Name: Ayush Jain

SAP ID: 60004200132
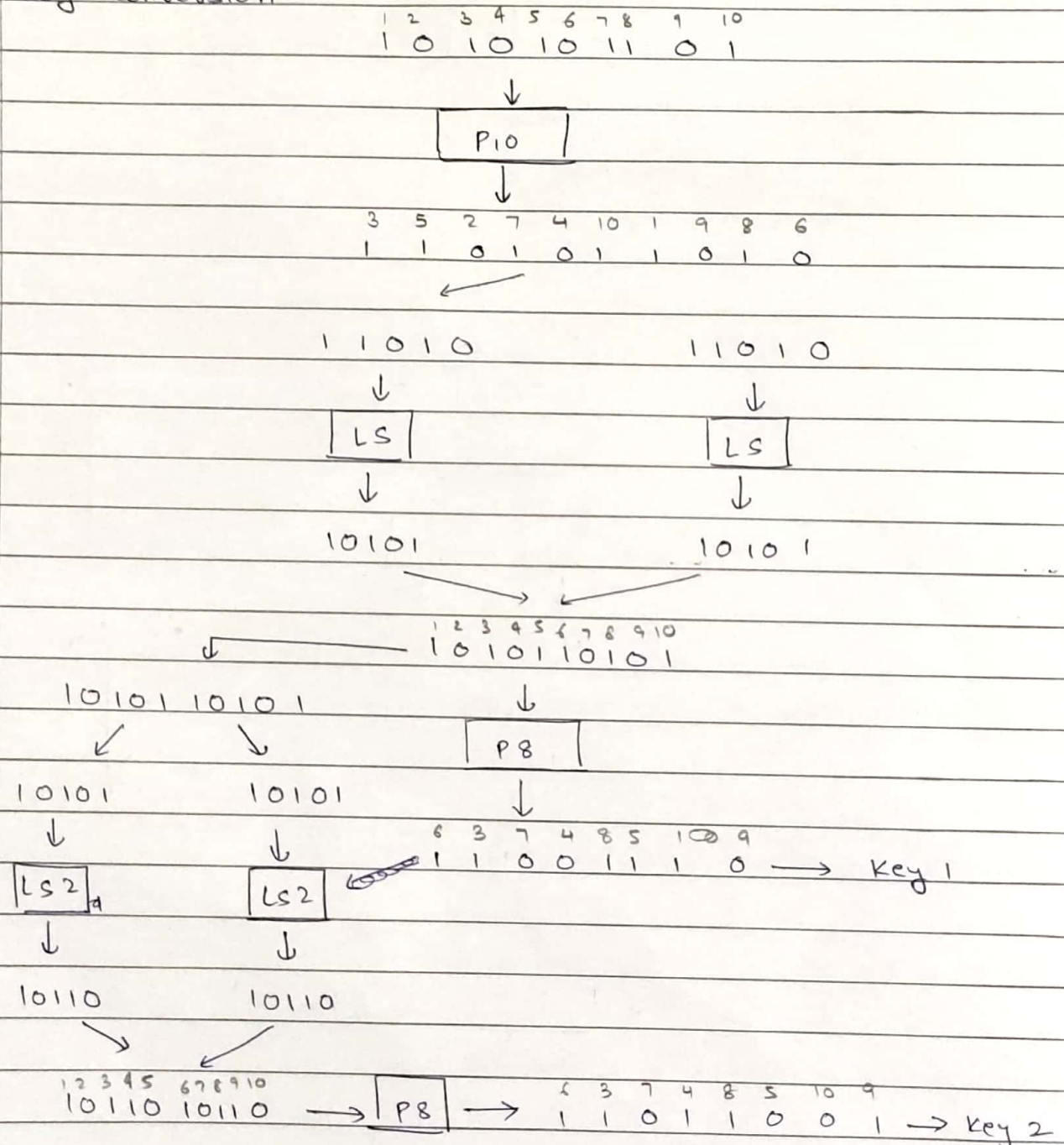
DIV: B

Computer Engineering

INS- Assignment 1

S-DES

1. Plaintext = FC (Hex)   and   Key Sequence = 1010101101

→   FC = $(15\ 12)_{10}$ = $(1111\ 1100)_2$

Key conversion:

