SIMPLIFIED AES (ADVANCED ENCRYPTION STANDARD)

Encryption

Given Plain Text:

Given Key:

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

KEY GENERATION PHASE

K_0 = $w_0 w_1$

K_1 = $w_2 w_3$

K_2 = $w_4 w_5$

w_0 =

w_1 =

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

RotateNibble(w_1) =

SubstituteNibble(RotateNibble(w_1)) =

=

$\oplus$ 1000 0000

$\oplus$

=

w_3 = $w_2 \oplus w_1$

=

$\oplus$

=

w_4 = $w_2 \oplus$ 0011 0000 $\oplus$ SubstituteNibble(RotateNibble(w_3))

RotateNibble(w_3) =

SubstituteNibble(RotateNibble(w_3)) =

=

$\oplus$ 0011 0000

$\oplus$

=

w_5 = $w_4 \oplus w_3$

=

$\oplus$

=

K_0 =
K_1 =
K_2 =

ADD ROUND KEY:

IT_1 = PlainText $\oplus$ K_0

=

$\oplus$

=

IT_1 =

ROUND 1:

Substitute Nibbles of IT_1:

SubstituteNibble( ) =

SubstituteNibble( ) =

SubstituteNibble( ) =

SubstituteNibble( ) =

IT_2 =

IT_2 =

Shift Rows of IT_2:

IT_3 =

IT_3 =

Mix Columns of IT_3:

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

=

1	4
4	1

x

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

=

$\oplus$

=

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

=

$\oplus$

=

S'_{10} = (4 x) ⊕ (1 x)

=

⊕

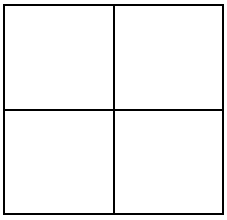
=

S'_{11} = (4 x) ⊕ (1 x)

=

⊕

=

S' = $\begin{matrix} S'_{00} & S'_{01} \\ S'_{10} & S'_{11} \end{matrix}$ =  = IT_4

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

=

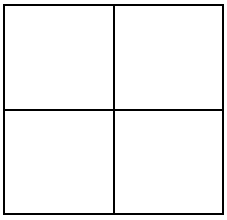
Add Round Key to IT_4:

IT_5 = $IT_4 \oplus K_1$

=

⊕

=

IT_5 = 

ROUND 2:

Substitute Nibbles of IT_5:

SubstituteNibble( ) =

SubstituteNibble( ) =

SubstituteNibble( ) =

SubstituteNibble( ) =

IT_6 =

IT_6 =

Shift Rows of IT_6:

IT_7 =

IT_7 =

Add Round Key to IT_7:

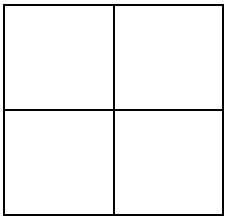
IT_8 = $IT_7 \oplus K_2$

=

$\oplus$

=

IT_8 =



Final Cipher Text = IT_8

=