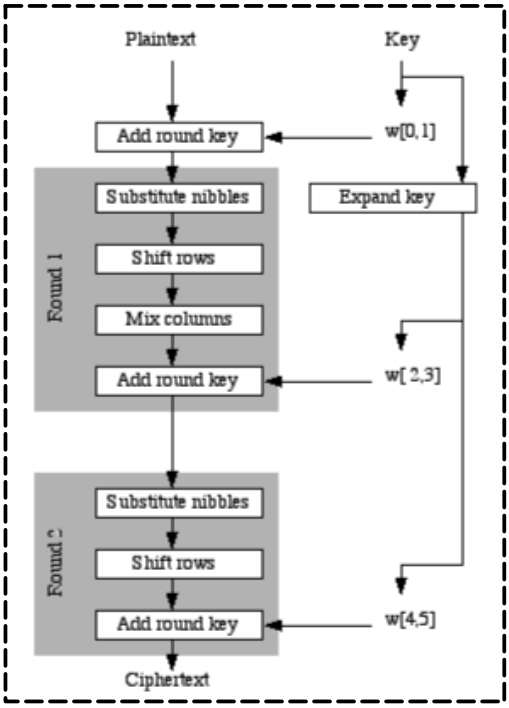
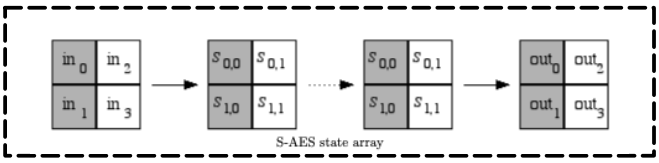
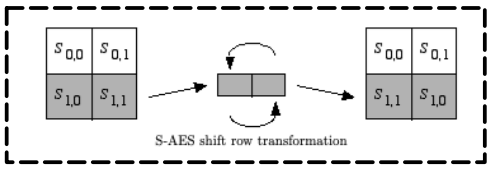
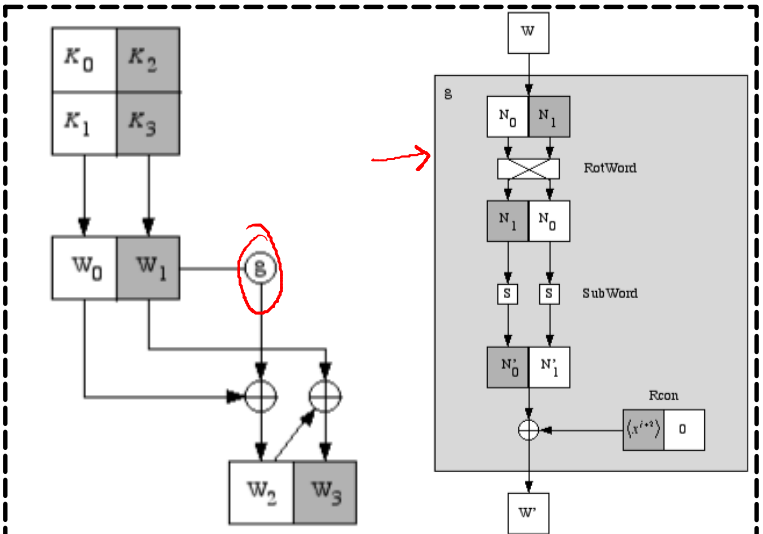


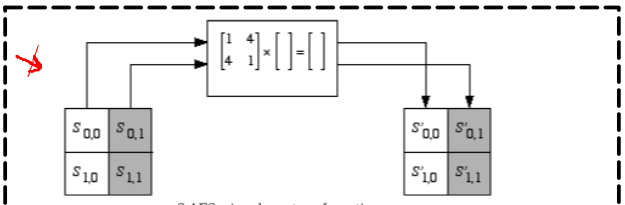


nibble	S-box(nibble)	nibble	S-box(nibble)
0000	1001	1000	0110
0001	0100	1001	0010
0010	1010	1010	0000
0011	1011	1011	0011
0100	1101	1100	1100
0101	0001	1101	1110
0110	1000	1110	1111
0111	0101	1111	0111





The g function is shown in the next diagram. It is very similar to AES, first rotating the nibbles and then putting them through the S-boxes. The main difference is that the round constant is produced using x^{j+2}, where j is the number of the round of expansion. That is, the first time you expand the key you use a round constant of $x^3 = 1000$ for the first nibble and 0000 for the second nibble. The second time you use $x^4 = 0011$ for the first nibble and 0000 for the second nibble.



These operations **are** done in GF(16), so remember that the 1 corresponds to the polynomial 1 and the 4 corresponds to the polynomial x^2. Thus this matrix could also be written as

$$\begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix}.$$

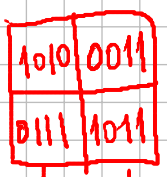
Don't forget to reduce modulo $x^4 + x + 1$.

