Assignment

(a) pc1

KL

0 1 1 1 0 0 1
1 1 0 1 0 1 1
0 1 1 1 0 1 0
0 1 1 1 0 1 1

KR

1 1 1 1 1 0 0
1 0 0 1 0 1 1
1 0 0 1 0 1 0
0 1 0 1 1 0 0

Left circular shift.

1 2 3 4 5 6 7
1 1 1 0 0 1 1
8 9 10 11 12 13 14
1 0 1 0 1 1 0
15 16 17 18 19 20 21
1 1 1 0 1 0 0
22 23 24 25 26 27 28
1 1 1 0 1 1 0

29 30 31 32 33 34 35
1 1 1 1 0 0 1
36 37 38 39 40 41 42
0 0 1 0 1 1 1
43 44 45 46 47 48 49
0 0 1 0 1 0 0
50 51 52 53 54 55 56
1 0 1 1 0 0 1

pc2

0 1 0 1 1 0
1 0 1 1 0 1
1 1 1 0 1 1
1 1 1 0 1 0
1 1

14 17 11 24 1 5
3 28 15 6 21 10
23 19 12 4 26 8
16 07 27 20 13 2
41 52 31 37 47 55
30 40 51 45 33 48
44 49 39 56 34 53
46 42 50 36 29 32

first 4 bits are:

0101

(5) 0x53

5th row
3rd col in S-Box

⇒ ed

(6) 0xfc

⇒ 10

4th row
12th col

(7)

- [23 c4 c7 e1]
1. [1a be c7 9a]
2. [42 04 46 c5]
3. [c2 5d 3a 18]

⇒ [23 c4 c7 e1]

[be c7 9a 1a]

[46 c5 42 04]

[18 c2 5d 3a]

(8) [f1 f3 a4 7b]

[7e d1 d2 19]

[fb d2 da 15]

[f1 bi ee]

ft

After applying shift row:

$$\begin{bmatrix} f1 & f3 & a4 & 76 \\ f1 & d2 & 19 & 7e \\ da & 15 & fd & d2 \\ ee & ff & ff & b1 \end{bmatrix}$$

⑨ Imp

$$\begin{bmatrix} 23 & c4 & c7 & e1 \end{bmatrix}$$

$$\begin{bmatrix} 1A & be & c7 & 9a \end{bmatrix}$$

$$\begin{bmatrix} 42 & 04 & 46 & c5 \end{bmatrix}$$

$$\begin{bmatrix} c2 & 5d & 3a & 18 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 23 & c4 & c7 & e1 \\ 1A & be & c7 & 9A \\ 42 & 04 & 46 & c5 \\ c2 & 5D & 3A & 18 \end{bmatrix}$$

$\Rightarrow (02 * 23)$ ⑦

$02 = 00000010 = x$ $\quad x(x^5 + x + 1)$

$23 = 00100011 = x^5 + x + 1$ $\quad = x^6 + x^2 + x$

$\Rightarrow$ ~~0100~~ $x^6 + x^2 + x$.

$\Rightarrow 01000110$

(03 * 1A)

⇒ 03 = 0 0 0 0 0 0 1 1 = $x + 1$

1A = 0 0 0 1 1 0 1 0 = $x^4 + x^3 + x$

$(x+1)(x^4 + x^3 + x)$

$x^5 + x^4 + x^2 + x^4 + x^3 + x$

$x^5 + x^2 + x^3 + x$

⇒ 0 0 0 1 0 1 1 1 0

(01 * 42)

01 = 0 0 0 0 0 0 0 1 = 1

42 = 0 1 0 0 0 0 1 0 = $x^6 + x$

⇒ $x^6 + x$

⇒ 0 0 1 0 0 0 0 0 1 0

(01 * C2)

01 = 00000001 = 1

C2 = 11 000010 = $x^7 + x^6 + x$

⇒ $x^7 + x^6 + x$

⇒ 0 1 1 0 0 0 0 0 1 0

0 0 1 0 0 0 1 1 0
0 0 0 1 0 1 1 1 0
0 0 1 0 0 0 0 1 0
0 1 1 0 0 0 0 1 0

0 1 1 1 0 1 0 0 0

⇒

(10)

5b	ec	e5	50
a8	ce	47	84
10	09	f9	c8
c4	a5	fc	76

Scanned by SCANit App

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 5b & ec & e5 & 50 \\ a8 & cc & 47 & 84 \\ 10 & 09 & f9 & 48 \\ c4 & a5 & fc & 76 \end{bmatrix}$$

02 * 5b

02 = 00000010 = x

5b = 01011011 = $x^6 + x^4 + x^3 + x + 1$

$\Rightarrow x^7 + x^5 + x^4 + x^2 + x$

$\Rightarrow$ 10110110

03 * a8

03 = 00000011 = $x + 1$

a8 = 10101000 = $x^7 + x^5 + x^3$

$(x+1)(x^7 + x^5 + x^3)$

$\Rightarrow x^8 + x^6 + x^4 + x^7 + x^5 + x^3$

Since we got x^8 in equation we need to use irreducible polynomial theorem i.e $x^8 = x^4 + x^3 + x + 1$

$\Rightarrow x^4 + x^3 + x + 1 + x^6 + x^4 + x^7 + x^5 + x^3$

$\Rightarrow x^7 + x^6 + x^5 + x + 1 \Rightarrow$ 11100011

(01) * (10)

01 = 00000001

10 = 00010000 = x^4

$1(x^4) = x^4$

$\Rightarrow$ 00010000

(01) * c4

01 = 00000001 = 1

c01 = 11000100 = $x^7 + x^6 + x^2$

$= 1(x^7 + x^6 + x^2)$

$\Rightarrow$ 11000100

Apply XOR to all

```
1 0 1 1 0 1 1 0
1 1 1 0 0 0 1 1
1 1 1 0 0 0 0 0
0 0 0 1 0 0 0 0
1 1 0 0 0 1 0 0
-----------------
1 0 0 0 0 0 0 1
```

$(10000001)_2 \xrightarrow{Hex} (81)_{16}$

① By using initial permutation table we get o/p as

```
1 1 0 0 0 1 1 1
1 0 1 1 1 1 0 0
1 1 1 0 0 0 1 0
0 1 0 1 1 1 0 1
1 1 1 1 0 1 0 0
1 0 1 1 1 1 1 1
0 1 1 1 1 0 0 0
0 1 0 1 1 0 1 1
```

② 8-bit i/p to s-box = 101110

row bits = 10 [in bin] $\Rightarrow$ 2 [in decimal]

col bits = 0111 [in bin] $\Rightarrow$ 7 [in dec]

2nd row 7th col

$\Rightarrow$ 7