Math 314 - Spring 2018 **Name:**_____
Mission 7 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

Use S-AES to encrypt the plaintext $P_1 = 1100110011110101$ using the key $K = 1110111011110000$.

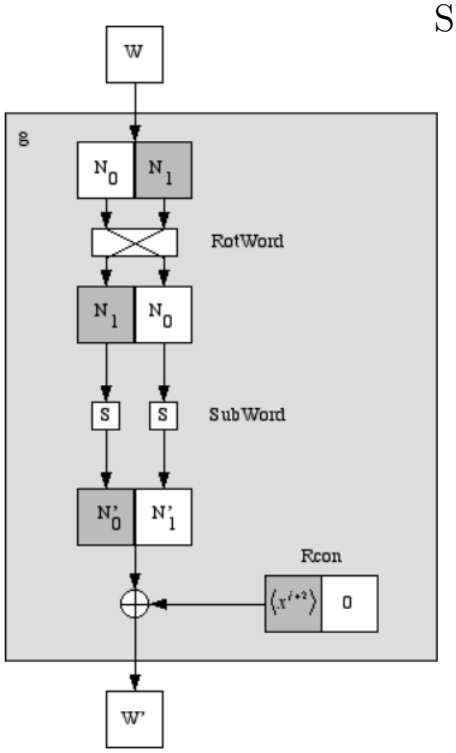
Determine the RoundKeys:

$K_0 = 1110111011110000$

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

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

Show your work here:



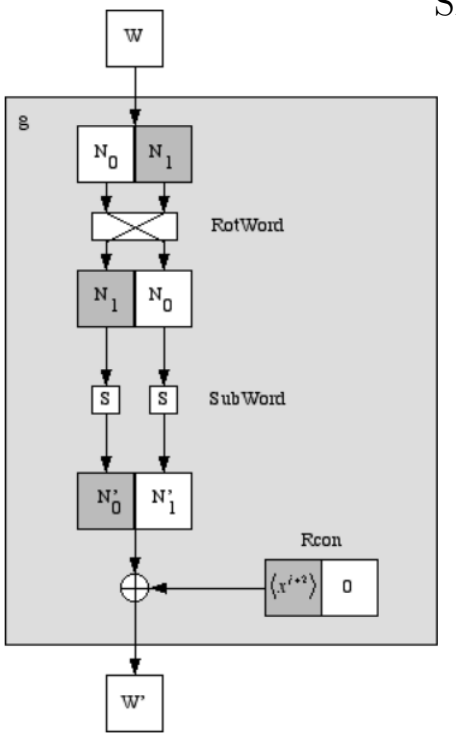
$g(W_1)$: _____

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

$K_1 = W_2 W_3$: _____.

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

Show your work here:



$g(W_3)$: _____

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

$K_2 = W_4 W_5$: _____.

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:

$$EM = \begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix} \begin{bmatrix} \underline{\qquad\qquad} & \underline{\qquad\qquad} \\ \underline{\qquad\qquad} & \underline{\qquad\qquad} \end{bmatrix} = \begin{bmatrix} \underline{\qquad\qquad} & \underline{\qquad\qquad} \\ \underline{\qquad\qquad} & \underline{\qquad\qquad} \end{bmatrix}$$
$$\equiv \begin{bmatrix} \underline{\qquad\qquad} & \underline{\qquad\qquad} \\ \underline{\qquad\qquad} & \underline{\qquad\qquad} \end{bmatrix} \pmod{x^4 + x + 1}.$$

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*,

$$\begin{bmatrix} \underline{\qquad} & \underline{\qquad} \\ \underline{\qquad} & \underline{\qquad} \end{bmatrix}$$

Then shift the entries in the bottom row.

Resulting Matrix: $\begin{bmatrix} \underline{\qquad} & \underline{\qquad} \\ \underline{\qquad} & \underline{\qquad} \end{bmatrix}$

Round 2: Add Round Key:
Rewrite as string C_2 : _____
Compute $C_2 \oplus K_2$: _____
Final Cipher Text: $C =$ _____

Part 2: Modes of Operation

Check your work with Sage! Correct the above as necessary.

Now, suppose that in addition to the plaintext from part 1, $P_1 = 1100110011110101$ you also want to send a second message, $P_2 = 1011011101111011$, using the same key. Using Sage (no need to do this by hand) determine the corresponding ciphertexts to be sent if you are using:

Electronic Codebook (ECB):

$C_1 = E_K(P_1)$:_____

$C_2 = E_K(P_2)$:_____

Cipher Block Chaining (CBC): (Use $C_0 = 0000000000000000$.)

$C_1 = E_K(P_1 \oplus C_0)$:_____

$C_2 = E_K(P_2 \oplus C_1)$:_____

Note: For the following modes, you will instead need to break your plaintext into 4 pieces with 8 bits each, $P_1 = 11001100$, $P_2 = 11110101$, $P_3 = 10110111$, $P_4 = 01111011$. The functions *head* and *tail* grab the left 8 and right 8 bits of a binary string respectively.

Cipher Feedback (CFB): (Use $X_1 = 0000000000000000$.)

$O_1 = head(E_K(X_1))$:_____ $C_1 = P_1 \oplus O_1$:_____

$X_2 = tail(X_1)C_1$:_____

O_2 :_____ C_2 :_____ X_3 :_____

O_3 :_____ C_3 :_____ X_4 :_____

O_4 :_____ C_4 :_____

Output Feedback (OFB): (Use $X_1 = 0000000000000000$.)

$O_1 = head(E_K(X_1))$:_____ $C_1 = P_1 \oplus O_1$:_____

$X_2 = tail(X_1)O_1$:_____

O_2 :_____ C_2 :_____ X_3 :_____

O_3 :_____ C_3 :_____ X_4 :_____

O_4 :_____ C_4 :_____

Counter (CTR): (Use $X_0 = 0000000000000000$.)

X_1 :_____ $O_1 = head(E_K(X_1))$:_____

$C_1 = P_1 \oplus O_1$:_____

X_2 :_____ O_2 :_____ C_2 :_____

X_3 :_____ O_3 :_____ C_3 :_____

X_4 :_____ O_4 :_____ C_4 :_____