1	2	3	4	5	6	7	8	9	10
1	0	1	0	1	0	11		0	1

↓

[P10]

↓

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

↙

1 1 0 1 0   1 1 0 1 0

↓   ↓

[LS]   [LS]

↓   ↓

10101   10101

↘   ↙

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

↓

[P8]

↓

6	3	7	4	8	5	10	9
1	1	0	0	11	1	0	→ Key 1

↓

10101 10101

↙   ↘

10101   10101

↓   ↓

[LS 2]   [LS2]

↓   ↓

10110   10110

↘   ↙

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

→ [P8] →

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

Sundaram

Consider PT:
1 2 3 4 5 6 7 8
1 1 1 1 1 1 0 0

↓

| IP |

↓

2 6 3 1 4 8 5 7   1 2 3 4
1 1 1 1 1 0 1 0   1 0 1 0

(i) ⌐⌐⌐⌐   ↳ (ii)

↓

| EP |

↓

4←4 1 2 3   2 3 4 1
0 1 0 1   0 1 0 1

↓

⊕ ← key 1

↓

0 1 0 1 0 1 0 1
⊕ 1 1 0 0 1 1 1 0
――――――――――――
1 0 0 1 1 0 1 1

row
1 0 0 1
column

row = (11)₂ = 3
Column = (00)₂ = 0

$row = (11)_2 = 3$
$Column = (00)_2 = 0$

↓   ↓
| S0 | | S1 |

↓   ↓
1 1   0 1

⌐⌐⌐⌐⌐⌐
1 2 3 4
1 1 0 1

↓

(P4)

↓

2 4 3 1
1 1 0 1

⊕ 1 1 1 1 — (from i)
――――――――
0 0 1 0

Given: 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

$$0\ 0\ 1\ 0 \qquad 1\ 0\ 1\ 0$$

$$\downarrow \qquad\qquad \downarrow$$

$$1\ 0\ 1\ 0 \qquad 0\ 0\ 1\ 0$$

$$A \qquad\qquad B$$
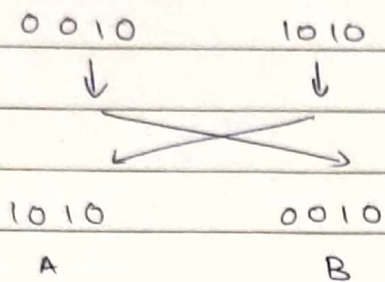
$$\overset{1\ 2\ 3\ 4}{0\ 0\ 1\ 0} \longrightarrow (c)$$

$$\downarrow$$

$$\boxed{EP}$$

$$\downarrow$$

$$\overset{4\ \ 1\ \ 2\ \ 3\ \ 2\ \ 3\ \ 4\ \ 1}{0\ 0\ 0\ 1\ 0\ 1\ 0\ 0}$$

$$\oplus \quad 1\ 1\ 0\ 1\ 1\ 0\ 0\ 1$$

$$\overline{}$$

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

(S0) (S1)

$$row = 2 \qquad\qquad row = 3$$
$$col = 2 \quad\downarrow \qquad \downarrow \quad col = 2$$

$$0\ 1 \qquad\quad 0\ 0$$

$$0\ 1\ 0\ 0$$

$$\downarrow$$

(Pu)

$$\downarrow$$

$$\overset{2\ \ 4\ \ 3\ \ 1}{1\ 0\ 0\ 0}$$

$$\oplus \quad 1\ 0\ 1\ 0 \quad \text{—(from A)}$$

$$0\ 0\ 1\ 0$$

$$\overset{1\ 2\ 3\ 4\ \ 5\ 6\ 7\ 8}{0\ 0\ 1\ 0\ \ 0\ 0\ 1\ 0}$$

$$\downarrow$$

$$\boxed{JP^{-1}}$$

$$\downarrow$$

$$\overset{4\ \ 1\ \ 3\ \ 5\ \ 7\ \ 2\ \ 8\ \ 6}{CT = (0\ 0\ 1\ 0\ 1\ 0\ 0\ 0)} \longrightarrow CT\ (28)_{16}$$

Sundaram

Page 3