Ankit Goyal
17103011

ISS ASSIGNMENT-3

2.

(a) Plain text = 1 1 0 1 0 1 0 1
Key = 0 1 1 1 0 1 0 0 0 1

Key Generation :-

(i) After P10 ⇒ 1 0 1 0 1 1 0 0 0 1
L_0 = 1 0 1 0 1 R_0 = 1 0 0 0 1

(ii) After 1- left shift
L_1 = 0 1 0 1 1 R_1 = 0 0 0 1 1

(iv) After P8 : P8 (0 1 0 1 1 0 0 0 1 1) ⇒ 0 0 0 1 0 1 1 1
∴ K_1 = 0 0 0 1 0 1 1 1

(v) After 2- left shift
L_4 = 0 1 1 0 1 , R_4 = 0 1 1 0 0

(vi) After P8 : 0 1 1 0 1 1 0 0
K_2 = 0 1 1 0 1 1 0 0

Encryption :-

(i) Plain text : 1 1 0 1 0 1 0 1
(ii) After IP = 1 1 0 1 1 1 0 0

L = 1 1 0 1 , R = 1 1 0 0
(iii) E/P(R) = 0 1 1 0 1 0 0 1
(iv) 0 1 1 0 1 0 0 1
0 0 0 1 0 1 1 1 (K_1)

After XOR) 0 1 1 1 1 1 1 0

(v) Output of S_0 (0111) = 00
output of S_1 (1110) = 00

(vi) After P_4 : 0 0 0 0

(vii)
```
  0 0 0 0
  1 1 0 1
XOR=> 1 1 0 1
```

(viii) After 1 Round => 1 1 0 0 1 1 0 1
L = 1 1 0 0 , R = 1 1 0 1

(ix) E/p(R) = 1 1 1 0 1 0 1 1

(x)
```
  1 1 1 0 1 0 1 1
  0 1 1 0 1 1 0 0
XOR=> 1 0 0 0 0 1 1 1
```

(xi) S_0(1000) = 00
S_1(0111) = 11
] 0 0 1 1

(xii) After P_4 : 0 1 1 0

(xiii)
```
  0 1 1 0
  1 1 0 0
XOR=> 1 0 1 0
```

(xiv) Text After Round 2 => 1 0 1 0 1 1 0 1
IP^{-1} (1010 1101) => 0 1 1 1 0 0 1 1

∴ Cipher text => 0 1 1 1 0 0 1 1

(B) Plain text : 0 1 0 0 1 1 0 0

Key : 1 1 1 1 1 1 1 1 1 1

Key Generation :

After P_{10} : 1 1 1 1 1 1 1 1 1 1

L : 1 1 1 1 1 , R = 1 1 1 1 1

→ Left shift (L1)

L : 1 1 1 1 1 , R = 1 1 1 1 1

→ P8 (1 1 1 1 1 1 1 1 1 1) → 1 1 1 1 1 1 1 1

K_1 = 1 1 1 1 1 1 1 1

→ Left shift (2)

L = 1 1 1 1 , R = 1 1 1 1 1

→ P8 (1 1 1 1 1 1 1 1 1 1) → 1 1 1 1 1 1 1 1

K_2 = 1 1 1 1 1 1 1 1

Encryption

- Plain text: 0 1 0 0 1 1 0 0
- IP(0 1 0 0 1 1 0 0) = 1 1 0 0 0 0 1 0
- L = 1 1 0 0 , R = 0 0 1 0
- EP(R) = 0 0 0 1 0 1 0 0

0 0 0 1 0 1 0 0

⊕ 1 1 1 1 1 1 1 1 (K_1)

1 1 1 0 1 0 1 1

- $S_0(1110) = 11$ } $\Rightarrow 1101$
  $S_1(1011) = 01$

- $P_4(1101) = 1101$
- $1101 \oplus 1100 = 0001$
- After Round1 $\Rightarrow$ 00100001

- $L_0 = 0010$, $R = 0001$
- $E(R) = 10000010$

$$\begin{array}{r} 10000010 \\ \oplus\ 11111111 \quad K_2 \\ \hline 01111101 \end{array}$$

- $S_0(0111) = 00$ } $\Rightarrow 0000$
  $S_1(1101) = 00$

- $P_4(0000) = 0000$

$$\begin{array}{r} 0000 \\ \oplus\ 0010 \\ \hline 0010 \end{array}$$

Round 2 $\Rightarrow$ 00100001

$IP^{-1}(00100001) \Rightarrow 00100010$

$\therefore$ Cipher text $\Rightarrow$ 00100010

Page No.
Date : / /20

(c) Plain text : 0 0 00 0 0 0 0

Key : 0 0 0 0 0 0 0 0 0 0

Key Generation :

- P_{10} = 0 0 0 0 0 0 0 0 0 0
- L = 0 0 0 0 0 , R = 0 0 0 0 0
- Left shift (L) : 0 0 0 0 0
  (R) : 0 0 0 0 0
- P_8 : 0 0 0 0 0 0 0 0
  K_1 = 0 0 0 0 0 0 0 0
- Left shift (2) :
  L = 0 0 0 0 0
  R = 0 0 0 0 0
- P_8 : 0 0 0 0 0 0 0 0
  K_2 = 0 0 0 0 0 0 0 0

