Information Security
Assignment #1

2021-CS-695

plain text: ISLAMABAD IS THE CAPITAL OF PAKISTAN.

Key: MY NAME IS NIMRA JAB

Step 1: Making 4x4 Matrix (16 bytes)

I	M	D	H
S	A	I	E
L	B	S	C
A	A	T	A

Step 2: Convert it into hexa.

49	4D	44	48
53	41	49	45
4C	42	53	43
41	41	54	41

Step 3: Making I.V of 4x4 Matrix

00	06	06	01
02	00	08	03
04	09	02	05
01	03	04	00

Step 4: Taking X-OR b/w plain text and IV.

$$\begin{bmatrix} 49 & 4D & 44 & 48 \\ 53 & 41 & 49 & 45 \\ 4C & 42 & 53 & 43 \\ 41 & 41 & 54 & 41 \end{bmatrix} \oplus$$

$$\begin{bmatrix} 00 & 06 & 06 & 01 \\ 02 & 00 & 08 & 03 \\ 04 & 09 & 02 & 05 \\ 01 & 03 & 04 & 00 \end{bmatrix}$$

$$= \begin{bmatrix} 49 & 4B & 42 & 49 \\ 51 & 41 & 41 & 46 \\ 48 & 4B & 51 & 46 \\ 40 & 42 & 50 & 41 \end{bmatrix}$$

Step 5: Apply AES

- **key:** Convert key into hexa.

$$\begin{bmatrix} M & M & N & A \\ Y & E & I & J \\ N & I & M & A \\ A & S & R & B \end{bmatrix}$$

$$\begin{bmatrix} 4D & 4D & 4E & 41 \\ 59 & 45 & 49 & 4A \\ 4E & 49 & 4D & 41 \\ 41 & 53 & 52 & 42 \end{bmatrix}$$

- W[0] = (4D, 59, 4E, 41)

  W[1] = (4D, 45, 49, 53)

  W[2] = (4E, 49, 4D, 52)

  W[3] = (41, 4A, 41, 42)

- Pass W[3] from (g)function

(g) function:

→ circular byte left shif of W[3]:
(4A, 41, 42, 41)

→ Byte substitution (S-box): (D6, 83, 2C, 83)

→ Adding round constant : (01, 00, 00, 00)
: (01, 00, 00, 00) ⊕ (D6, 83, 2C, 83)
(D7, 83, 2C, 83)

4D	4D	4F	41
59	45	49	4A
4E	49	4D	41
41	53	52	42

- W[0] = (4D, 59, 4E, 41)

  W[1] = (4D, 45, 49, 53)

  W[2] = (4E, 49, 4D, 52)

  W[3] = (41, 4A, 41, 42)

- Pass W[3] from (g) function

(g) function:

→ circular byte left shif of W[3]:
(4A, 41, 42, 41)

→ Byte substitution (S-box): (D6, 83, 2C, 83)

→ Adding round constant : (01, 00, 00, 00)
: (01, 00, 00, 00) ⊕ (D6, 83, 2C, 83)
(D7, 83, 2C, 83)

W[4]: W[0] ⊕ g(W[3])

= (4D, 59, 4E, 41) ⊕ (D7, B3, 2C, 83)
= (9A, DA, 62, C2)

W[5]: W[4] ⊕ W[1]

= (9A, DA, 62, C2) ⊕ (4D, 45, 49, 53)
= (D7, 9F, 2B, 91)

W[6]: W[5] ⊕ W[2]

= (D7, 9F, 2B, 91) ⊕ (4E, 49, 4D, 52)
= (99, E6, 66, C3)

W[7]: W[6] ⊕ W[3]

= (99, E6, 66, C3) ⊕ (41, 4A, 41, 42)
= (D8, AC, 27, 81)

• pass W[7] from g function.

→ circular byte left shift of W[7]:
= (AC, 27, 81, D8)

→ Byte substitution: (S-box):
= (61, 91, CC, 0C)

⇒ Adding round constant: (02, 00, 00, 00)

(02, 00, 00, 00) ⊕ (61, 91, CC, 0C)
= (63, 91, CC, 0C)

W[8]: W[4] ⊕ g(W[7])

(9A, DA, 62, C2) ⊕ (63, 91, CC, 0C)
= (F9, 4B, AE, CE)

W[9]: W[8] ⊕ W[5]

= (F9, 4B, AE, CE) ⊕ (D7, 9F, 2B, 91)
= (2E, D4, 85, 5F)

W[10]: W[9] ⊕ W[6]

