Show the output After one AES Round if (Show your work) :
Input = **ea835cF00445332d655d98ad8596b0c5**
Cipher Key = **ac7766f319fadc2128d12941575c006a**
Constant of multiplication by X = (0001 1011).

- Find the four state as follows:
- Sub-byte for all bytes of the state
- Shift Row all bytes of the state
- Mix-Column for the first byte of the resultant state
- Add-Round for the first byte of the resultant state

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

(a) S-box

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	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

AES Single Round Example

The Input block of data to a single round of AES algorithm with 128 bits length is

EA	04	65	85
83	45	5D	96
5C	33	98	B0
F0	2D	AD	C5

and a round key input to this round is

AC	19	28	57
77	FA	D1	5C
66	DC	29	00
F3	21	41	6A

Find the data of output block from this round

Answer:

After Substitute Bytes Transformation

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

After Shift Row Transformation

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

After Mix Column Transformation

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 87 & F2 & 4D & 97 \\ 6E & 4C & 90 & EC \\ 46 & E7 & 4A & C3 \\ A6 & 8C & D8 & 95 \end{bmatrix} = \begin{bmatrix} 47 & 40 & A3 & 4C \\ 37 & D4 & 70 & 9F \\ 94 & E4 & 3A & 42 \\ ED & A5 & A6 & BC \end{bmatrix}$$

- To find the first byte after Mix Column, we do matrix multiplication over GF(2^8) as follows:

$$(02 * 87) \oplus (03 * 6E) \oplus 46 \oplus A6 = 47$$

We have $02 * 87 = (0000\ 0010) * (1000\ 0111) = (0000\ 1110) \oplus (0001\ 1011)$

$$= (0001\ 0101)$$

After Mix Column Transformation

- To find the first byte after Mix Column, we do matrix multiplication over $GF(2^8)$ as follows:

In particular, multiplication of a value by (i.e., by {02}) can be implemented as a 1-bit left shift followed by a conditional bitwise XOR with (0001 1011)

$(02 * 87) \oplus (03 * 6E) \oplus 46 \oplus A6 = 47$

We have $02 * 87 = (0000\ 0010) * (1000\ 0111) = (0000\ 1110) \oplus (0001\ 1011)$
$= (0001\ 0101)$

and $(03 * 6E) = (0000\ 0011) * (0110\ 1110) = (0000\ 0001) * (0110\ 1110) \oplus (0000\ 0010) * (0110\ 1110)$

$= (0110\ 1110) \oplus (1101\ 1100) = (1011\ 0010)$

and $(46) = (0100\ 0110)$

and $(A6) = (1010\ 0110)$

Then the first byte $= (0001\ 0101) \oplus (1011\ 0010) \oplus (0100\ 0110) \oplus (1010\ 0110) = (0100\ 0111) = (47)$

- After Add Round Key Transformation

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

$\oplus$

AC	19	28	57
77	FA	D1	5C
66	DC	29	00
F3	21	41	6A

=

EB	59	8B	1B
40	2E	A1	C3
F2	38	13	42
1E	84	E7	D2

The value of the first byte of after Add Round Key = (47) $\oplus$ (AC)

(47) $\oplus$ (AC) = (0100 0111) $\oplus$ (1010 1100) = (1110 1011) = (EB)

The value of the first byte of after Add Round Key = (47) $\oplus$ (AC) = (EB)