Math 314 - Fall 2019 **Name:**_____
Mission 6 Partner:_____
Note: This mission must be turned in on this sheet to receive credit.

S-BOX for S-AES

Input	Output		Input	Output
0000	1001		1000	0110
0001	0100		1001	0010
0010	1010		1010	0000
0011	1011		1011	0011
0100	1101		1100	1100
0101	0001		1101	1110
0110	1000		1110	1111
0111	0101		1111	0111

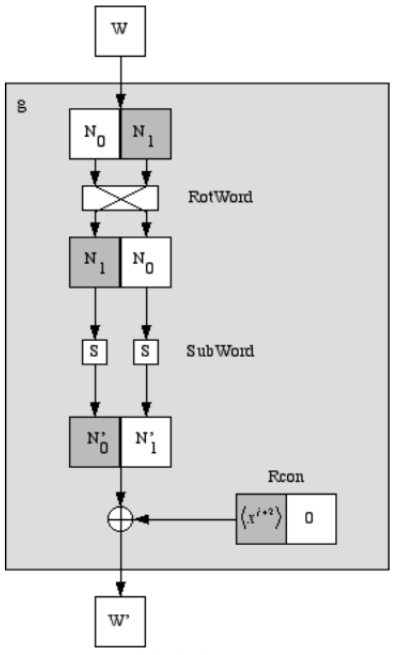
1. Using S-AES encrypt $P_1 = 1100110011110111$ using the key $K = 1110111011110001$.

Determine the RoundKeys: Start with $K_0 = 1110111011110001$

Break into two pieces: $W_0 =$ _____ $W_1 =$ _____

Compute $g(W_1)$: (Remember, $i = 1$ in this step.)

Show your work here:



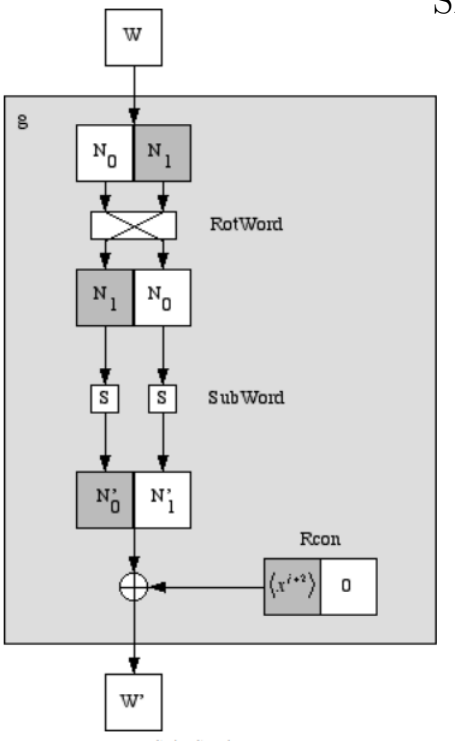
$g(W_1)$: _____

$W_2 = W_0 \oplus g(W_1)$: _____ $W_3 = W_1 \oplus W_2$:_____.

$K_1 = W_2W_3$: _____.

Compute $g(W_3)$: (Remember, $i = 2$ in this step.)

Show your work here:



$g(W_3)$: _____

$W_4 = W_2 \oplus g(W_3)$: _____ $W_5 = W_3 \oplus W_4$:_____.

$K_2 = W_4W_5$: _____.

Round 0: Add Round Key: $P_1 \oplus K_0$: _____.

Round 1: Substitution: _____ _____ _____ _____.

Round 1: Shift Rows: First, write as a matrix filling entries in down *columns*,

$$\begin{bmatrix} \_\_\_\_\_ & \_\_\_\_\_ \\ \_\_\_\_\_ & \_\_\_\_\_ \end{bmatrix}$$

Then shift the entries in the bottom row.

Resulting Matrix: $\begin{bmatrix} \_\_\_\_\_ & \_\_\_\_\_ \\ \_\_\_\_\_ & \_\_\_\_\_ \end{bmatrix}$

Round 1: Mix Columns:

Convert elements to $\mathbb{F}_{16}$, and then perform the matrix multiplication:

$$EM = \begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix} \begin{bmatrix} \_\_\_\_\_ & \_\_\_\_\_ \\ \_\_\_\_\_ & \_\_\_\_\_ \end{bmatrix} = \begin{bmatrix} \_\_\_\_\_ & \_\_\_\_\_ \\ \_\_\_\_\_ & \_\_\_\_\_ \end{bmatrix}$$

$$\equiv \begin{bmatrix} \_\_\_\_\_ & \_\_\_\_\_ \\ \_\_\_\_\_ & \_\_\_\_\_ \end{bmatrix} \pmod{x^4 + x + 1}.$$

Round 1: Add Round Key:

Rewrite as string C_1 : _____

Compute $C_1 \oplus K_1$: _____

Round 2: Substitution: _____ _____ _____ _____.

Round 2: Shift Rows: First, write as a matrix filling entries in down *columns*,

$$\begin{bmatrix} \_\_\_\_\_ & \_\_\_\_\_ \\ \_\_\_\_\_ & \_\_\_\_\_ \end{bmatrix}$$

Then shift the entries in the bottom row.

Resulting Matrix: $\begin{bmatrix} \_\_\_\_\_ & \_\_\_\_\_ \\ \_\_\_\_\_ & \_\_\_\_\_ \end{bmatrix}$

Round 2: Add Round Key:

Rewrite as string C_2 : _____

Compute $C_2 \oplus K_2$: _____

Final Cipher Text: $C =$ _____

---

2. Recall the encryption matrix for AES is $E = \begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix}$ over the finite field $\mathbb{F}_{16}$ with irreducible polynomial x^4+x+1. Compute the decryption matrix $D = E^{-1}$.