= (2E, D4, 85, 5F) ⊕ (99, E6, 66, C3)
= (B7, 32, E3, 9C)

W[11] W[10] ⊕ W[7]
= (B7, 32, E3, 9C) ⊕ (08, AC, 27, 81)
= (6F, 9E, C4, 1D)

Keys:

Round 0:
$$\begin{bmatrix} 4D & 4D & 4E & 41 \\ 59 & 45 & 49 & 4A \\ 4E & 49 & 4D & 41 \\ 41 & 53 & 52 & 42 \end{bmatrix}$$

Round 1:
$$\begin{bmatrix} 9A & D7 & 99 & D8 \\ DA & 9F & E6 & AC \\ 62 & 2B & 66 & 27 \\ C2 & 91 & C3 & 81 \end{bmatrix}$$

Round 2:
$$\begin{bmatrix} F9 & 2E & B7 & 6F \\ 4B & D4 & 32 & 9E \\ AE & 85 & E3 & C4 \\ CE & 5F & 9C & 1D \end{bmatrix}$$

Initial Round:-

taking X-OR b/w Plaintext and Round "0" key.

$$\begin{bmatrix} 49 & 4B & 42 & 49 \\ 51 & 41 & 41 & 46 \\ 48 & 4B & 51 & 46 \\ 40 & 42 & 50 & 47 \end{bmatrix} \oplus \begin{bmatrix} 4D & 4D & 4E & 41 \\ 59 & 45 & 49 & 4A \\ 4E & 49 & 4D & 41 \\ 41 & 53 & 52 & 42 \end{bmatrix}$$

$$\begin{bmatrix} 04 & 05 & 0C & 08 \\ 08 & 04 & 04 & 0C \\ 06 & 02 & 18 & 07 \\ 01 & 11 & 03 & 03 \end{bmatrix}$$

Rama # 1:-

- **Substitute Bytes:-** (S-box)

$$\begin{bmatrix} F2 & 6B & FE & 30 \\ 30 & F2 & F2 & FE \\ 6E & 77 & AD & C5 \\ 7C & 82 & 7B & 7B \end{bmatrix}$$

- **Shift Rows:-**

$$\begin{bmatrix} F2 & 6B & FE & 30 \\ F2 & F2 & FE & 30 \\ AD & C5 & 6F & 77 \\ 7B & 7C & 82 & 7B \end{bmatrix}$$

- **Mix Column:-**

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} F2 & 6B & FE & 30 \\ F2 & F2 & FE & 30 \\ AD & C5 & 6F & 77 \\ 7B & 7C & 82 & 7B \end{bmatrix}$$

$$\begin{bmatrix} D4 & 62 & 13 & 3C \\ 3A & BC & 2A & B2 \\ 9C & 8C & 43 & 63 \\ F4 & 72 & 97 & E1 \end{bmatrix}$$

Add Round key:

$$\begin{bmatrix} D4 & 62 & 13 & 3C \\ 3A & BC & 2A & B2 \\ 9C & 8C & 43 & 63 \\ F4 & 72 & 97 & E1 \end{bmatrix} \oplus \begin{bmatrix} 9A & D7 & 99 & D8 \\ DA & 9F & E6 & AC \\ 62 & 2B & 66 & 27 \\ C2 & 91 & C3 & 81 \end{bmatrix}$$

$$\begin{bmatrix} 4E & B5 & 8A & E4 \\ 0E & 23 & AA & 1E \\ FE & A7 & 25 & 44 \\ 36 & E3 & 54 & 60 \end{bmatrix}$$

Final Round:-

- **Substitute Bytes:** (S-box)

$$\begin{bmatrix} 2F & D5 & 7E & 69 \\ AB & 26 & AC & 72 \\ BB & 5C & 3F & 1B \\ 05 & 11 & 20 & D0 \end{bmatrix}$$

Shift Rows:

$$\begin{bmatrix} 2F & D5 & 7E & 69 \\ 26 & AC & 72 & AB \\ 3F & 1B & BB & 5C \\ D0 & 05 & 11 & 20 \end{bmatrix}$$

Add Round key.

$$\begin{bmatrix} 2F & D5 & 7E & 69 \\ 26 & AC & 72 & AB \\ 3F & 1B & BB & 5C \\ D0 & 05 & 11 & 20 \end{bmatrix} \oplus \begin{bmatrix} F9 & 2E & B7 & 6F \\ 4B & D4 & 32 & 9E \\ AE & 85 & E3 & C4 \\ CE & 5F & 9C & 1D \end{bmatrix}$$

$$\begin{bmatrix} D6 & FB & C9 & 06 \\ 6D & 78 & 40 & 35 \\ 91 & 9E & 58 & 98 \\ 1E & 51 & 8D & 3D \end{bmatrix}$$

