16-124-836
Marcel Matti ZAUDER

2.4 Question 4

2.4.A Given Plaintext and Key

PLAINTEXT: 0F 0E 0D 0C 0B 0A 09 08 07 06 05 04 03 02 01 00
KEY: 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02

Show the original contents of STATE as a 4x4 matrix

0F	0B	07	03
0E	0A	06	02
0D	09	05	01
0C	08	04	00

Show the value of STATE after initial AddRoundKey

0D	09	05	01
0C	08	04	00
0F	0B	07	03
0E	0A	06	02

Show the value of STATE after SubBytes

D7	01	6B	7C
FE	30	F2	63
76	2B	C5	7B
AB	67	6F	77

Show the value of STATE after ShiftRows

D7	01	6B	7C
30	F2	63	FE
C5	7B	76	2B
77	AB	67	6F

Show the value of STATE after MixColumns

57	DF	62	A5
94	D8	50	89
EF	E3	4D	65
79	C7	66	8F

2.4.B Show the first eight words of the key expansion for a 128-bit key of value 1. Assume that you are in the first round.

128-bit KEY: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01

$$\mathcal{W}(0) = \begin{bmatrix} 0x0 \\ 0x0 \\ 0x0 \\ 0x0 \end{bmatrix}, \mathcal{W}(1) = \begin{bmatrix} 0x0 \\ 0x0 \\ 0x0 \\ 0x0 \end{bmatrix}, \mathcal{W}(2) = \begin{bmatrix} 0x0 \\ 0x0 \\ 0x0 \\ 0x0 \end{bmatrix}, \mathcal{W}(3) = \begin{bmatrix} 0x0 \\ 0x0 \\ 0x0 \\ 0x1 \end{bmatrix}$$

16-124-836
Marcel Matti ZAUDER

$$\mathcal{W}(4) = \begin{bmatrix} 0x62 \\ 0x63 \\ 0x7c \\ 0x63 \end{bmatrix}, \mathcal{W}(5) = \begin{bmatrix} 0x62 \\ 0x63 \\ 0x7c \\ 0x63 \end{bmatrix}, \mathcal{W}(6) = \begin{bmatrix} 0x62 \\ 0x63 \\ 0x7c \\ 0x63 \end{bmatrix}, \mathcal{W}(7) = \begin{bmatrix} 0x62 \\ 0x63 \\ 0x7c \\ 0x62 \end{bmatrix}$$