Date : ______________

Cryptography and Network Security

Digital Assignment — I

[redacted]

Course code : BCSE309L
Slot : E2 + TE2
Class no. : 0744

Question.

Given the plaintext {0F0E0D0C 0B0A0908 0706050403020100} and the Key {0202020202020202020202020202 0202} :

a) Show the original contents of state, displayed as a 4 × 4 matrix.

b) Show the value of state after initial AddRoundKey.

c) Show the value of state after SubBytes.

d) Show the value of state after Shiftrows.

e) Show the value of state after MixColumns.

Date :

Answer

a) The original contents of State, displayed as a 4 × 4 matrix.

$$\text{State} = \begin{bmatrix} 00 & 04 & 08 & 0C \\ 01 & 05 & 09 & 0D \\ 02 & 06 & 0A & 0E \\ 03 & 07 & 0B & 0F \end{bmatrix}$$

arrangement of values of plaintext in 4 × 4 matrix.

$$\text{Key} = \begin{bmatrix} 02 & 02 & 02 & 02 \\ 02 & 02 & 02 & 02 \\ 02 & 02 & 02 & 02 \\ 02 & 02 & 02 & 02 \end{bmatrix}$$

arrangement of values of key in 4 × 4 matrix

Date : ____________

b) The value of state after initial AddRoundKey.

After AddRoundKey.

We do XOR for 00 $\oplus$ 02, 01 $\oplus$ 02 and so on.

For example, 00 $\oplus$ 02, we need to convert those into binary & then do XOR (if both bits are 1 then xORed bit will be 0, if both bits are 0 then xORed bit will be 0, if one of the bit is 0 & one bit is 1 then xORed bit will be 1] operation.

Then we get the hexadecimal equivalent.

$$\begin{array}{lcl} 00 & = & 00000000 \\ 02 & = & 00000010 \\ \hline \oplus\; 02 & = & 00000010 \end{array}$$

XOR

i/p		o/p
0	0	0
0	1	1
1	0	1
1	1	0

$$\begin{bmatrix} 00 & 04 & 08 & 0C \\ 01 & 05 & 09 & 0D \\ 02 & 06 & 0A & 0E \\ 03 & 07 & 0B & 0F \end{bmatrix} \oplus \begin{bmatrix} 02 & 02 & 02 & 02 \\ 02 & 02 & 02 & 02 \\ 02 & 02 & 02 & 02 \\ 02 & 02 & 02 & 02 \end{bmatrix}$$

$$= \begin{bmatrix} 02 & 06 & 0A & 0E \\ 03 & 07 & 0B & 0F \\ 00 & 04 & 08 & 0C \\ 01 & 05 & 09 & 0D \end{bmatrix}$$

$\nearrow$ xoRed with plaintext matrix.

01 = 00000001
02 = 00000010
⊕ 03 = 00000011

02 = 00000010
02 = 00000010
⊕ 00 = 00000000

03 = 00000011
02 = 00000010
⊕ 01 = 00000001

06 = 00000110
02 = 00000010
⊕ 04 = 00000100

07 = 00000111
02 = 00000010
⊕ 05 = 00000101

08 = 00001000
02 = 00000010
⊕ 0A = ~~0~~00010010

09 = 00001001
02 = 00000010
⊕ 0B = 00001011

04 = 00000100
⊕ 02 = 00000010
06 = 00000110

05 = 00000101
⊕ 02 = 00000010
07 = 00000111

0A = 00001010
⊕ 02 = 00000010
08 = 00001000

0B = 00001011
⊕ 02 = 00000010
09 = 00001001

0C = 00001100
⊕ 02 = 00000010
0E = 00001110

0D = 00001101
⊕ 02 = 00000010
0F = 00001111

0E = 00001110
⊕ 02 = 00000010
0C = 00001100

Date :

c) The value of state after Subbytes

In this step, we use a lookup table called S-box to perform a byte-by-byte substitution of the block.

For example,

9E	Row 9 → Column E	0B

So, the value of State after SubBytes :—

$$\begin{bmatrix} 02 & 06 & 0A & 0E \\ 03 & 07 & 0B & 0F \\ 00 & 04 & 08 & 0C \\ 01 & 05 & 09 & 0D \end{bmatrix} \Rightarrow \begin{bmatrix} 27 & 71 & 72 & 2B \\ 80 & 23 & AB & 6F \\ 7F & 6E & FA & D4 \\ 45 & 83 & 7D & 6B \end{bmatrix}$$

d) Value of state after ShiftRows

In this step, a forward shift row transformation, called ShiftRows, is performed.

→ The first row of state is not altered.

→ For the second row, a 1-byte circular left shift is performed.

→ For the third row, a 2 byte circular left shift is performed.

→ For the fourth row, a 3 byte circular left shift is performed.

So, the value of state after ShiftRows :—

$$\begin{bmatrix} 27 & 71 & 72 & 2B \\ 80 & 23 & AB & 6F \\ 7F & 6E & FA & D4 \\ 45 & 83 & 7D & 6B \end{bmatrix} \Rightarrow \begin{bmatrix} 80 & 6E & 7D & 2B \\ 7F & 83 & 72 & 6F \\ 45 & 71 & AB & D4 \\ 27 & 23 & FA & 6B \end{bmatrix}$$

Date : ____________

e) Value of State after MixColumns.

In this step, each column of state matrix is multiplied with a fixed polynomial modulo $(x^4 + 1)$ over $GF(2^8)$ and then reduced modulo $x^4 + 1$.

Mix Columns :

$$\begin{bmatrix} 65 & 8E & 4B & A4 \\ B0 & 72 & B1 & 86 \\ D5 & 13 & 1F & 27 \\ B5 & D6 & 77 & 5D \end{bmatrix}$$

These are values of the State Matrix after each step of AES encryption process with the given plaintext and Key.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Table 1: S-box