Math 314 - Spring 2020 **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

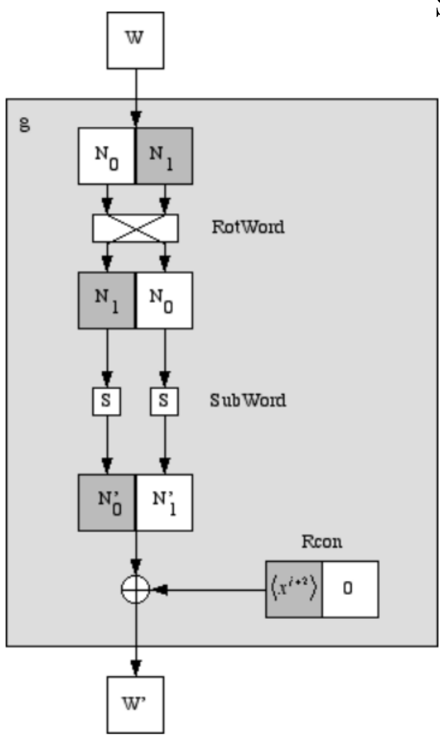
Use S-AES to encrypt the plaintext $P_1 = 1110110011110101$ using the key $K = 0010111011110000$.

Determine the RoundKeys:

$K_0 = 0010111011110000$

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

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



Show your work here:

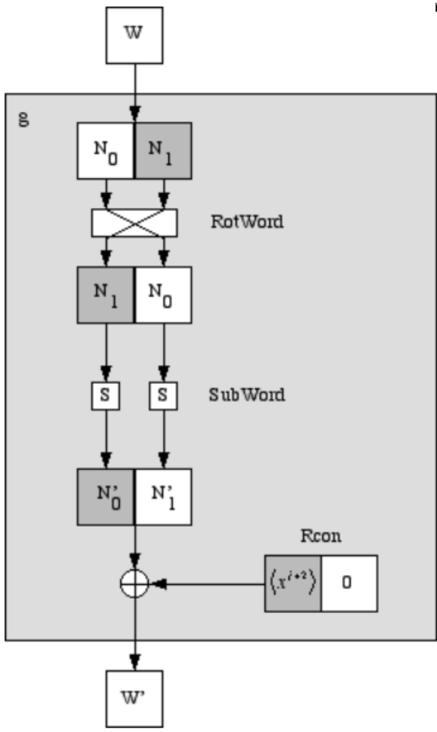
$g(W_1)$: ______________ W_1 : ______________

$\oplus W_0$: ______________ $\oplus W_2$: ______________

$= W_2$: ______________ $= W_3$: ______________

$K_1 = W_2 W_3$: ____________________________.

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



Show your work here:

$g(W_3)$: ______________ W_3 : ______________

$\oplus W_2$: ______________ $\oplus W_4$: ______________

$= W_4$: ______________ $= W_5$: ______________

$K_2 = W_4 W_5$: ____________________________.

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*. Then shift the entries in the bottom row.

$$\begin{bmatrix} \underline{\hspace{1.5cm}} & \underline{\hspace{1.5cm}} \\ \underline{\hspace{1.5cm}} & \underline{\hspace{1.5cm}} \end{bmatrix} \qquad \text{Resulting Matrix: } \begin{bmatrix} \underline{\hspace{1.5cm}} & \underline{\hspace{1.5cm}} \\ \underline{\hspace{1.5cm}} & \underline{\hspace{1.5cm}} \end{bmatrix}$$

Round 1: Mix Columns:

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

$$EM = \begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix} \begin{bmatrix} \underline{\hspace{2cm}} & \underline{\hspace{2cm}} \\ \underline{\hspace{2cm}} & \underline{\hspace{2cm}} \end{bmatrix} = \begin{bmatrix} \underline{\hspace{2.5cm}} & \underline{\hspace{2.5cm}} \\ \underline{\hspace{2.5cm}} & \underline{\hspace{2.5cm}} \end{bmatrix}$$

$$\equiv \begin{bmatrix} \underline{\hspace{2cm}} & \underline{\hspace{2cm}} \\ \underline{\hspace{2cm}} & \underline{\hspace{2cm}} \end{bmatrix} \quad (\mathrm{mod}\ x^4 + x + 1).$$

Round 1: Add Round Key:

Rewrite as string

C_1 :__________________________

$\oplus K_1$:__________________________

=__________________________.

Round 2: Substitution: ______ ______ ______ ______.

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

$$\begin{bmatrix} \underline{\hspace{1.5cm}} & \underline{\hspace{1.5cm}} \\ \underline{\hspace{1.5cm}} & \underline{\hspace{1.5cm}} \end{bmatrix}$$

Then shift the entries in the bottom row.

Resulting Matrix: $\begin{bmatrix} \underline{\hspace{1.5cm}} & \underline{\hspace{1.5cm}} \\ \underline{\hspace{1.5cm}} & \underline{\hspace{1.5cm}} \end{bmatrix}$

Round 2: Add Round Key:

Rewrite as string

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, $P_1 = 1110110011110101$ you also want to send a second message, $P_2 = 1111011101111011$, 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 $C_0 = 0000000000000000$.)

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

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

Cipher Feedback (CFB): (Use $C_0 = 0000000000000000$.)

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

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

Output Feedback (OFB): (Use $O_0 = 0000000000000000$.)

$O_1 = E_K(O_0)$:________________________

$C_1 = O_1 \oplus P_1$:________________________

$O_2 = E_K(O_1)$:________________________

$C_2 = O_2 \oplus P_2$:________________________

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

X_1 :________________________

$C_1 = E_K(X_1) \oplus P_1$:________________________

X_2 :________________________

$C_2 = E_K(X_2) \oplus P_2$:________________________