JUNAID GIRKAR
60004190057.

S-DES

www.jeevandeep.in
PAGE NO.
DATE: / /

PT = FC

Key = 1010 101101

S-1) 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 1 1 0 1

P_{10}

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

1 1 0 1 0 | 1 1 0 1 0

LS | LS

1 0 1 0 1 | 1 0 1 0 1

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

1 0 1 0 1 1 0 1 0 1

P_8

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

Key1 =

1 0 1 0 1 | 1 0 1 0 1

LS-2 | LS-2

1 0 1 1 0 | 1 0 1 1 0

1 0 1 1 0 1 0 1 1 0

P_8

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

= key 2.

Consider P4 = 1 2 3 4 5 6 7 8
1 1 1 1 1 1 0 0

↓

IP

↓

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

(i) ← | → (ii)

EP

↓

0 1 0 1 0 1 0 1
4 1 2 3 2 3 4 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 row

↙ ↘

S_0 S_1

↓ ↓

$(3)_{10}$ $(1)_{10}$

$(11)_2$ $(01)_2$

↘ ↙

1 1 0 1

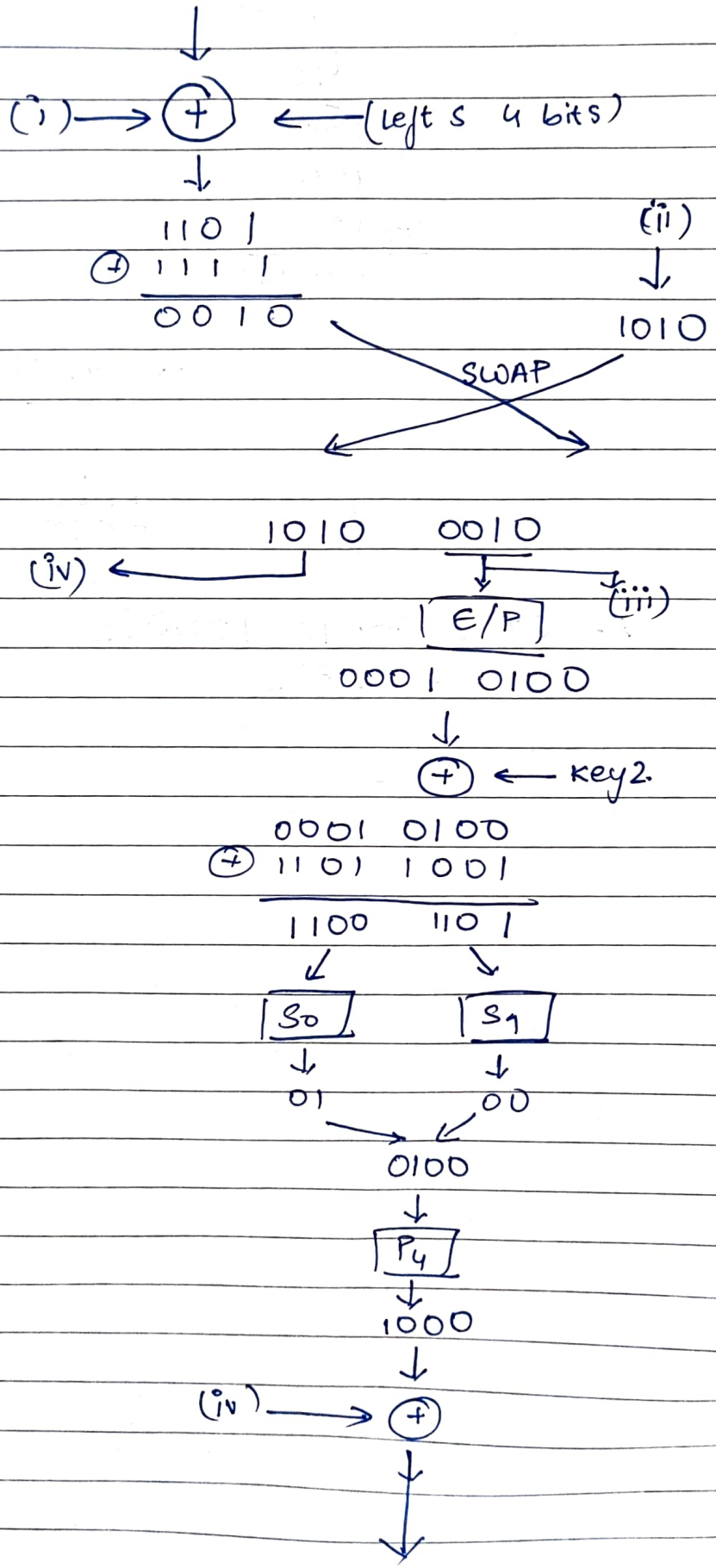
↓

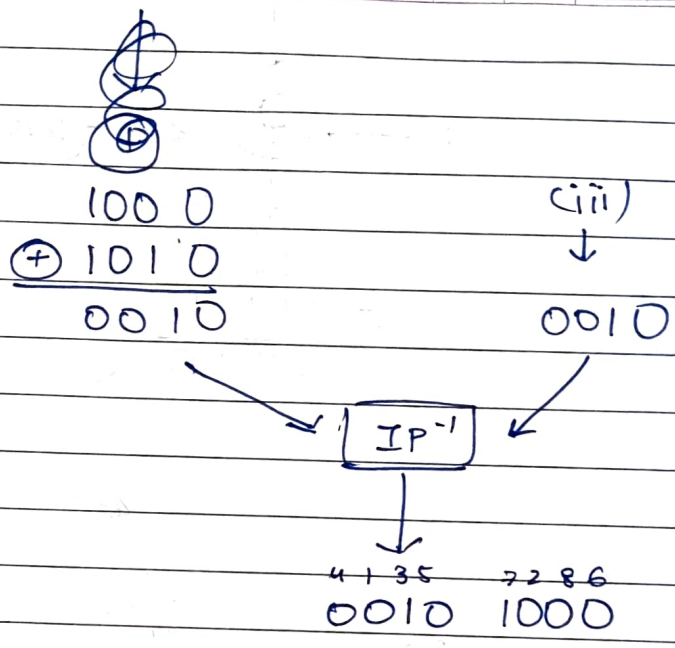
P_4

↓

1 1 0 1
2 3 4 1

↓





$\therefore$ CT = $(0010\ 1000)_2$

$= (28)_{16}$