SIMPLIFIED AES (ADVANCED ENCRYPTION STANDARD)

Encryption

Given Plain Text: 0001 0010 0011 0100

Given Key: 0101 0110 0111 1000

Given Matrix: $\begin{matrix} 1 & 4 \\ 4 & 1 \end{matrix}$

Key Generation Phase

$K_0 = w_0w_1$

$K_1 = w_2w_3$

$K_2 = w_4w_5$

$w_0 =$ 0101 0110

$w_1 =$ 0111 1000

$w_2 = w_0 \oplus 1000\ 0000 \oplus \text{SubstituteNibble}(\text{RotateNibble}(w_1))$

RotateNibble(w_1) = 1000 0111

SubstituteNibble(RotateNibble(w_1)) = 0110 0101

$= 0101 \quad 0110$

$\oplus\, 1000\ 0000$

$\oplus\, 0110 \quad 0101$

$= 1011 \quad 0011$

$w_3 \quad = w_2 \oplus w_1$

$= 1011 \quad 0011$

$\oplus\, 0111 \quad 1000$

$= 1100 \quad 1011$

$w_4 \quad = w_2 \oplus 0011\ 0000 \oplus \text{SubstituteNibble}(\text{RotateNibble}(w_3))$

$\text{RotateNibble}(w_3) = 1011 \quad 1100$

$\text{SubstituteNibble}(\text{RotateNibble}(w_3)) = 0011 \quad 1100$

$= 1011 \quad 0011$

$\oplus\, 0011\ 0000$

$\oplus\, 0011 \quad 1100$

$= 1011 \quad 1111$

$w_5 \quad = w_4 \oplus w_3$

$= 1011 \quad 1111$

$\oplus\, 1100 \quad 1011$

$= 0111 \quad 0100$

K_0 =	0101	0110	0111	1000
K_1 =	1011	0011	1100	1011
K_2 =	1011	1111	0111	0100

Add Round Key:

IT_1 = PlainText ⊕ K_0

= 0001 0010 0011 0100

⊕ 0101 0110 0111 1000

= 0100 0100 0100 1100

$$IT_1 = \begin{array}{|c|c|}\hline 4 & 4 \\ \hline 4 & C \\ \hline\end{array}$$

Round 1:

Substitute Nibbles of IT_1:

SubstituteNibble(0100) = 1101

SubstituteNibble(0100) = 1101

SubstituteNibble(0100) = 1101

SubstituteNibble(1100) = 1100

IT_2 = 1101 1101 1101 1100

$$IT_2 \quad = \quad \begin{array}{|c|c|}\hline D & D \\ \hline D & C \\ \hline\end{array}$$

Shift Rows of IT$_2$:

IT_3 = 1101 1100 1101 1101

$$IT_3 \quad = \quad \begin{array}{|c|c|}\hline D & D \\ \hline C & D \\ \hline\end{array}$$

Mix Columns of IT$_3$:

$$S' \quad = \quad M_e \times IT_3 = \begin{matrix} S'_{00} & S'_{01} \\ S'_{10} & S'_{11} \end{matrix}$$

$$= \begin{array}{|c|c|}\hline 1 & 4 \\ \hline 4 & 1 \\ \hline\end{array} \quad x \quad \begin{array}{|c|c|}\hline D & D \\ \hline C & D \\ \hline\end{array}$$

S'_{00} = (1 x D) $\oplus$ (4 x C)

= 1101

$\oplus$ 0101

= 1000

S'_{01} = (1 x D) $\oplus$ (4 x D)

= 1101

$\oplus$ 0001

= 1100

$S'_{10} = (4\ x\ D) \oplus (1\ x\ C)$

$= 0001$

$\oplus\ 1100$

$= 1101$

$S'_{11} = (4\ x\ D) \oplus (1\ x\ D)$

$= 0001$

$\oplus\ 1101$

$= 1100$

$$S' = \begin{matrix} S'_{00} & S'_{01} \\ S'_{10} & S'_{11} \end{matrix} = \begin{array}{|c|c|}\hline 8 & C \\ \hline D & C \\ \hline \end{array} = IT_4$$

$IT_4 = S'_{00}\ S'_{10}\ S'_{01}\ S'_{11}$

$= 1000 \quad 1101 \quad 1100 \quad 1100$

Add Round Key to IT_4:

$IT_5 = IT_4 \oplus K_1$

$= 1000 \quad 1101 \quad 1100 \quad 1100$

$\oplus\ 1011 \quad 0011 \quad 1100 \quad 1011$

$= 0011 \quad 1110 \quad 0000 \quad 0111$

$$IT_5 = \begin{array}{|c|c|}\hline 3 & 0 \\ \hline E & 7 \\ \hline \end{array}$$

Round 2:

Substitute Nibbles of IT_5:

SubstituteNibble(0011) = 1011

SubstituteNibble(1110) = 1111

SubstituteNibble(0000) = 1001

SubstituteNibble(0111) = 0101

IT_6 = 1011 1111 1001 0101

IT_6 =

B	9
F	5

Shift Rows of IT_6:

IT_7 = 1011 0101 1001 1111

IT_7 =

B	9
5	F

Add Round Key to IT_7:

$IT_8 = IT_7 \oplus K_2$

= 1011 0101 1001 1111

$\oplus$ 1011 1111 0111 0100

= 0000 1010 1110 1011

IT_8 =

0	E
A	B

Final Cipher Text = IT_8

= 0 A E B