Block 8:- $\begin{bmatrix} P & L & A & T \\ I & O & K & A \\ T & F & I & N \\ A & P & S & . \end{bmatrix}$

- Convert the block 8 text into hexadecimal.

$$\begin{bmatrix} 50 & 4C & 41 & 54 \\ 49 & 4F & 4B & 41 \\ 54 & 46 & 49 & 4E \\ 41 & 50 & 53 & 2E \end{bmatrix}$$

- $$\begin{bmatrix} 50 & 4C & 41 & 54 \\ 49 & 4F & 4B & 41 \\ 54 & 46 & 49 & 4E \\ 41 & 50 & 53 & 2E \end{bmatrix} \oplus \begin{bmatrix} D6 & FB & C9 & 06 \\ 6D & 78 & 40 & 35 \\ 91 & 9E & 58 & 98 \\ 1E & 51 & 8D & 3D \end{bmatrix}$$

$$\begin{bmatrix} 86 & B7 & 88 & 52 \\ 24 & 37 & 0B & 74 \\ C5 & D8 & 11 & D6 \\ 5F & 01 & DE & 13 \end{bmatrix}$$

Apply AES

Initial Round:

taking X-OR b/w plain text and Round "0" key.

$$\begin{bmatrix} 86 & B7 & 88 & 52 \\ 24 & 37 & 0B & 74 \\ C5 & D8 & 11 & D6 \\ 5F & 01 & DE & 13 \end{bmatrix} \oplus \begin{bmatrix} 4D & 4D & 4E & 41 \\ 59 & 45 & 49 & 4A \\ 4E & 49 & 4D & 41 \\ 41 & 53 & 62 & 42 \end{bmatrix}$$

$$= \begin{bmatrix} CB & FA & C6 & 13 \\ 7D & 72 & 42 & 3E \\ 8B & 91 & 5C & 97 \\ 1E & 52 & 8C & 51 \end{bmatrix}$$

Round # 1:

- **Substitute Byte:** (S-box)

$$\begin{bmatrix} 1F & 2D & B4 & 7D \\ FF & 40 & 2C & B2 \\ 3D & 81 & 4A & 88 \\ 72 & 00 & 64 & D1 \end{bmatrix}$$

- **Shift Rows:**

$$\begin{bmatrix} 1F & 2D & B4 & 7D \\ 40 & 2C & B2 & FF \\ 4A & 88 & 3D & 81 \\ D1 & 72 & 00 & 64 \end{bmatrix}$$

- **Mix Column:**

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} 1F & 2D & B4 & 7D \\ 40 & 2C & B2 & FF \\ 4A & 88 & 3D & 81 \\ D1 & 72 & 00 & 64 \end{bmatrix}$$

$$\begin{bmatrix} 65 & D4 & 83 & 05 \\ 90 & 84 & 8C & 64 \\ A3 & 9C & 7C & 37 \\ 92 & 37 & 48 & 31 \end{bmatrix}$$

- **Add Round key:**

$$\begin{bmatrix} 65 & D4 & 83 & 05 \\ 90 & 84 & 8C & 64 \\ A3 & 9C & 7C & 37 \\ 92 & 37 & 48 & 31 \end{bmatrix} \oplus \begin{bmatrix} 9A & D7 & 99 & D8 \\ DA & 9E & E6 & AC \\ 62 & 2B & 66 & 27 \\ C2 & 91 & C3 & 81 \end{bmatrix}$$

$$\begin{bmatrix} FF & 03 & 1A & DD \\ 4A & 1B & 6A & C8 \\ C1 & B7 & 1A & 10 \\ 50 & A6 & 8B & B0 \end{bmatrix}$$

Final Round:

- **Substitute Byte:**

$$\begin{bmatrix} 16 & 7B & A2 & C1 \\ D6 & AF & 02 & E8 \\ 78 & A9 & A2 & CA \\ 53 & 24 & 3D & E7 \end{bmatrix}$$

Shift Rows:

$$\begin{bmatrix} 16 & 7B & A2 & C1 \\ AF & 02 & EB & D6 \\ A2 & CA & 78 & A9 \\ E7 & 53 & 24 & 3D \end{bmatrix}$$

