Assignment 2

Tasnim Sakib Apon
ID : 20241068
CSE 490

Assignment 2

Tasnim Salsabil Apon 20241068

1. (a) chiper text = plain text ⊕ key stream.

$$C_0 = P_0 \oplus S_0$$

Both sender and recivers have same algorithm. In Alice case, Trudy knows the plain text and the chiper text. If he does X-OR operation with plain text and chiper text, then he can get the key stream easily.

$$S_0 = P_0 \oplus C_0 \;,\; S_1 = P_1 \oplus C_1 \;,\; S_2 = P_2 \oplus C_2$$

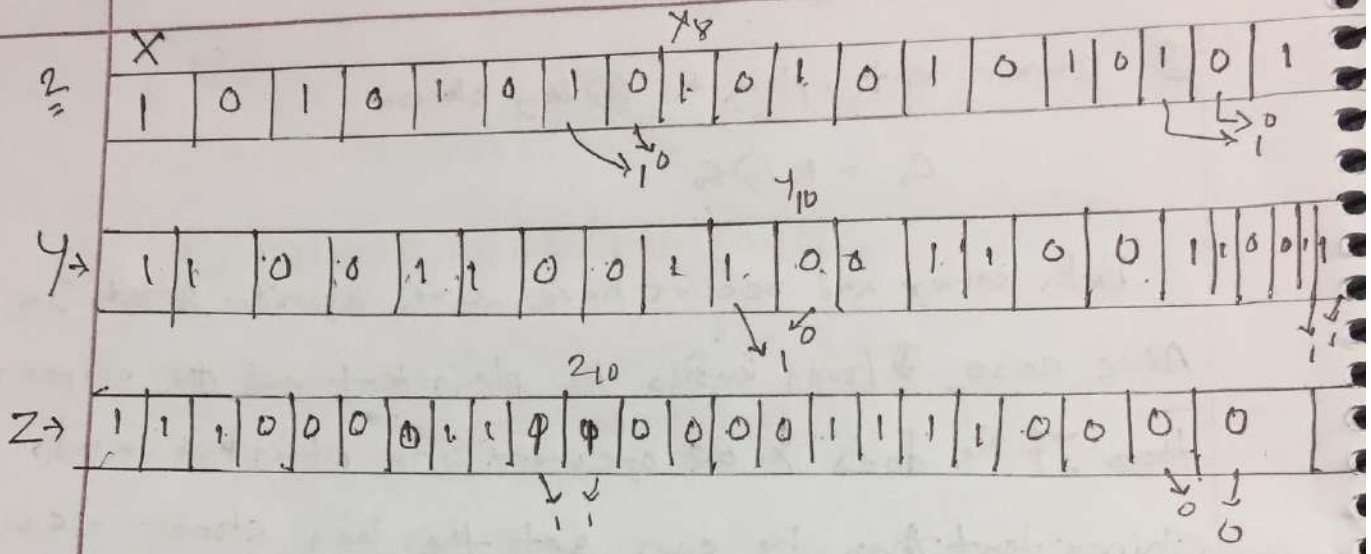
(b) Trudy cannot change the key stream but she can change plain text. P to P'. In order to get a new chiper text C', we can say that trudy will replace the equation of decryption. $C = P \oplus S$ to $C' = P \oplus P \oplus S$

we know, $S = C \oplus P$

to get $C' = P' \oplus S$

we will replace the key and will get

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



$maj(x_8, y_{10}, z_{10}) = maj(1, 0, 1) = 1.$

The 1st key stream bit

$X_8 = 1 = maj$:

so X has to be shifted

value will be placed in new X_0 position.

$X_0 = x_{13} \oplus x_{16} \oplus x_{12} \oplus x_{18}$

Value in $X_0 = 0 \oplus 1 \oplus 0 \oplus 1$

$= 0.$

Likewise

$Z_7 = 1, Z_{20} = 0, Z_{21} = 0, Z_{22} = 0.$

$\therefore Z_7 \oplus Z_{20} \oplus Z_{21} \oplus Z_{22} = 1$

So Now,

$X = 0101010101010101010$

$Y = 11001100110011001100$

$Z = 11110000111100001111000$

$x_{18} \oplus y_{21} \oplus z_{22} = 1$

$\therefore$ 1st key stream bit is 1.

