

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 $K = 1110111011110000$.

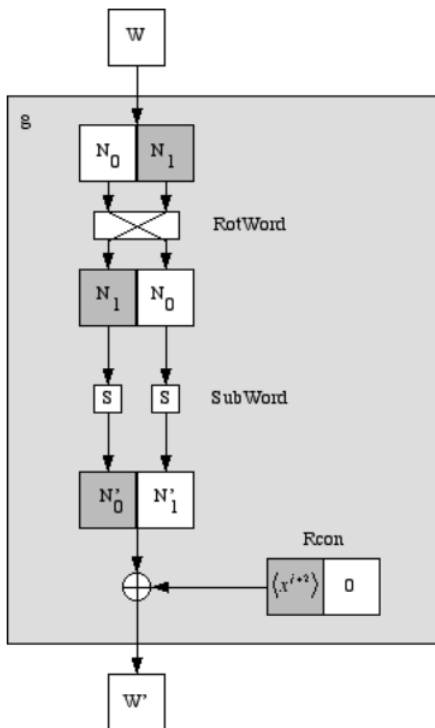
Determine the RoundKeys:

$K_0 = 1110111011110000$

Break into two pieces: $W_0 = \underline{\hspace{2cm}}$ $W_1 = \underline{\hspace{2cm}}$

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

Show your work here:



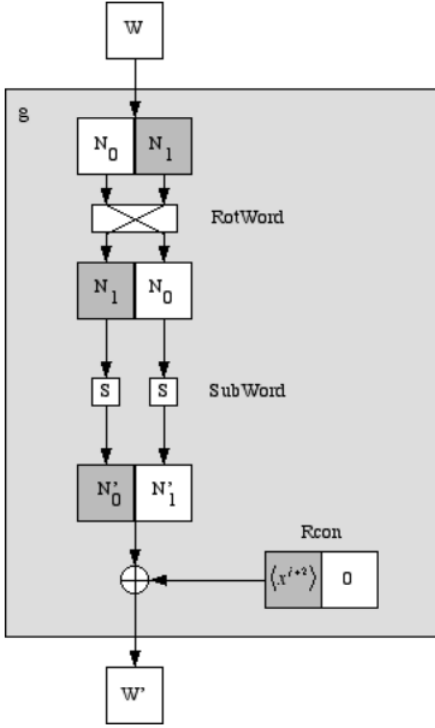
$g(W_1) : \underline{\hspace{2cm}}$

$W_2 = W_0 \oplus g(W_1) : \underline{\hspace{2cm}}$ $W_3 = W_1 \oplus W_2 : \underline{\hspace{2cm}}$.

$K_1 = W_2W_3 : \underline{\hspace{2cm}}$.

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

Show your work here:



$g(W_3) : \underline{\hspace{2cm}}$

$W_4 = W_2 \oplus g(W_3) : \underline{\hspace{2cm}}$ $W_5 = W_3 \oplus W_4 : \underline{\hspace{2cm}}$.

$K_2 = W_4W_5 : \underline{\hspace{2cm}}$.

Round 0: Add Round Key: $P_1 \oplus K_0 : \underline{\hspace{2cm}}$.

Round 1: Substitution: $\underline{\hspace{2cm}}$.

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

$$\begin{bmatrix} \underline{\hspace{1cm}} & \underline{\hspace{1cm}} \\ \underline{\hspace{1cm}} & \underline{\hspace{1cm}} \end{bmatrix}$$

Then shift the entries in the bottom row.

Resulting Matrix: $\begin{bmatrix} \underline{\hspace{1cm}} & \underline{\hspace{1cm}} \\ \underline{\hspace{1cm}} & \underline{\hspace{1cm}} \end{bmatrix}$

Round 1: Mix Columns:

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

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

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*,

$$\begin{bmatrix} \underline{\hspace{2cm}} & \underline{\hspace{2cm}} \\ \underline{\hspace{2cm}} & \underline{\hspace{2cm}} \end{bmatrix}$$

Then shift the entries in the bottom row.

Resulting Matrix: $\begin{bmatrix} \underline{\hspace{2cm}} & \underline{\hspace{2cm}} \\ \underline{\hspace{2cm}} & \underline{\hspace{2cm}} \end{bmatrix}$

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):

$$C_1 = E_K(P_1) : \underline{\hspace{10em}}$$

$$C_2 = E_K(P_2) : \underline{\hspace{10em}}$$

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

$$C_1 = E_K(P_1 \oplus C_0) : \underline{\hspace{10em}}$$

$$C_2 = E_K(P_2 \oplus C_1) : \underline{\hspace{10em}}$$

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

$$C_1 = E_K(C_0) \oplus P_1 : \underline{\hspace{10em}}$$

$$C_2 = E_K(C_1) \oplus P_2 : \underline{\hspace{10em}}$$

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

$$O_1 = E_K(O_0) : \underline{\hspace{10em}}$$

$$C_1 = O_1 \oplus P_1 : \underline{\hspace{10em}}$$

$$O_2 = E_K(O_1) : \underline{\hspace{10em}}$$

$$C_2 = O_2 \oplus P_2 : \underline{\hspace{10em}}$$

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

$$X_1 : \underline{\hspace{10em}}$$

$$C_1 = E_K(X_1) \oplus P_1 : \underline{\hspace{10em}}$$

$$X_2 : \underline{\hspace{10em}}$$

$$C_2 = E_K(X_2) \oplus P_2 : \underline{\hspace{10em}}$$