Add Round Key:

$$\begin{bmatrix} 16 & 7B & A2 & C1 \\ AF & 02 & E8 & D6 \\ A2 & CA & 78 & A9 \\ E7 & 53 & 24 & 3D \end{bmatrix} \oplus \begin{bmatrix} F9 & 2E & B7 & 6F \\ 4B & D4 & 32 & 9E \\ AE & 85 & E3 & C4 \\ CE & 5F & 9C & 1D \end{bmatrix}$$

$$\begin{bmatrix} EF & 55 & 15 & AE \\ E4 & D6 & DA & 48 \\ 0C & 4F & 9B & 6D \\ 29 & 0C & B8 & 20 \end{bmatrix}$$

Decryption: (Block # 1)

- **Initial Round:**

$$\begin{bmatrix} D6 & FB & C9 & 06 \\ 6D & 78 & 40 & 35 \\ 91 & 9E & 58 & 98 \\ 1E & 51 & 8D & 3D \end{bmatrix} \oplus \begin{bmatrix} F9 & 2E & B7 & 6F \\ 4B & D4 & 32 & 9E \\ AE & 85 & E3 & C4 \\ CE & 5F & 9C & 1D \end{bmatrix}$$

$$\begin{bmatrix} 2F & D5 & 7E & 69 \\ 26 & AC & 72 & AB \\ 3F & 1B & BB & 5C \\ D0 & 0E & 11 & 20 \end{bmatrix}$$

Round # 1:- (Main Round)

- **Inverse Shift Rows:**

$$\begin{bmatrix} 2F & D5 & 7E & 69 \\ AB & 26 & AC & 72 \\ BB & 5C & 3F & 1B \\ 0E & 11 & 20 & D0 \end{bmatrix}$$

- **Inverse substitute Byte:**

$$\begin{bmatrix} 4E & B5 & 8A & E4 \\ 0E & 23 & AA & 1E \\ FE & A7 & 25 & 44 \\ D7 & E3 & 54 & 60 \end{bmatrix}$$

- **Column Mixing:**

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} * \begin{bmatrix} 4E & B5 & 8A & E4 \\ 0E & 23 & AA & 1E \\ FE & A7 & 25 & 44 \\ D7 & E3 & 54 & 60 \end{bmatrix}$$

$$\begin{bmatrix} 34 & D2 & AF & C9 \\ B0 & 05 & 95 & 3D \\ 56 & 7F & A2 & CE \\ 13B & 7A & C9 & E4 \end{bmatrix}$$

- Add Round key:

$$\begin{bmatrix} 34 & D2 & AF & C9 \\ B0 & 05 & 95 & 3D \\ 56 & 7F & A2 & CE \\ BB & 7A & C9 & E4 \end{bmatrix} \oplus \begin{bmatrix} 9A & D7 & 99 & D8 \\ DA & 9F & E6 & AC \\ 62 & 2B & 66 & 27 \\ C2 & 91 & C3 & 81 \end{bmatrix}$$

$$\begin{bmatrix} AE & D5 & 36 & 11 \\ 6A & 9A & 73 & 91 \\ 34 & 54 & C4 & E9 \\ 79 & EB & 0A & 65 \end{bmatrix}$$

- Final Round:
- Inverse Shift Row:

$$\begin{bmatrix} AE & D5 & 36 & 11 \\ 91 & 6A & 9A & 73 \\ C4 & E9 & 34 & 54 \\ EB & 0A & 65 & 79 \end{bmatrix}$$

- Inverse substitute Byte:

$$\begin{bmatrix} BE & B5 & 24 & E3 \\ AC & 58 & 37 & 8F \\ 88 & EB & 28 & FD \\ 3C & A3 & BC & AF \end{bmatrix}$$

- Add Round key.

$$\begin{bmatrix} BE & B5 & 24 & E3 \\ AC & 58 & 37 & 8F \\ 88 & EB & 28 & FD \\ 3C & A3 & BC & AF \end{bmatrix} \oplus \begin{bmatrix} 4D & 4D & 4E & 41 \\ 59 & 45 & 49 & 4A \\ 4E & 49 & 4D & 41 \\ 41 & 53 & 52 & 42 \end{bmatrix}$$

$$\begin{bmatrix} F3 & F8 & 6A & A2 \\ F5 & 1D & 7E & C5 \\ C6 & A2 & 64 & BC \\ 7D & F0 & EE & ED \end{bmatrix}$$

