NAME : JAWAD AHMED

ROLL NO : 20P-0165

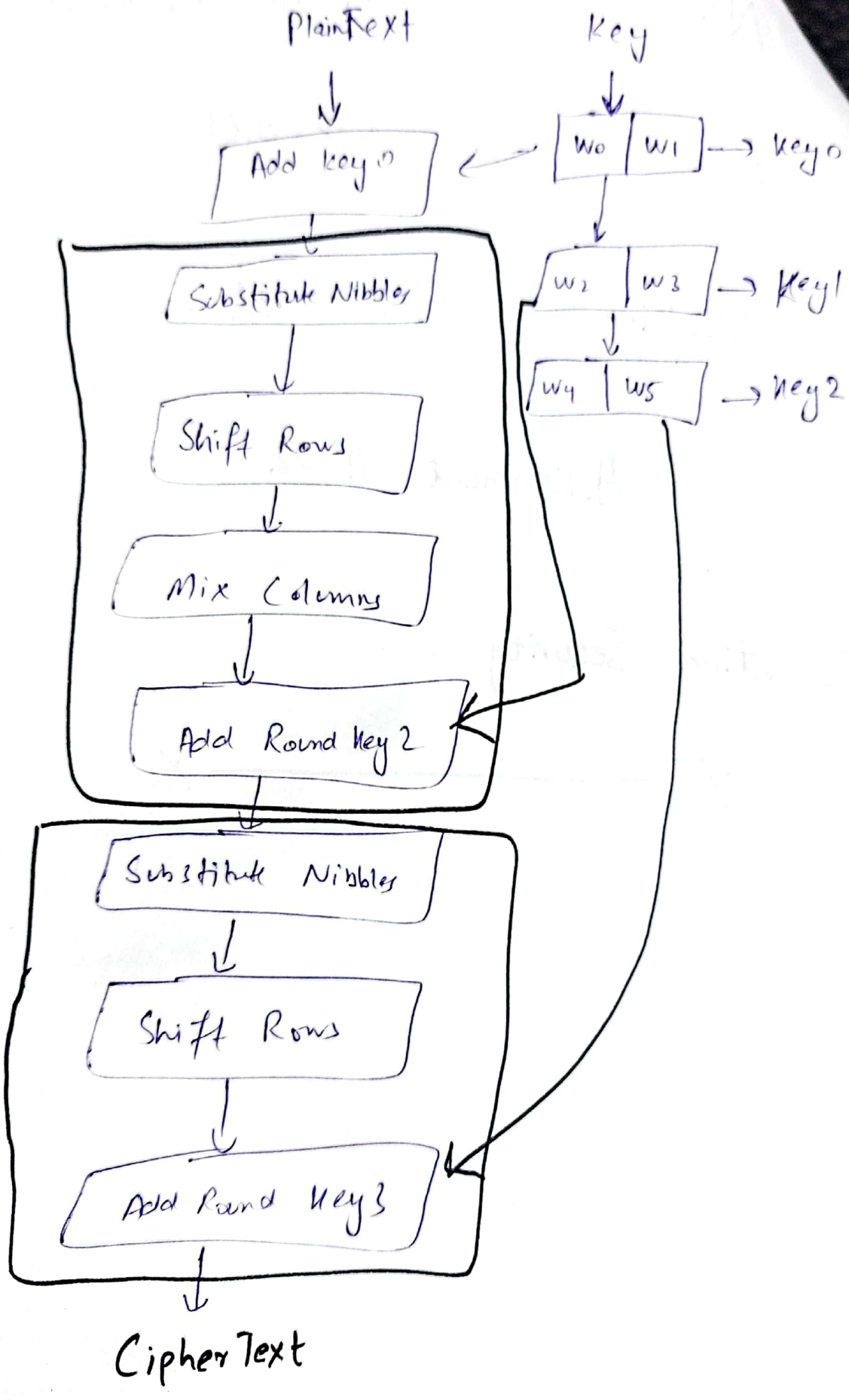
Section : BCS-7A

Assignment # 02

Information Security

X ——————————— X

S-AES Diagram



Simplified AES

:-

PlainText (16 Bit) = 1101 0111 0010 1000

Key (16-Bit) = 0100 1010 1111 0101

Solution:-

Step1: Key Generation

① Split key into two words

w_0 = 0100 1010

w_1 = 1111 0101

We need to find ③ round keys.

$key_0 = w_0\ w_1$

$key_1 = w_2\ w_3$

$key_2 = w_4\ w_5$

Find w_2

w_2 = w_0 XOR 1000 0000 XOR SubNib(RotNib(w_1))

→ Ⓐ

RotNib ⇒ Move left 4 bits to right and right 4 bits to left.

