

**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

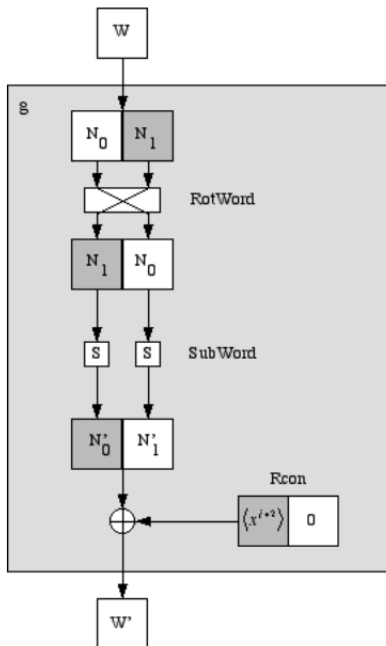
1. Using S-AES encrypt  $P_1 = 1101110011110111$  using the key  $K = 1110111010110011$ .

**Determine the RoundKeys:** Start with  $K_0 = 111011101110001$

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



**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*,

$$\begin{bmatrix} \text{---} & \text{---} \\ \text{---} & \text{---} \end{bmatrix}$$

Then shift the entries in the bottom row.

Resulting Matrix:  $\begin{bmatrix} \text{---} & \text{---} \\ \text{---} & \text{---} \end{bmatrix}$

**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  $D = E^{-1}$ .