Exercise: Use the key 1010 0111 0011 1011 to encrypt the plaintext "ok" as expressed in ASCII, that is 0110 1111 0110 1011. The designers of S-AES got the ciphertext 0000 0111 0011 1000. Do You?

P

C

Key Expansion



w_0 w_1

$w_2 = g(w_1) \oplus w_0$

$w_3 = w_2 \oplus w_1$

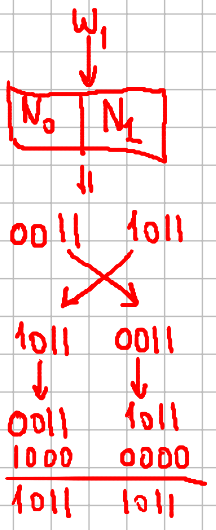
$w_4 = g(w_3) \oplus w_2$

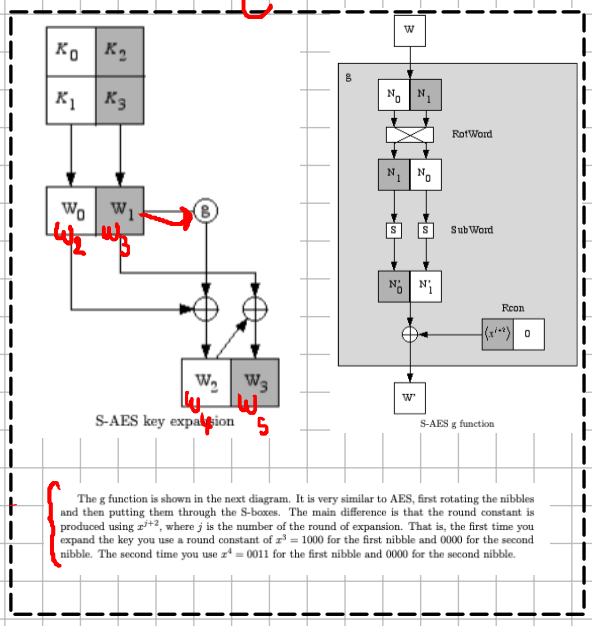
$w_5 = w_4 \oplus w_3$

$w_0 = 1010\ 0111$

$w_1 = 0011\ 1011$

$g(w_1) = ?$





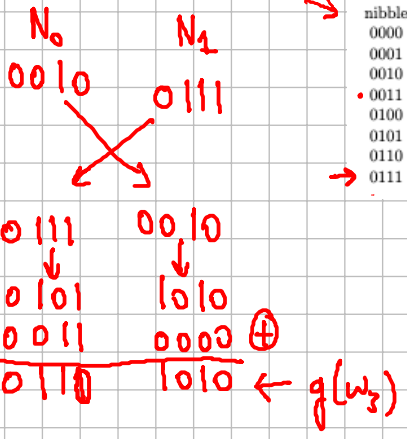
The g function is shown in the next diagram. It is very similar to AES, first rotating the nibbles and then putting them through the S-boxes. The main difference is that the round constant is produced using x^{j+2}, where j is the number of the round of expansion. That is, the first time you expand the key you use a round constant of $x^3 = 1000$ for the first nibble and 0000 for the second nibble. The second time you use $x^4 = 0011$ for the first nibble and 0000 for the second nibble.

w_2: 1011 1011 ⊕ 1010 0111 = 0001 1100 ← w_2

$w_3 = w_2 \oplus w_1$: 0001 1100 ⊕ 0011 1011 = 0010 0111 ← w_3

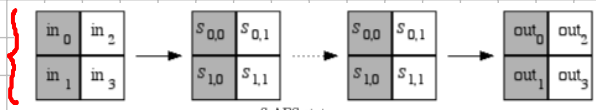
w_4: 0110 1010 ⊕ 0001 1100 = 0111 0110 ← w_4

w_5: 0111 0110 ⊕ 0010 0111 = 0101 0001

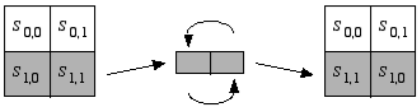


nibble	S-box(nibble)	nibble	S-box(nibble)
0000	1001	1000	0110
0001	0100	1001	0010
0010	1010	1010	0000
0011	1011	1011	0011
0100	1101	1100	1100
0101	0001	1101	1110
0110	1000	1110	1111
0111	0101	1111	0111

