

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 $P_1 = 0011000011110101$ using the key $K = 0100110001110000$.

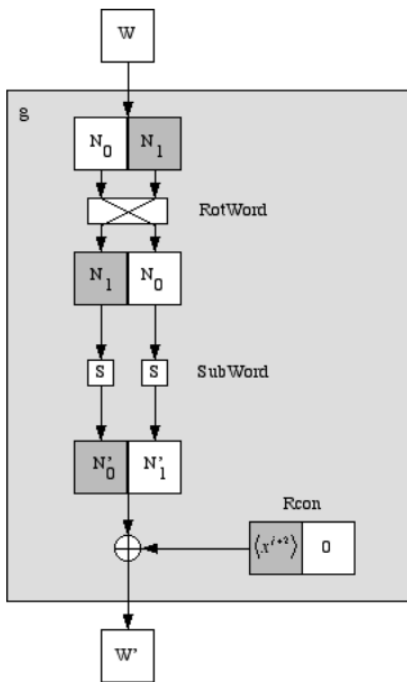
Determine the RoundKeys:

$K_0 = 0100110001110000$

Break into two pieces: $W_0 = \underline{01001100}$ $W_1 = \underline{01110000}$

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

Show your work here:



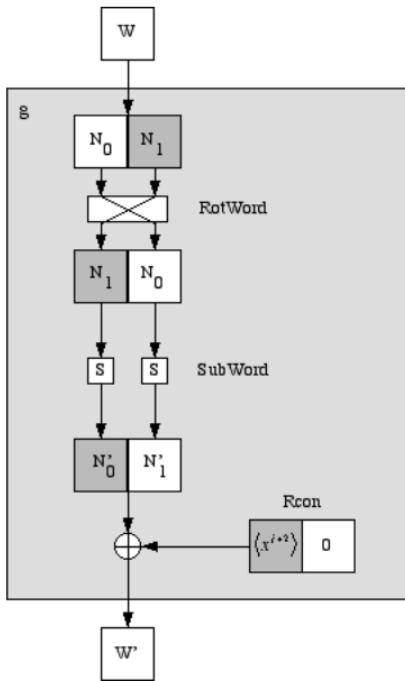
$g(W_1) : \underline{00010101}$

$W_2 = W_0 \oplus g(W_1) : \underline{01011001}$ $W_3 = W_1 \oplus W_2 : \underline{00101001}$.

$K_1 = W_2W_3 : \underline{0101100100101001}$.

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

Show your work here:



$g(W_3) : \underline{00011010}$

$W_4 = W_2 \oplus g(W_3) : \underline{01000011}$ $W_5 = W_3 \oplus W_4 : \underline{01101010}$.

$K_2 = W_4W_5 : \underline{0100001101101010}$.

Round 0: Add Round Key: $P_1 \oplus K_0 : \underline{0111110010000101}$.

Round 1: Substitution: 0101 1100 0110 0001.

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

$$\begin{bmatrix} \underline{0101} & \underline{0110} \\ \underline{1100} & \underline{0001} \end{bmatrix}$$

Then shift the entries in the bottom row.

$$\begin{bmatrix} \underline{0101} & \underline{0110} \\ \underline{0001} & \underline{1100} \end{bmatrix}$$

Round 1: Mix Columns:

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

$$\begin{aligned} ME &= \begin{bmatrix} \underline{x^2 + 1} & \underline{x^2 + x} \\ \underline{1} & \underline{x^3 + x^2} \end{bmatrix} \begin{bmatrix} \underline{1} & \underline{x^2} \\ \underline{x^2} & \underline{1} \end{bmatrix} = \begin{bmatrix} \underline{x^4 + x^3 + x^2 + 1} & \underline{x^4 + x} \\ \underline{x^5 + x^4 + 1} & \underline{x^3} \end{bmatrix} \\ &\equiv \begin{bmatrix} \underline{x^3 + x^2 + x} & \underline{1} \\ \underline{x^2} & \underline{x^3} \end{bmatrix} \pmod{x^4 + x + 1}. \end{aligned}$$

Round 1: Add Round Key:

Rewrite as string C_1 : 1110010000011000

Compute $C_1 \oplus K_1$: 1011110100110001

Round 2: Substitution: 0011 1110 1011 0100.

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

$$\begin{bmatrix} \underline{0011} & \underline{1011} \\ \underline{1110} & \underline{0100} \end{bmatrix}$$

Then shift the entries in the bottom row.

$$\begin{bmatrix} \underline{0011} & \underline{1011} \\ \underline{0100} & \underline{1110} \end{bmatrix}$$

Round 2: Add Round Key:

Rewrite as string C_2 : 0011010010111110

Compute $C_2 \oplus K_2$: 0111011111010100

Final Cipher Text: $C =$ 0111011111010100

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):

$C_1 = E_K(P_1)$:0111011111010100

$C_2 = E_K(P_2)$:1101101110110010

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

$C_1 = E_K(P_1 \oplus C_0)$:0111011111010100

$C_2 = E_K(P_2 \oplus C_1)$:1011001100111001

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 $X_1 = 0000000000000000$.)

$$O_1 = L_8(E_K(X_1)) : \underline{00110110} \quad C_1 = P_1 \oplus O_1 : \underline{00000110}$$

$$X_2 = R_8(X_1)C_1 : \underline{0000000000000110}$$

$$O_2 : \underline{00111000} \quad C_2 : \underline{11001101} \quad X_3 : \underline{0000011011001101}$$

$$O_3 : \underline{10011110} \quad C_3 : \underline{00101001} \quad X_4 : \underline{1100110100101001}$$

$$O_4 : \underline{00010010} \quad C_4 : \underline{01101001}$$

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

$$O_1 = L_8(E_K(X_1)) : \underline{00110110} \quad C_1 = P_1 \oplus O_1 : \underline{00000110}$$

$$X_2 = R_8(X_1)O_1 : \underline{0000000000110110}$$

$$O_2 : \underline{01101000} \quad C_2 : \underline{10011101} \quad X_3 : \underline{0011011001101000}$$

$$O_3 : \underline{11111001} \quad C_3 : \underline{01001110} \quad X_4 : \underline{0110100011111001}$$

$$O_4 : \underline{10011111} \quad C_4 : \underline{11100100}$$

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

$$X_1 : \underline{0000000000000001} \quad O_1 = L_8(E_K(X_1)) : \underline{00111011}$$

$$C_1 = P_1 \oplus O_1 : \underline{00001011}$$

$$X_2 : \underline{0000000000000010} \quad O_2 : \underline{00110000} \quad C_2 : \underline{11000101}$$

$$X_3 : \underline{0000000000000011} \quad O_3 : \underline{00110100} \quad C_3 : \underline{10000011}$$

$$X_4 : \underline{0000000000000100} \quad O_4 : \underline{00111110} \quad C_4 : \underline{01000101}$$