Muhammad Rafay
20P-0018

Assignment No. 2
Information Security.

S-AES

Inputs for Encryption:

16-bit Plaintext P : 1101 0111 0010 1000

16-bit Key K : 0100 1010 1111 0101

Key Generation.

Split. w_0 = 0100 1010 , w_1 = 1111 0101

Key_0 = $w_0 w_1$ = K

Other Keys.

w_2 = w_0 XOR 10000000 SubNib(RotNib(w_1))

w_2 = 0100 1010 XOR ↑ SubNib(0101 1111)

XOR 10000000

∴ RotNib() Rotates the nibbles

∴ SubNib() 'S-Box substitution on nibbles using encryption S-Box'

= 1100 1010 XOR SubNib (0101 1111)

= 1100 1010 XOR 0001 0111

w_2 = 1101 1101

$w_3 = w_2$ XOR w_1

= 1101 1101 XOR 1111 0101

= 0010 1000

w_4 = 1000 0111

$w_5 = w_4$ XOR w_3

= 1000 0111 XOR 0010 1000

= 1010 1111

$w_4 = w_2$ XOR 0011 0000 XOR SubNib(RotNib(w_3))

$w_4 = w_2$ XOR 00110000 XOR SubNib (RotNib (00101000)))

w_4 = 1101 1101 XOR 0011 0000 XOR SubNib(1000 0010)

w_4 = 1110 1101 XOR 0110 1010

Sub-keys are:

Key$_0$ = $w_0 w_1$: 0100 1010 1111 0101

key$_1$ = $w_2 w_3$ = 1101 1101 0010 1000

key$_2$ = $w_4 w_5$ = 1000 0111 1010 1111

Encryption.

Add.
Round 0 Key:

Plain text XOR key$_0$.

= 1101 0111 0010 1000 XOR 0100 1010 1111 0101

= 1001 1101 1101 1101

Round 1.

Nibble Substitution. using (S-boxes)

Input = 1001 1101 1101 1101

Output = ~~1001~~ 0010 1110 1110 1110

Shift Row. "Swap 2nd & 4th nibble"

= 0010 1110 1110 1110

Mix Columns

"Matrix Multiplication with Constant Matrix, Me

using $GF(2^4)$

$$Me = \begin{matrix} 1 & 4 \\ 4 & 1 \end{matrix} \qquad S = \begin{matrix} 0010 & 1110 \\ 1110 & 1110 \end{matrix} = \begin{matrix} S_{00}' & S_{01}' \\ S_{10} & S_{11}' \end{matrix}$$

$S' = Me \times S$

S_{00}' = 0010 XOR (4 x 1110)

= 0010 XOR (4 x E)

= 0010 XOR D

= 0010 XOR 1101

= 1111

S_{10}' = (4 x 0010) XOR 1101

= 1000 XOR 1101

= ~~0011~~ 0110

S_{01}' = 1110 XOR (4x 1110)

= 1110 XOR 1101

= 0011

S_{11}' = (4x 1110) XOR 1110

= 1101 XOR 1110

= 0011

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

= 1111 0110 0011 0011

Add Round 1 Key.

= 1111 0110 00110011 XOR 1101 1101 0010 1000

= 0010 1011 0001 1011

FINAL Round.

Nibble Substitution.

= 1010 0011 0100 0011

Shift Row

= 1010 0011 0100 0011

Add Round 2 Key. = 1010 0011 0100 0011 XOR

1000 0111 1010 1111

= 0010 0100 1110 1100

Cipher Text. 0010 0100 1110 1100

Decryption.

Add Round 2 Key.

= 0010 0100 1110 1100 XOR 1000 0111 1010 1111

= 1010 0011 0100 0011

Inverse Shift Row

= 1010 0011 0100 0011

Inverse Nibble Sub. (Use decryption S-box)

= 0010 1011 0001 1011

Add Round 1 Key.

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

$$= \begin{matrix} 1111 & 0011 \\ 0110 & 0011 \end{matrix}$$

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

$$= \begin{matrix} 9 \times S_{00} \text{ XOR } 2 \times S_{10} & 9 \times S_{01} \text{ Xor } 2 \times S_{11} \\ 2 \times S_{00} \text{ XOR } 9 \times S_{10} & 2 \times S_{01} \text{ XOR } 9 \times S_{11} \end{matrix}$$

S_{00}' = (9 x 1111) XOR (2 x 0110)

= 9 x F XOR 2 x 6

= 1110 XOR 1100 = 0010

S'_{10} = 2 x 1111 XOR 9x 0110

= 2 x F XOR 9 x 6

= D XOR 3

= 1101 XOR 0011

= 1110

S'_{01} = 9 x 0011 XOR 2 x 0011

= 9x3 XOR 2 x 3

= 1000 XOR 0110

= 1110

S'_{11} = 2 x 0011 XOR 9 x 0011

= 1110

Output = 0010 1110 1110 1110

Inverse Shif Row = 0010 1110 1110 1110

Add Round 0 Key.

= 1001 1101 1101 1101 XOR 0100 1010 111 0101

= 1101 0111 0010 1000

Plain Text = 1101 0111 0010 1000

Original = 1101 0111 0010 1000

Decryption Worked.