Shoaib Akhtar

20P-0147

Assignment #08

S-AES

Submitted to: Sir Ameen.

BS-CS - 7B.

Simplified AES example.

Plaintext ⇒ 1101 0111 0010 1000

16 bit key ⇒ 0100 1010 1111 0101

(1) Key Generation

(Sol)

To input key, is splited into two words w0, w1

w0 ⇒ 0100 1010
w1 = 1111 0101

Now we have to find w8

w8 = w0 ⊕ RCON1 ⊕ SubNib(RotNib(w1))

Now RCON1 ⇒ 10000000

w8 ⇒ 01001010 ⊕ 10000000 ⊕ SubNib(0101 1111)

Now, SubNib(0101) ⇒ 0001
SubNib(1111) ⇒ 0111

w8 ⇒ 11001010 ⊕ 00010111

w8 ⇒ 1101 1101

$w_3 = w_0 \oplus w_1$

$w_3 = 1101\ 1101 \oplus 1111\ 0101$

$\boxed{w_3 = 0010\ 1000}$

$w_4 = w_0 \oplus RCON_3 \oplus SubNib(RotNib(w_3))$

$w_4 \Rightarrow 1101\ 1101 \oplus 0011\ 0000 \oplus SubNib(RotNib(0010\ 1000))$

$w_4 \Rightarrow 1110\ 1101 \oplus SubNib(1000\ 0010)$

$SubNib(1000) \Rightarrow 0110$

$SubNib(0010) \Rightarrow 1010$

$w_4 = 1110\ 1101 + 0110\ 1010$

$\boxed{w_4 \Rightarrow 1000\ 0111}$

$w_5 \Rightarrow w_4 \oplus w_3$

$w_5 = 1000\ 0111 \oplus 0010\ 1000$

$\boxed{w_5 \Rightarrow 1010\ 1111}$

No 0, Key 0 => w0 w1

Key 0 = 0100 1010 1111 0101

Key 1 = w2 w3

Key 1 => 1101 1101 0010 1000

Key 2 => w4 w5

Key 2 = 1000 0111 1010 1111

S-AES Encryption!

① Add Round 0 key.

plaintext ⊕ key0

1101 0111 0010 1000 ⊕ 0100 1010 1111 0101

⇒ 1001 1101 1101 1101.

② Round 1 (Nibble Substitution)

S(1001) ⇒ 0010
S(1101) ⇒ 1110
S(1101) ⇒ 1110
S(1101) ⇒ 1110

⇒ 0010 1110 1110 1110

Apply Shift Row, i.e "Swap 2nd nibble" with "4th nibble".

⇒ 0010 1110 1110 1110.

Mix Columns!

$$Me = \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}, \quad S \Rightarrow \begin{bmatrix} 0010 & 1116 \\ 1110 & 1110 \end{bmatrix}$$

$$S = \begin{bmatrix} 0010 & 1116 \\ 1110 & 1110 \end{bmatrix} \Rightarrow \begin{matrix} S_{00} & S_{01} \\ S_{10} & S_{11} \end{matrix}$$

$S = Me \times S$

$S_{00} = 0010 \oplus 1110$

$S_{00} \Rightarrow 0010 \times 1 \oplus (1110 \times 4)$

$1110 \times 4 \Rightarrow (x^3 + x^2 + x) \times x^2$

$\Rightarrow x^5 + x^4 + x^3$

To be reduced modulo $(x^4 + x + 1)$

$$\begin{array}{r} x+1 \\ x^4+x+1 \overline{)\ x^5+x^4+x^3} \\ -(x^5+x^2+x) \\ \hline x^4+x^3+x^2+x \\ -(x^4+x^2+1) \\ \hline x^3+x^2+1 \end{array}$$

$x^3 + x^2 + 1 \Rightarrow 1101$

$S_{00} \Rightarrow 0010 \oplus 1101$

$S_{00} \Rightarrow 1111$

$S_{01} \Rightarrow (1 \times 1110) \oplus (4 \times 1110)$

$S_{01} = 1110 \oplus 0011$

$S_{01} = 0011$

$S_{10} \Rightarrow (4 \times 0010) \oplus (1 \times 1110)$

$S_{10} = 1000 \oplus 1110$

$S_{10} = 0110$

$S_{11} = (4 \times 1110) \oplus (1110 \times 1)$

$S_{11} = 1101 \oplus 1110$

$S_{11} = 0011$

Output $\Rightarrow$ S_{00} S_{10} S_{01} S_{11}

1111 0110 0011 0011

Now & XOR with key 1.

1111 0110 0011 0011 ⊕
1101 1101 0010 1000

0010 1011 0001 1011

Final Round Nibble Substitution.

S(0010) ⇒ 1010
S(1011) = 0011
S(0001) = 0100
S(1011) = 0011

~~Apply Shift Row (2nd and 4th)~~

~~1010 0100 0011 0011~~

1010 0011 0100 0011

Apply Shift key. (2nd and 4th)

1010 0100 0011 0011

Now, XOR with key 2.

Key 2 ⊕ 1010 0011 0100 0011

1000 0111 1010 1111 ⊕
1010 0011 0100 0011

0010 0100 1110 1100

cipher text ⇒ 0010 0100 1110 1100