Encryption :

- Plain text = 0 0 0 0 0 0 0 0
- IP = 0 0 0 0 0 0 0 0
- L = 0 0 0 0 , R = 0 0 0 0
- E/P(R) = 0 0 0 0 0 0 0 0

  0 0 0 0 0 0 0 0
  ⊕ 0 0 0 0 0 0 0 0 (K)
  0 0 0 0 0 0 0 0

Page No.
Date : / /20

$S_0(0000) = 01$ } 0100
$S_1(0000) = 00$

$P_4(0100) = 1000$

$1000 \oplus 0000 \Rightarrow 1000$

Round 1: 0000 1000
L = 0000 , R = 1000

$E/P(R) = 01000000$

$$\begin{array}{r} 0100\ 0001 \\ \oplus\ 0000\ 0000 \quad \text{(KY)} \\ \hline 0100\ 0001 \end{array}$$

$S_0(0100) = 11$ } 1110
$S_1(0001) = 10$

$P_4(1110) = 1011$

$1011 \oplus 0000 = 1011$

After Round 2 $\Rightarrow$ 10111000

$IP^{-1}(10111000) = 11110000$

Cipher text $\Rightarrow$ 11110000

(1) Plain text ⇒ 11111111

Key ⇒ 1111111111

Key Gen ⇒

P10 ⇒ 1111111111

L ⇒ 11111 , R = 11111

⇒ Shift 1 ⇒

L = 11111 , R = 11111

P8 = 11111111

∴ K1 = 11111111

⇒ Shift 2 ⇒

L = 11111 , R = 11111

⇒ P8 = 11111111

K2 = 11111111

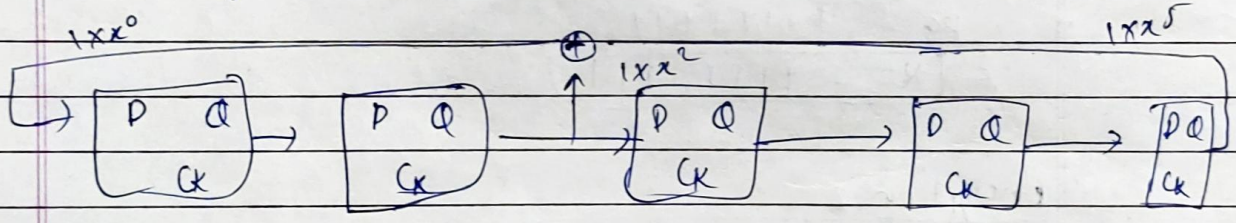
Encryption

- plaintext ⇒ 11111111
- IP ⇒ 1111 1111
- L ⇒ 1111 , R = 1111
- EP(R) = 1111 1111
- 11111111 ⊕ 11111111 ⇒ 00000000
- S_0(0000) = 01 } 0100
  S_1(0000) = 00 }
- P4 = 1000
- 1000 ⊕ 1111 ⇒ 0111
- After Round 1 ⇒ 1111 0111
- L = 1111 , R = 0111
- EP(R) = 10111110
- 10111110 ⊕ 11111111 ⇒ 01000001
- S_0(0100) = 11 } 1110
  S_1(0001) = 10 }

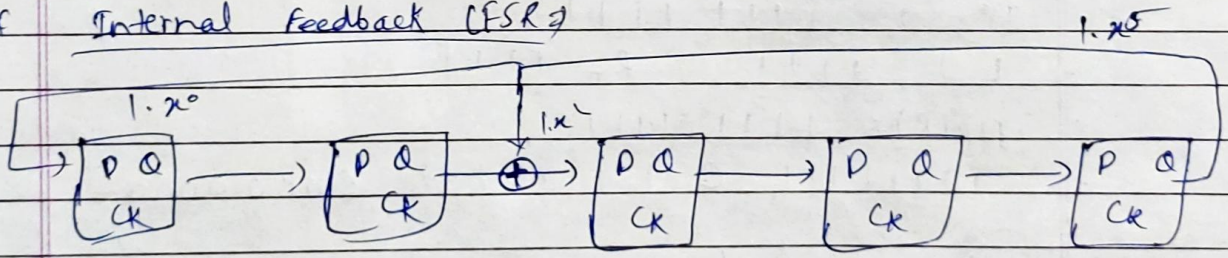
- $P_4 = 1011$
- $1011 \oplus 1111 \Rightarrow 0100$
- After Round 2 $\Rightarrow$ 01000111
- SP^{-1} = 000011111
- ∴ Cipher text = 00001111

1. Polynomial $\Rightarrow$ $x^5 + x^2 + 1$
   degree (n) = 5

* External feedback LFSR $\Rightarrow$



* Internal feedback LFSR $\Rightarrow$



Periods $\Rightarrow$ $2^n - 1 = 2^5 - 1$
$= 32 - 1$
Periods = 31