For 2nd keystream bit.

$x_8 = 1,\ y_{10} = 0,\ z_{10} = 1.$

$m = \max(1, 0, 1) = 1$

So registers X steps, Y does not & Z steps.

$z_{13} = 1,\ x_{14} = 0,\ x_{12} = 1,\ x_{18} = 0,$ ~~x 5 +~~

$x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18} = 0$

$z_{17} = 0\ z_{20} = 0,\ z_{21} = 0\ z_{22} = 0$

$\therefore z_{17} \oplus z_{20} \oplus z_{21} \oplus z_{22} = 0$

Now,

$x = 001\,01\,01\,01\,01\,01\,01\,01\,01$

$y = 11\,00\,11\,00\,11\,00\,11\,00\,11$

$z = 0\,1111\,0000\,1111\,0000\,1111\,00.$

$x_{18} = 1 \quad y_{21} = 1 \quad z_{22} = 0$

So ~~$1 \oplus 1 \oplus 0 = 0$~~

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

∴ 2nd key ~~stream~~ bit = 0.

For third key stream bit,

$x_8 = 1, \quad y_{10} = 0 \quad z_{10} = 1$

$m = \text{maj}(1,0,1) = 1$

So register x steps, y doesn't and z steps.

$x_{13} = 1, \quad x_{16} = 1, \quad x_{12} = 0, \quad x_{18} = 1$

∴ $x_{13} \oplus x_{16} \oplus x_{12} \oplus x_{18} = 1.$

$z_7 = 0, \quad z_{20} = 1, \quad z_{21} = 0, \quad z_{22} = 0$

∴ $z_7 \oplus z_{20} \oplus z_{21} \oplus z_{22} = 1.$

Now

$x = 1\,0\,0\,1\,0\,1\,\ 0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0$

$y = 1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1$

$z = 1\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,0$

$x_{18} \oplus y_{21} \oplus z_{22} = 1$

$\therefore$ 3rd bit stream = 1.

4th : $x_8 = 0,\ y_{10} = 0,\ z_{10} = 1$

$\therefore m = maj(0, 0, 1) = 0$

Here x and y will step and z does not step.

$x_{13} = 1,\ x_{14} = 0,\ x_{12} = 1,\ x_{18} = 0.$

$x_{13} \oplus x_{14} \oplus x_{12} \oplus x_{18} = 0.$

$y_{20} = 1,\ y_{21} = 1,$

So $y_{20} \oplus y_{21} = 0$

Now,

$x = 0\,1\,0\,0\,1\,0\,1\ 0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1$

$y = 0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1$

$z = 1\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,0$

$x_{18} = 1$, $y_{21} = 1$ $z_{22} = 0$

So $x_{18} \oplus y_{21} \oplus z_{22} = 0$

∴ 4th key stream bit = 0.

∴ Next 4 key stream bit = 1010

3. (a) Bits in each plain text ⇒ 64

(b) Bits in each chiper text ⇒ 64

(c) Bits in the key ⇒ 56

(d) Bits in each subkey ⇒ 48

(e) Number of rounds ⇒ 16

(f) Number of S-boxes ⇒ 8

(g) Number of bits of input for S-box ⇒ 6

(h) Numbers of bits of output of S-box ⇒ 4

4 In AES Add round key and byte substitution layer are used for confusion. The concept of confusion is making the relationship between the key and the chiper text. It increases the ambigity of chiper text. So Adding round key and byte substitution in AES is considered as confusion.

The shift row layers and mix column layers are used for defusion. The aim of defusion is to hide the relationship between ~~pain~~ plain and chiper text, so that attacker can easily find out the plain text. In AES, shift rows and mix column layers make the plain text ~~complicat~~ complicated to understand.