1810107

Assignment-02

Answer to the question-1

Here,

a) Trudy knows the plaintext P.

if somehow obtains the ciphertext C, trudy can determine the keystream K by the following way :

$$K = C \oplus P.$$

b) From question-① we get,

$$K = C \oplus P \quad -①$$

We can write,

$$C' = K \oplus P'$$

$$= C \oplus P \oplus P' \quad [K = C \oplus P \text{ from } ①]$$

So, Trudy can create a ciphertext message C'.

(showed)

Answer to the Question-2

Given,

$X = 1,0,1,0,1,0,1,0,1,0,1,0,1,0,1$

$Y = 1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1$

$Z = 1,1,1,0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0,0,0$

$majority, m = maj(x_8, y_{10}, z_{10})$

$= maj(1, 0, 1)$

$= 1$

Incase of first bit %

Since, $x_8 = m$

$t = x_3 \oplus x_6 \oplus x_2 \oplus x_0$

$= 0 \oplus 1 \oplus 0 \oplus 1$

$= 1 \oplus 1$

$= 0$

Here

Since, $y_{10} \neq m$.

Y will not shift.

Since, $z_{10} = z_7 \oplus z_{20} \oplus z_{21} \oplus z_{22}$

$= 1 \oplus 0 \oplus 0 \oplus 0$

$= 1 \oplus 0$

$= 1$

New

$X = 0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0$

$Y = 1\,1\,0\,0\;1\,1\,0\,0\;1\,1\,0\,0\;1\,1\,0\,0\;1\,1\,0\,0\;1\,1$

$Z = 1\,1\,1\,1\,0\,0\,0\,0\;1\,1\,1\,1\,0\,0\,0\,0\;1\,1\,1\,1\,0\,0\,0$

First key stream bit is $x_8 \oplus y_{21} \oplus z_{22}$

$= 0 \oplus 1 \oplus 0$

$= 1 \oplus 0$

$= 1$

Incase of 2nd bit's

major, $m = (0 \oplus 0 \oplus 1)$

$= 0 \oplus 1$

$= 1$

Since, $y_{10} \neq m$, y will not shift

$x_8 \neq m$, x will not shift.

$z_{10} = m$, z will shift.

$t = z_2 \oplus z_{21} \oplus z_{22} \oplus z_{20}$

$= 0 \oplus 0 \oplus 0 \oplus 0$

$= 0 \oplus 0$

$= 0$

New

X = 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0

Y = 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1

Z = 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0

2nd key stream bit is $x_2 \oplus y_2 \oplus z_2$

$= 0 \oplus 1 \oplus 0$

$= 1 \oplus 0$

$= 1$

In case of 3rd bit:

majority $= m(0 \oplus 0 \oplus 1)$

$= 1$

X, Y will not shift, Z will shift.

$t = 0 \oplus 1 \oplus 0 \oplus 0$

$= 1$

New,

X = 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0

Y = 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1

Z = 1 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0

3rd bit key stream is $x_{18} \oplus y_{21} \oplus z_{22}$

$= 0 \oplus 1 \oplus 0$

$= 1$

In case of 4th bit :

majority $m = m(0 \oplus 0 \oplus 1)$

$= 1$

Here, only Z will shift.

$t = 0 \oplus 1 \oplus 1 \oplus 0 = 0$

X = 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 0 0

Y = 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1

Z = 0 0 1 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1

4th bit is $x_{18} \oplus y_{21} \oplus z_{22}$

$= 0 \oplus 1 \oplus 1$

$= 0$

Next 4 keystream bits = 1 1 0 (Ans)

Answer to the Question - 3

a) 64 bit

b) 64 bit

c) 56 bit in Key

d) 48 bits in each sub Key

e) 16 rounds

f) 8 S-boxes

g) 48 bit

h) 32 bit

Answer to the Question - 4

In AES,

Add Round Key : Confusion

Shif Row Layer : Diffusion

Mix Column Layer : Diffusion

Byte Substitution : confusion