# ASSIGNMENT #02

FAROOQ HAIDER · SE7A - 20P 0091

Q. Encryption Decryption using S-AES

Key: 1010 0111 0011 1011

PT: 0110 1111 0110 1011

Sol:- ① Key Generation

Key: $\underbrace{1010\ 0111}_{W_0}\ \underbrace{0011\ 1011}_{W_1}$

Now; $W_2 = W_0 \oplus 1000\ 0000 \oplus \text{SubNib}(\text{RotNib}(W_1))$

(i) $\text{RotNib}(W_1)$

1011 0011

(ii) SubNib(1011 001)

0011 1011

(iii)

$$\begin{array}{r} 1000\ 0000 \\ 0011\ 1011 \\ \hline 1011\ 1011 \end{array}$$

(iv) $W_0 \oplus 1011\ 1011$

$$\begin{array}{r} 1011\ 1011 \\ 1010\ 0111 \\ \hline 0001\ 1100 \end{array}$$

Now;

$W_3 = W_2 \oplus W_1$

$$\begin{array}{r} = 0001\ 1100 \\ 0011\ 1011 \\ \hline \boxed{0010\ 0111} \end{array} \longrightarrow W_3$$

And;

$W_4 = W_2 \oplus 0011\ 0000 \oplus \text{SubNib}(\text{RotNib}(W_3))$

(i) $\text{RotNib}(W_3) = 0111\ 0010$

(ii) SubNib(0111 0010) ~~0010 0111~~

0101 1010

(iii) 0011 0000
0101 1010

0110 1010

(iv) $w_2 \oplus$ 0110 1010

0110 1010
0001 1100

0111 0110 → $w_4$

And finally;

$w_5 = w_4 \oplus w_3$
= 0111 0110
0010 0111

0101 0001

Here our keys are;
$Key_0 = w_0w_1$ = 1010 0111 0011 1011
$Key_1 = w_2w_3$ = 0001 1100 0010 0111
$Key_2 = w_4w_5$ = 0111 0110 0101 0001

## ② ENCRYPTION

PT = 1101 0111 0010 1000

(i) PT $\oplus$ $Key_0$

0110 1111 0110 1011
1010 0111 0011 1011

1100 1000 0101 0000

(ii) S-box, just look up values in table

1100 0110 0001 1001

(iii) Shift Row's (2nd & 4th Nibble)

1100 1001 0001 0110

(iv) Mix columns:

Use the constant matrix $M_e$, with $GF(2^4)$;

$$\begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} S_{00} & S_{01} \\ S_{10} & S_{11} \end{bmatrix}$$

$$\begin{bmatrix} 1 \times 1100 \oplus 4 \times 1001 & 1 \times 0001 \oplus 0110 \times 4 \\ 4 \times 1100 \oplus 1 \times 1001 & 4 \times 0001 \oplus 0110 \times 1 \end{bmatrix}$$

$$\begin{bmatrix} 1100 \oplus 4 \times 9 & 1 \oplus 6 \times 4 \\ 4 \times 12 \oplus 1001 & 4 \times 1 \oplus 6 \times 1 \end{bmatrix}$$

$$\begin{bmatrix} 1100 \oplus 0010 & 0001 \oplus 1011 \\ 0101 \oplus 1001 & 0100 \oplus 0110 \end{bmatrix}$$

$$\begin{bmatrix} 1110 & 1010 \\ 1100 & 0010 \end{bmatrix}$$

or 1110 1100 1010 0010

(v) XOR with Key1

```
1110 1100 1010 0010
0001 1100 0010 0111
-------------------
1111 0000 1000 0101
```

Now we proceed with the final round of encryption.

(i) S-box substitution

0111 1001 0110 0001

(ii) Shift Row's (2nd & 4th Nibble)

0111 0001 0110 1001

(iii) XOR with Key2

```
0111 0001 0110 1001
0111 0110 0101 0001
-------------------
0000 0111 0011 1000
```

→ which is our ciphertext!

# ③ Decryption

Lets test our answer by decrypting the ciphertext we just made.

(i) XOR with Key 2

0000 0111 0011 1000
0111 0110 0101 0001

---

0111 0001 0110 1001

(ii) Inverse Swap Rows;

0111 1001 0110 0001

(iii) Inverse S-box Substitution

1111 0000 1000 0101

(iv) XOR with Key 1

1111 0000 1000 0101
0001 1100 0010 0111

---

1110 1100 1010 0010

(v) Inverse Mix Columns

$$\begin{bmatrix} 9 & 2 \\ 2 & 9 \end{bmatrix} \begin{bmatrix} 1110 & 1010 \\ 1100 & 0010 \end{bmatrix}$$

$$\begin{bmatrix} 9 \times 1110 \oplus 2 \times 1100 & 9 \times 1010 \oplus 2 \times 0010 \\ 2 \times 1110 \oplus 9 \times 1100 & 2 \times 1010 \oplus 9 \times 0010 \end{bmatrix}$$

$$\begin{bmatrix} 7 \oplus 11 & 5 \oplus 4 \\ 15 \oplus 6 & 7 \oplus 1 \end{bmatrix} = \begin{bmatrix} 0111 \oplus 1011 & 0101 \oplus 0100 \\ 1111 \oplus 0110 & 0111 \oplus 0001 \end{bmatrix}$$

$$= \begin{bmatrix} 1100 & 0001 \\ 1001 & 0110 \end{bmatrix}$$

(vi) Inverse Swap ;

1100 0110 0001 1001

(vii) Inverse S-box Substitution;

1100 1000 0101 0000

(viii) XOR with key$_0$

1100 1000 0101 0000
1010 0111 0011 1011

0110 1111 0110 1011

→ which is our original Plaintext.

Hence we have encrypted and decrypted the word "ok" using S-AES.