

**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  $K = 1110111011110000$ .

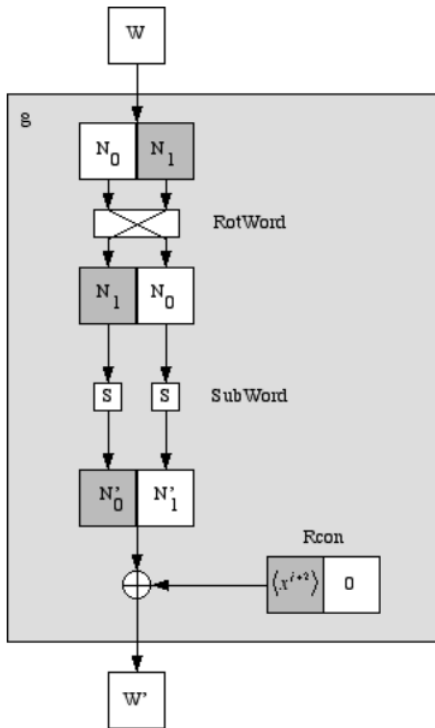
**Determine the RoundKeys:**

$K_0 = 1110111011110000$

Break into two pieces:  $W_0 =$  \_\_\_\_\_  $W_1 =$  \_\_\_\_\_

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

Show your work here:



$g(W_1) :$  \_\_\_\_\_



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

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

**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.

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

**Round 2:** Add Round Key:

Rewrite as string  $C_2$  : \_\_\_\_\_

Compute  $C_2 \oplus K_2$  : \_\_\_\_\_

**Final Cipher Text:**  $C =$  \_\_\_\_\_

## Part 2

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

Now, suppose 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,  $P_1 = 00110000$ ,  $P_2 = 11110101$ ,  $P_3 = 10110111$ ,  $P_4 = 01111011$ . The functions  $L_8$  and  $R_8$  grab the left 8 and right 8 bits of a binary string respectively.

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

$$O_1 = L_8(E_K(X_1)) : \underline{\hspace{10em}} \quad C_1 = P_1 \oplus O_1 : \underline{\hspace{10em}}$$

$$X_2 = R_8(X_1)C_1 : \underline{\hspace{10em}}$$

$$O_2 : \underline{\hspace{10em}} \quad C_2 : \underline{\hspace{10em}} \quad X_3 : \underline{\hspace{10em}}$$

$$O_3 : \underline{\hspace{10em}} \quad C_3 : \underline{\hspace{10em}} \quad X_4 : \underline{\hspace{10em}}$$

$$O_4 : \underline{\hspace{10em}} \quad C_4 : \underline{\hspace{10em}}$$

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

$$O_1 = L_8(E_K(X_1)) : \underline{\hspace{10em}} \quad C_1 = P_1 \oplus O_1 : \underline{\hspace{10em}}$$

$$X_2 = R_8(X_1)O_1 : \underline{\hspace{10em}}$$

$$O_2 : \underline{\hspace{10em}} \quad C_2 : \underline{\hspace{10em}} \quad X_3 : \underline{\hspace{10em}}$$

$$O_3 : \underline{\hspace{10em}} \quad C_3 : \underline{\hspace{10em}} \quad X_4 : \underline{\hspace{10em}}$$

$$O_4 : \underline{\hspace{10em}} \quad C_4 : \underline{\hspace{10em}}$$

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

$$X_1 : \underline{\hspace{10em}} \quad O_1 = L_8(E_K(X_1)) : \underline{\hspace{10em}}$$

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

$$X_2 : \underline{\hspace{10em}} \quad O_2 : \underline{\hspace{10em}} \quad C_2 : \underline{\hspace{10em}}$$

$$X_3 : \underline{\hspace{10em}} \quad O_3 : \underline{\hspace{10em}} \quad C_3 : \underline{\hspace{10em}}$$

$$X_4 : \underline{\hspace{10em}} \quad O_4 : \underline{\hspace{10em}} \quad C_4 : \underline{\hspace{10em}}$$