Name: Muhammad Sherjeel Akhtar

Roll No: 20p-0101

Subject: Information Security.

Section: BCS-7B

Assignment No: 02

Submmited To Respected Sir: Dr. Muhammad Amin

→ SIMPLIFIED - AES ENCRYPTION ←

- 16-bit plaintext 1010 1101 0011 1110

16-bit key k: 0110 1001 1010 0011

→ Splitting 16-bit key into two words w0 and w1

$w_0 = 0110\,1001$

$w_1 = 1010\,0011$

The first subkey $k_0 = w_0 w_1 = k$

Now to generate the other subkeys

$w_2 = w_0 \oplus 10000000 \oplus SubNib(RotNib(w_1))$

$RotNib(w_1) = 0011\,1010$

Now by using S-Box table $SubNib(Rot(w_1))$

	00	01	10	11
00	9	4	A	B
01	D	1	8	5
10	6	2	0	3
11	C	E	F	7

$0110\,1001 \oplus 10000000 \oplus 0110\,0010$

$1110\,1001 \oplus 0110\,0010$

$w_2 = 1000\,1011$

$w_3 = w_2 \oplus w_1$

$= 1000\,1011 \oplus 1010\,0011$

$w_3 = 0010\,1000$

$w_4 = w_2 \oplus 0011\,0000 \oplus SubNib(RotNib(w_3))$

$= 1000\,1011 \oplus 0011\,0000 \oplus SubNib(RotNib(0010\,1000))$

$RotNib(0010\,1000) = 1000\,0010$

$SubNib(1000\,0010)$

$= 0110\,1010$

$w_4 = 1000\,1011 \oplus 0011\,0000 \oplus 0110\,1010$

$w_4 = 1011\,1011 \oplus 0110\,1010$

$w_4 = 1101\,0001$

$w_5 = w_4 \oplus w_3 = 1101\,0001 \oplus 0010\,1000 = 1111\,1001$

Now Subkey are: $key\,0 = w_0 w_1 = 0110\,1001\,1010\,0011$

$key\,1 = w_2 w_3 = 1000\,1011\,0010\,1000$

$key\,2 = w_4 w_5 = 1101\,0001\,1111\,1001$

→ Add Round key :
Plain text : 1010 1101 0011 1110 ⊕ key 0
key 0 = 0 1110 0011 1010 0011
= 1100 0100 1001 1101
Nibble Substitution (S-Box)
Input = 1100 0100 1001 1101
Output = 1110 1110 1001 0010
Shift Row
Swap 2 and 4
1110 0010 1001 1110
Mix Columns → Apply Matrix Multiplication.
Mix Cols.

$$= \begin{pmatrix} 1110 & 1001 \\ 0010 & 1110 \end{pmatrix} \times \begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix} = \begin{pmatrix} E & 9 \\ 2 & E \end{pmatrix} \times \begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} E\times1 \oplus 9\times4 & 2\times1 \oplus E\times4 \\ E\times4 \oplus 9\times1 & 2\times4 \oplus E\times1 \end{pmatrix} = \begin{pmatrix} E \oplus 2 & 2 \oplus D \\ D \oplus 4 & 8 \oplus E \end{pmatrix}$$

$$= \begin{pmatrix} 1110 \oplus 0010 & 0010 \oplus 1101 \\ 1101 \oplus 1001 & 1000 \oplus 1110 \end{pmatrix} = \begin{pmatrix} 1100 & 1111 \\ 0100 & 0110 \end{pmatrix}$$

= 1100 0100 1111 0110 → Now Add Round 1 key.
= 1100 0100 1111 0110 ⊕ 1000 1011 0010 1000 = 0100 1111 1101 1110
→ Now Nibble Substitution,
0100 1111 1101 1110
NibSub = 1101 0111 1110 1111 → Shift Row swap 2 and 4 Nibble
= 1101 1111 1110 0111 → Now Add Round 2 key.
= 1101 1111 1110 0111 ⊕ 1101 0001 1111 1001
= Cipher text = 0000 1110 0001 1110

⇒ DECRYPTION ⇐

• Add Round key-2
0000 1110 0001 1110 ⊕ 1100 0001 1111 1001 = 1100 1111 1110 0111
→ INVERSE SHIFT ROW : 1100 0111 1110 1111
→ INVERSE Nib Sub : 1100 1111 0100 1110
Now Add Round 1 key : 1100 1111 0100 1110 ⊕ 1000 1011 0010 1000
= 1100 0100 1111 0110.

⇒ INVERSE MIX COLUMNS ⇐

$$S = \begin{pmatrix} 1100 & 1111 \\ 0100 & 0110 \end{pmatrix}$$

$$= \begin{pmatrix} 9\times1100 \oplus 2\times0100 & 9\times1111 \oplus 2\times0110 \\ 2\times1100 \oplus 9\times0100 & 2\times1111 \oplus 9\times0110 \end{pmatrix}$$

$S_{00} = (9 \times 1100 \oplus 2 \times 0100)$

$= (9 \times C \oplus 2 \times 4) = (6 \oplus 8) = (0110 \oplus 1000) = 1110$ (3)

$S_{10} = (92 \times C \oplus 9 \times 0100) = (2 \times C \oplus 9 \times 4) = B \oplus 2 = 1011 \oplus 0010$

$= \boxed{1001}$

$S_{01} = 9 \times 1111 \oplus 2 \times 0110$

$= 9 \times F \oplus 2 \times 6$

$= E \oplus C$

$= 1110 \oplus 1100$

$= \boxed{0010}$

$S_{11} = 2 \times 1111 \oplus 9 \times 0110$

$S_{11} = 2 \times F \oplus 9 \times 6$

$= D \oplus 3$

$= 1101 \oplus 0011$

$= \boxed{1110}$

Output = 1110 1001 0010 1110

Inverse Shift Row

$\Rightarrow$ 1110 1110 0010 1001

Now Inverse Nibble Sub

$= 0100\ 0100\ 1001\ 0000$

Now Add Round 0 key

$$\begin{array}{r} 0100\ 0100\ 1001\ 0000 \\ \oplus \\ 0110\ 1001\ 1010\ 0011 \end{array}$$

$$= 0.0110\ 1001\ 1110$$