SubNib ⇒ Take left and right 4 bit and see Table and replace those nibble with Table corresponding value.

Put w_0 & w_1 in (A)

$W_2 = 0100\ 1010 \oplus 1000\ 0000 \oplus \text{SubNib}(\text{RotNib}(1111\ 0101))$

$= 0100\ 1010 \oplus 1000\ 0000 \oplus \text{SubNib}(0101\ 1111)$

$= 0100\ 1010 \oplus 1000\ 0000 \oplus 0001\ 0111$

$= 1100\ 1010 \oplus 0001\ 0111$

$W_2 = 1101\ 1101$

$W_3 = W_2 \text{ XOR } W_1$

$= 1101\ 1101 \oplus 1111\ 0101$

$W_3 = 0010\ 1000$

$= W_2 \text{ XOR } 00110000 \text{ XOR } SubNib(RotNib(W_3))$ (3)

$= 1101\ 1101 \oplus 0011\ 0000 \oplus SubNib(RotNib(0010\ 1000))$

$= 1101\ 1101 \oplus 0011\ 0000 \oplus SubNib(1000\ 0010)$

$= 1101\ 1101 \oplus 0011\ 0000 \oplus 0110\ 1010$

$= 1110\ 1101 \oplus 0110\ 1010$

$W_4 = 1000\ 0111$

$W_5 = W_4 \text{ XOR } W_3$

$= 1000\ 0111 \oplus 0010\ 1000$

$W_5 = 1010\ 1111$

Sub-key are:

$Key_0 = W_0\ W_1$

$= 0100\ 1010\ 1111\ 0101$

$Key_1 = W_2\ W_3$

$= 11011101\ 00101000$

$Key_2 = w_4\ w_5$

$= 1000\ 0111\ 1010\ 1111$

Step2:- Encryption

① Add Round 0 Key

= PlainText XOR Key0

= 1101 0111 0010 1000 ⊕ 0100 1010

1111 0101

= 1001 1101 1101 1101

② Nibble Substitution

= 0010 1110 1110 1110

③ Mix Column

$$m_e = \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}, \quad S = \begin{bmatrix} 0010 & 1110 \\ 1110 & 1110 \end{bmatrix}$$

$S' = m_e \times S$

$= 0010 \text{ XOR } (4 \times 1110)$

$= 0010 \text{ XOR } (4 \times E)$

$= 0010 \text{ XOR } (D)$

$= 0010 \text{ XOR } 1101$

In Hex 1110 = E

See Table 4XE the value = D

replace D with Hex value

$S_{00}' = 1111$

Calculate other values S_{10} S_{01} S_{11}

Output = S_{00}' S_{10}' S_{01}' S_{11}'

= 1111 0110 0011 0011

Add Round 1 Key

(1) Nibble Substitution (S-boxes)

= 1010 0011 0100 0011

(2) Shift Rows (2) & (4)

= 1010 0011 0100 0011

③ Add Round 2 Key

= 1010 0011 0100 0011 ⊕ 1000 0111 1010

cipher-text = 0010 0100 1110 1100

Decryption

① Add Round 2 key

= 0010 0100 1110 1100 ⊕

1000 0111 1010 1111

= 1010 0011 0100 0011

② Inverse of Shift row

= 1010 0011 0100 0011

③ Inverse of Nibble Substitution

= 0010 1011 0001 1011

Add Round Key

= 0010 1011 ⊕ 0001 1011

1101 1101 ⊕ 0010 1000

= 1111 0110 ⊕ 0011 0011

(5) Inverse of Mix Column.

1111 0011

0110 0011

$$S' = \begin{bmatrix} S_{00}' & S_{01}' \\ S_{10}' & S_{11}' \end{bmatrix}$$

$$= \begin{bmatrix} 9 \times S_{00} \oplus 2 \times S_{10} & 9 \times S_{01} \oplus 2 \times S_{11} \\ 2 \times S_{00} \oplus 9 \times S_{10} & 2 \times S_{01} \oplus 9 \times S_{11} \end{bmatrix}$$

Output = 0010 1110 1110 1110

(5) Inverse of Shift Row

= 0010 1110 1110 1110

(6) Inverse of Nibble Sub

= 1001 1101 1101 1101

(7) Add Round 0 key

= 1D01 1101 1101 1101

⊕ 0100 1010 1111 0101

Plaintext = 1101 0111 0010 1000

Decryption works!