Activity # 5

Cipher text

$$\begin{pmatrix} 29 & 57 & 40 & 1A \\ C3 & 14 & 22 & 02 \\ 50 & 20 & 99 & D7 \\ 5F & F6 & B3 & 3A \end{pmatrix}$$

key 10:

$$\begin{pmatrix} 28 & 6D & CC & 3B \\ F0 & A4 & CD & 31 \\ DE & 24 & A4 & 6F \\ F8 & 4A & FF & 26 \end{pmatrix}$$

Ciphertext ⊕ key 10

We get this

$$= \begin{pmatrix} 01 & 3A & 8C & 21 \\ 3E & B0 & E2 & 33 \\ 8E & 04 & 3D & B8 \\ A7 & BC & 4D & 1C \end{pmatrix}$$

Round 9

Inverse shift Rows

$$\begin{pmatrix} 01 & 3A & 8C & 21 \\ 3E & B0 & E2 & 33 \\ 8E & 04 & 3D & B8 \\ AF & BC & 4D & 1C \end{pmatrix} \Rightarrow \begin{pmatrix} 01 & 3A & 8C & 21 \\ 33 & 3E & B0 & E2 \\ 3D & B8 & 8E & 04 \\ BC & 4D & 1C & AF \end{pmatrix}$$

Inverse Sub bytes

$$\begin{pmatrix} 01 & 3A & 8C & 21 \\ 33 & 3E & B0 & E2 \\ 3D & B8 & 8E & 04 \\ BC & 4D & 1C & AF \end{pmatrix} \Rightarrow \begin{pmatrix} 09 & A2 & F0 & 7B \\ 66 & D1 & FC & 3B \\ 8B & 9A & E6 & 30 \\ 78 & 65 & C4 & 89 \end{pmatrix}$$

Adding Round key i.e key 9

$$\begin{pmatrix} 09 & A2 & F0 & 7B \\ 6b & D1 & fC & 3B \\ 8B & 9A & E6 & 30 \\ 78 & 65 & C4 & 89 \end{pmatrix} \oplus \begin{pmatrix} Bf & 45 & A1 & 57 \\ E2 & 59 & 64 & F1 \\ Bf & FA & 80 & CB \\ 90 & B2 & B4 & D8 \end{pmatrix}$$

$$2 \begin{pmatrix} B6 & E7 & 51 & 8C \\ 84 & 88 & 98 & CA \\ 34 & 60 & 66 & FB \\ E8 & D7 & 70 & 51 \end{pmatrix}$$

Inverse mix column

$$\begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix} \begin{pmatrix} B6 & E7 & 51 & 8C \\ 84 & 88 & 98 & CA \\ 34 & 60 & 66 & fB \\ E6 & D7 & 70 & 51 \end{pmatrix}$$

Result on next page

$$\begin{pmatrix} BF & 5C & AF & 10 \\ B7 & 20 & 49 & D7 \\ 72 & AD & 28 & 89 \\ 2C & 2D & 27 & 9F \end{pmatrix}$$

Round 8:

Inverse shift Rows

$$\begin{pmatrix} BF & 5C & AF & 10 \\ BF & 20 & 49 & D7 \\ 72 & AD & 28 & 89 \\ 2C & 2D & 27 & 9F \end{pmatrix} \Rightarrow \begin{pmatrix} BF & 5C & AF & 10 \\ D7 & BF & 20 & 49 \\ 28 & 89 & 72 & AD \\ 9F & 2C & 2D & 27 \end{pmatrix}$$

Inverse Sub bytes

$$\begin{pmatrix} BF & 5C & Af & 10 \\ D7 & Bf & 20 & 49 \\ 28 & 89 & 72 & AD \\ 9f & 2C & 2D & 27 \end{pmatrix} \Rightarrow \begin{pmatrix} F4 & A7 & 1B & 7C \\ 0D & f4 & 54 & A4 \\ EE & f2 & 1E & 18 \\ 6E & 42 & FA & 3D \end{pmatrix}$$

Adding Round key i.e key8

$$\begin{pmatrix} F4 & A7 & 1B & 7C \\ 0D & F4 & 54 & A4 \\ EE & F2 & 1E & 18 \\ 6E & 42 & FA & 3D \end{pmatrix} \oplus \begin{pmatrix} 8E & FA & E4 & 56 \\ 51 & BB & 3D & 95 \\ EF & 45 & 7A & 4B \\ 21 & 22 & 06 & 6C \end{pmatrix}$$

$$\begin{pmatrix} 7A & 5D & ff & 2A \\ 5C & 4f & 69 & 31 \\ \cancel{1B} & \cancel{76} & \cancel{65} & \doteq \\ 01 & B7 & 64 & 53 \\ 4f & 60 & fC & 51 \end{pmatrix}$$