W0 = 1010 0111
W1 = 0011 1011
W2 = 0001 1100
W3 = 0010 0111
W4 = 0111 0110
W5 = 0101 0001

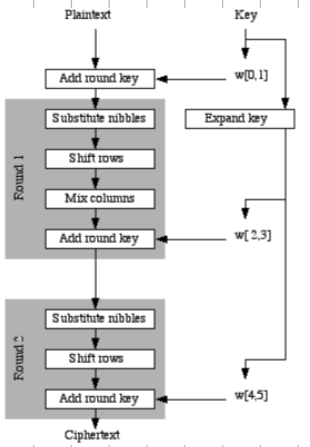


S-AES state array

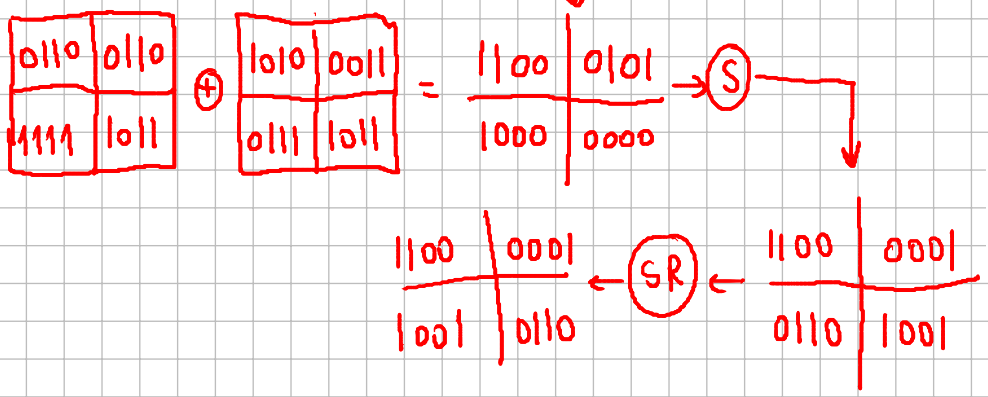


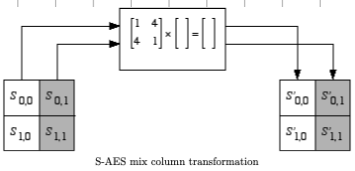
S-AES shift row transformation

nibble	S-box(nibble)	nibble	S-box(nibble)
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



pT= 0110 1111 0110 1011





S-AES mix column transformation

These operations are done in GF(16), so remember that the 1 corresponds to the polynomial 1 and the 4 corresponds to the polynomial x^2. Thus this matrix could also be written as

$$\begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix}.$$

Don't forget to reduce modulo $x^4 + x + 1$.

$$\begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix} \begin{bmatrix} x^3+x^2 & 1 \\ x^3+1 & x^2+x \end{bmatrix} = \begin{bmatrix} x^3+x^2+x^5+x^2 & 1+x^4+x^3 \\ x^5+x^4+x^3+1 & x^2+x^2+x \end{bmatrix}$$

$$= \begin{bmatrix} x^5+x^3 & x^4+x^3+1 \\ x^5+x^4+x^3+1 & x \end{bmatrix}$$

$$= \begin{bmatrix} x^3+x^2+x & x^3+x \\ x^3+x^2 & x \end{bmatrix}$$

$$= \begin{bmatrix} 1110 & 1010 \\ 1100 & 0010 \end{bmatrix}$$

$$\oplus \begin{bmatrix} 0001 & 0010 \\ 1100 & 0111 \end{bmatrix} = \begin{bmatrix} 1111 & 1000 \\ 0000 & 0101 \end{bmatrix}$$

1111 | 1000
0000 | 0101

S

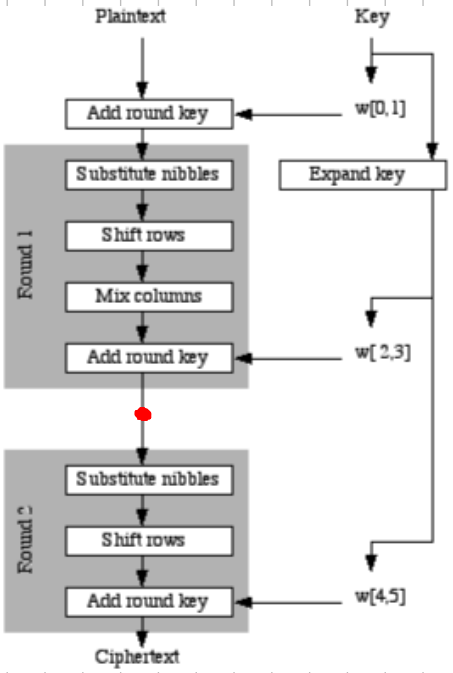
0111 | 0110
001 | 000

SR

0111 | 0110 ⊕
000 | 001

nibble	S-box(nibble)	nibble	S-box(nibble)
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

W0 = 1010 0111
W1 = 0011 1011
W2 = 0001 1100
W3 = 0010 0111
W4 = 0111 0110
W5 = 0101 0001



0111 | 0101
0110 | 0001 = 0000 | 0011
0111 | 1000

0000 0111 0011 1000 ✓