UEE4611 Assignment #5 Solution

1.

(a) Determine the multiplicative inverse of $\{02\}$ in $GF(2^8) = \mathbb{Z}_2[x]/x^8 + x^4 + x^3 + x + 1\rangle$.

(b) Verify the entry for $\{02\}$ in the S-box.

(a)

$\{02\}$ is equivalent to $\{00000010\}$ in $GF(2^8) = \mathbb{Z}_2[x]/x^8 + x^4 + x^3 + x + 1\rangle$, which can be represented as x.
So the question can be expressed as $xp(x) \equiv 1(\mod x^8 + x^4 + x^3 + x + 1)$. And by Extended Euclidean algorithm, we can get that

$$x^8 + x^4 + x^3 + x + 1 = x(x^7 + x^3 + x^2 + 1) + 1.$$

So we know that the multiplicative inverse of x in $GF(2^8)$ is $x^7 + x^3 + x^2 + 1$, which can be represented as $\{10001101\}$ or $\{8D\}$.

(b)

$$X \times B \oplus C = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \{77\}$$

2.Consider the encryption algorithm of AES. Given the plaintext

$$\{0F0E0D0C0B0A09080706050403020100\}$$

and the key

$$\{20202020202020202020202020202020202\},$$

(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.

(a)

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

(b)

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

(c)

$$B' = XB \oplus C, \textbf{where } X = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}, C = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

$$B = \{02\}^{-1} = \{8D\} = \{10001101\}$$

$$\Rightarrow XB \oplus C = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

After calculations, we obtain $\begin{bmatrix} D7 & 01 & 6B & 7C \\ FE & 30 & F2 & 63 \\ 76 & 2B & C5 & 7B \\ AB & 67 & 6F & 77 \end{bmatrix}$.

(d)

$$\begin{bmatrix} D7 & 01 & 6B & 7C \\ 30 & F2 & 63 & FE \\ C5 & 7B & 76 & 2B \\ 77 & AB & 67 & 6F \end{bmatrix}$$

(e)

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} D7 & 01 & 6B & 7C \\ 30 & F2 & 63 & FE \\ C5 & 7B & 76 & 2B \\ 77 & AB & 67 & 6F \end{bmatrix} = \begin{bmatrix} 57 & DF & 62 & A5 \\ 94 & D8 & 50 & 89 \\ EF & E3 & 4D & 65 \\ 79 & C7 & 66 & 8F \end{bmatrix}$$

$$S_{00} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \oplus \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$
$$\oplus \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \oplus \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} = 57$$

Other factors can be determined in the same way.