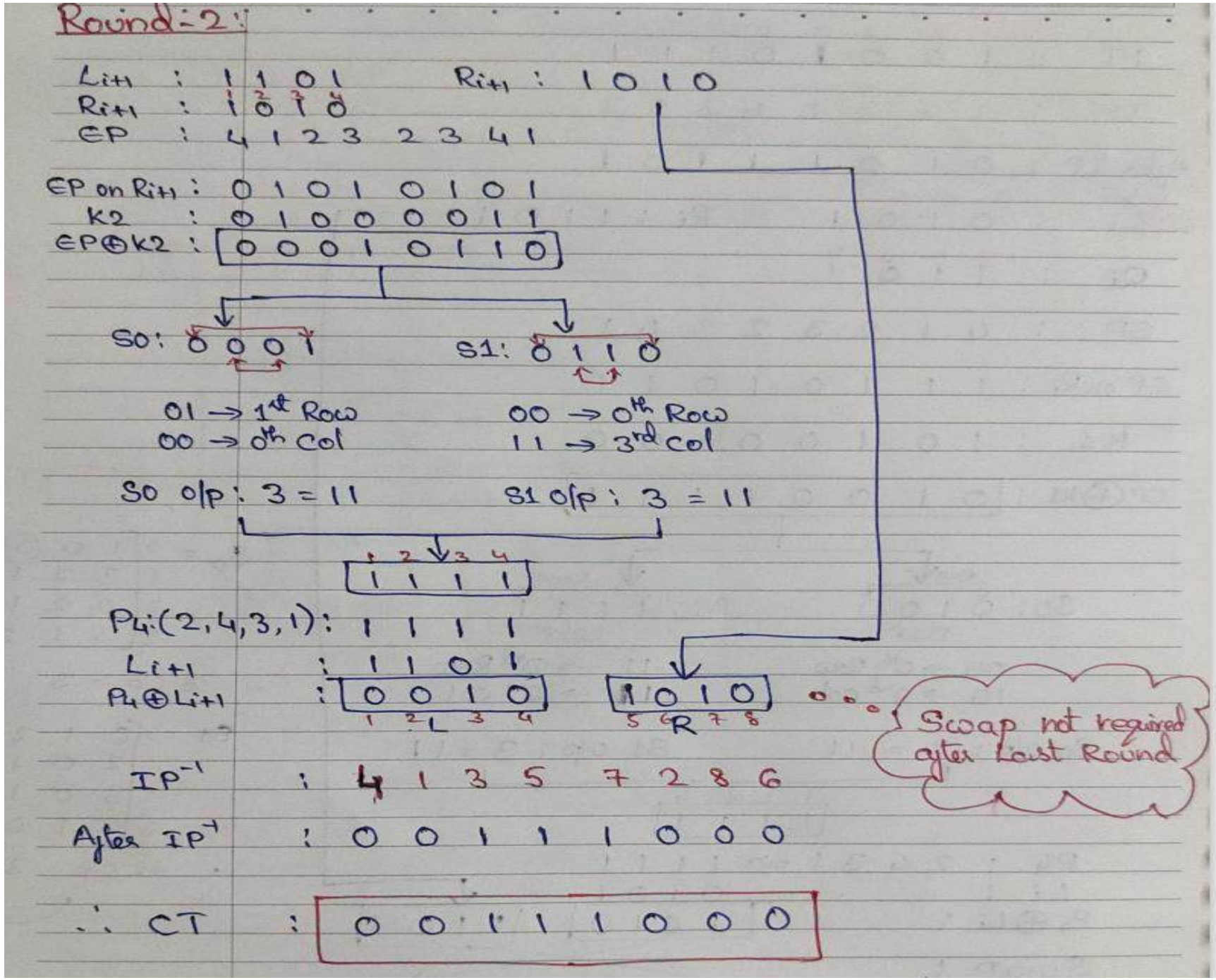


S-DES Encryption



	1	2	3	4	5	6	7	8
IP :	2	6	3	1	4	8	5	7
IP^{-1} :	4	1	3	5	7	2	8	6


PT : 1 0 0 1 0 1 1 1
IP : 2 6 3 1 4 8 5 7
After IP : 0 1 0 1 1 1 0 1
Round-1
Li : 0 1 0 1 Ri : 1 1 0 1
Ri : 1 1 0 1
EP : 4 1 2 3 2 3 4 1
EP on Ri : 1 1 1 0 1 0 1 1
K1 : 1 0 1 0 0 1 0 0
EP ⊕ K1 : 0 1 0 0 1 1 1 1
Row
Row
S0 : 0 1 0 0
S1 : 1 1 1 1
Col
Col
00 → 0th Row
10 → 2nd col
11 → 3rd Row
1● → 3rd col
S0 o/p : 3 = 11
S1 o/p : 3 = 11
P4 : 2 4 3 1 ⇒ 1 1 1 1
Li : 0 1 0 1
P4 ⊕ Li : 1 0 1 0
1 1 0 1
Swap :
Li+1 1 1 0 1
1 0 1 0 Ri+1
To Round-2
S0 = 0 1 0 3 2
1 3 2 1 0
2 0 2 1 3
3 3 1 3 2
S0 o/p = 3
S1 = 0 0 1 2 3
1 2 0 1 3
2 3 0 1 2
3 2 1 0 3
S1 o/p = 3


Round-2:
Li+1 : 1 1 0 1
Ri+1 : 1 0 1 0
EP : 4 1 2 3 2 3 4 1
EP on Ri+1 : 0 1 0 1 0 1 0 1
K2 : 0 1 0 0 0 0 1 1
EP⊕K2 : 0 0 0 1 0 1 1 0
S0: 0 0 0 1
S1: 0 1 1 0
01 → 1st Row
00 → 0th Col
00 → 0th Row
11 → 3rd Col
S0 o/p: 3 = 11
S1 o/p: 3 = 11
1 2 3 4
1 1 1 1
P4:(2,4,3,1): 1 1 1 1
Li+1 : 1 1 0 1
P4⊕Li+1 : 0 0 1 0
1 2 L 3 4
1 0 1 0
5 6 R 7 8
Swap not required after last Round
IP-1 : 4 1 3 5 7 2 8 6
After IP-1 : 0 0 1 1 1 0 0 0
∴ CT : 0 0 1 1 1 0 0 0