Inverse mix column:

$$\begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix} \begin{pmatrix} 7A & 5D & ff & 2A \\ 5C & 4f & 69 & 31 \\ 01 & B7 & 64 & 53 \\ 4f & 60 & fC & 51 \end{pmatrix}$$

result is on next page

$$\begin{pmatrix} 53 & 43 & 4F & 85 \\ 39 & 06 & 0A & 52 \\ 8E & 93 & 3B & 57 \\ 5D & F8 & 95 & BD \end{pmatrix}$$

Round 7:

After Inverse shift Rows

$$\begin{pmatrix} 53 & 43 & 4f. & 85 \\ 52 & 39 & 06 & 0A \\ 3B & 57 & 8E & 93 \\ BD & 5D & F8 & 95 \end{pmatrix}$$

After Inverse Sub bytes

$$\begin{pmatrix} 50 & 64 & 92 & 67 \\ 48 & 5b & A5 & A3 \\ 49 & DA & E6 & 22 \\ CD & 8D & E1 & 67 \end{pmatrix}$$

Adding Round key ie key 7

$$\begin{pmatrix} 50 & 64 & 92 & 67 \\ 48 & 5B & A5 & A3 \\ 49 & DA & E6 & 22 \\ CD & 8D & E1 & 67 \end{pmatrix} \oplus \begin{pmatrix} CC & 74 & 1E & B2 \\ 96 & EA & 83 & A8 \\ ED & AA & 3F & 31 \\ 16 & 03 & 24 & 6A \end{pmatrix}$$

$$= \begin{pmatrix} BD & ED & 16 & 02 \\ 12 & C9 & B4 & 7A \\ C7 & 1A & 76 & 88 \\ 91 & F1 & E2 & 56 \end{pmatrix}$$

After ~~[illegible]~~ Inverse Mix column

$$\begin{pmatrix} 14 & 8F & C0 & 5E \\ 93 & A4 & 60 & 0f \\ 25 & 2B & 24 & 92 \\ 77 & E8 & 40 & 75 \end{pmatrix}$$

Round 6: Round 6

After Applying this
We get

$$\begin{matrix} 9B & 23 & 5D & 2F \\ 51 & 5F & 1C & 38 \\ 20 & 22 & BD & 91 \\ 68 & F0 & 32 & 56 \end{matrix}$$

Round 5:

After Round 5 we get this

$$\begin{pmatrix} B1 & 08 & 04 & E7 \\ CA & FC & B1 & B2 \\ 51 & 54 & C9 & 6C \\ ED & E1 & D3 & 20 \end{pmatrix}$$

Round 4:

After Round 4 we get this

$$\begin{matrix} 78 & 70 & 99 & 4B \\ 76 & 76 & 3C & 39 \\ 30 & 70 & 37 & 34 \\ 54 & 23 & 5B & F1 \end{matrix}$$

Round 3.

After Round 3 we get this output.

$$\begin{pmatrix} 43 & 0E & 09 & 3D \\ C6 & 57 & 08 & F8 \\ A9 & C0 & EB & 7F \\ 62 & C8 & FE & 37 \end{pmatrix}$$

Round 2 :

After round 2 we get this

$$\begin{matrix} 58 & 15 & 59 & CD \\ 47 & B6 & D4 & 39 \\ 08 & 1C & E2 & DF \\ 8B & BA & E8 & CE \end{matrix}$$

Round 1

After Round 1 we get this

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ C0 & 2f & 93 & 92 \\ AB & 30 & Af & C7 \\ 20 & CB & 2B & A2 \end{pmatrix}$$

Round 0 :

After inverse shift Rows

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ 92 & C0 & 2F & 93 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{pmatrix}$$

After Sub bytes.

$$\begin{pmatrix} 00 & 3C & 6E & 47 \\ 1F & 4E & 22 & 74 \\ 0E & 08 & 1B & 31 \\ 54 & 59 & 0B & 1A \end{pmatrix}$$

After Adding key i.e Round0.

We get this

$$\begin{pmatrix} 54 & 4F & 4E & 20 \\ 77 & 6E & 69 & 54 \\ 6F & 65 & 6E & 77 \\ 20 & 20 & 65 & 6F \end{pmatrix}$$

This is the final Result.