(Block # 2)

$$\begin{bmatrix} EF & 55 & 15 & AE \\ E4 & D6 & DA & 48 \\ 0C & 4F & 9B & 6D \\ 29 & 0C & B8 & 20 \end{bmatrix}$$

- Initial Round:

$$\begin{bmatrix} EF & 55 & 16 & AE \\ E4 & D6 & DA & 48 \\ 0C & 4F & 9B & 6D \\ 29 & 0C & B8 & 20 \end{bmatrix} \oplus \begin{bmatrix} F9 & 2E & B7 & 6F \\ 4B & D4 & 32 & 9E \\ AE & 85 & E3 & C4 \\ CE & 5F & 9C & 1D \end{bmatrix}$$

$$= \begin{bmatrix} 16 & 7B & A2 & C1 \\ AF & 02 & E8 & D6 \\ A2 & CA & 78 & A9 \\ E7 & 53 & 24 & 3D \end{bmatrix}$$

Round # 1 (Main Round)

- Inverse Shift Row:

$$\begin{bmatrix} 16 & 7B & A2 & C1 \\ D6 & AF & 02 & E8 \\ 78 & A9 & A2 & CA \\ 53 & 24 & 3D & E7 \end{bmatrix}$$

- Inverse Substitute Byte:

$$\begin{bmatrix} FF & 03 & 1A & DD \\ 4A & 2B & 6A & C8 \\ C1 & B7 & 1A & 10 \\ 50 & A6 & 8b & B0 \end{bmatrix}$$

Column Mixing:

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \times \begin{bmatrix} FF & 03 & 1A & DD \\ 4A & 1B & 6A & C8 \\ C1 & 87 & A1 & 10 \\ 50 & A6 & 8b & B0 \end{bmatrix}$$

$$\begin{bmatrix} 69 & FF & 52 & 84 \\ 30 & 10 & 8B & F2 \\ 1F & 09 & 8B & 38 \\ 62 & DF & B3 & FB \end{bmatrix}$$

Add Round key:

$$\begin{bmatrix} 69 & FF & 52 & 84 \\ 30 & 10 & 8B & F2 \\ 1F & 09 & 8B & 38 \\ 62 & DF & B3 & FB \end{bmatrix} \oplus \begin{bmatrix} 9A & D7 & 99 & D8 \\ DA & 9F & E6 & AC \\ 62 & 2B & 66 & 27 \\ C2 & 91 & C3 & 81 \end{bmatrix}$$

$$\begin{bmatrix} F3 & 28 & CB & 5C \\ EA & 8F & 6D & 5E \\ 7D & 22 & ED & 1F \\ A0 & 4E & 70 & 7A \end{bmatrix}$$

Final Round:

- **Inverse shift row:**

$$\begin{bmatrix} F3 & 28 & CB & 5C \\ 5E & EA & 8F & 6D \\ ED & 1F & 7D & 22 \\ 4E & 70 & 7A & A0 \end{bmatrix}$$

Inverse substitute Byte:

$$\begin{bmatrix} 7E & EE & 59 & A7 \\ 9D & BB & 73 & B3 \\ 53 & CB & 13 & 94 \\ b6 & D0 & BD & 47 \end{bmatrix}$$

Add Round key:

$$\begin{bmatrix} 7E & EE & 59 & A7 \\ 9D & BB & 73 & B3 \\ 53 & CB & 13 & 94 \\ b6 & D0 & BD & 47 \end{bmatrix} \oplus \begin{bmatrix} 4D & 4D & 4E & 41 \\ 59 & 45 & 49 & 4A \\ 4E & 49 & 4D & 41 \\ 41 & 53 & 52 & 42 \end{bmatrix}$$

$$\begin{bmatrix} 33 & A3 & 17 & E6 \\ C4 & FE & 3A & F9 \\ 1D & 82 & 5E & D5 \\ F7 & 83 & EF & 05 \end{bmatrix}$$

- XOR with I.V

$$\begin{bmatrix} 00 & 06 & 06 & 01 \\ 02 & 00 & 08 & 03 \\ 04 & 09 & 02 & 05 \\ 01 & 03 & 04 & 00 \end{bmatrix} \oplus \begin{bmatrix} 33 & A3 & 17 & E6 \\ C4 & FE & 3A & F9 \\ 1D & 82 & 5E & D5 \\ F7 & 83 & EF & 05 \end{bmatrix}$$

$$\begin{bmatrix} 33 & A5 & 11 & E7 \\ C6 & FE & 32 & FA \\ 19 & 8B & 5C & D0 \\ F6 & 80 & EB & 05 \end{bmatrix}$$