

Simplified AES

16-bit block

16-bit key

4 x 4 S-box

Field \mathbb{F}_{16}

Modulus $X^4 + X + 1$

2 rounds

SPN

Musa, A., Schaefer, E., and Wedig, S. 2010. "A Simplified AES Algorithm and Its Linear and Differential Cryptanalysis." *Cryptologia* 27(12), 148 – 177.

S-box

Input nibble	Output nibble
0000	1001
0001	0100
0010	1010
0011	1011
0100	1101
0101	0001
0110	1000
0111	0101
1000	0110
1001	0010
1010	0000
1011	0011
1100	1100
1101	1110
1110	1111
1111	0111

Construction of S-box

Input nibble

$$0101 \quad X^2 + 1$$

Construct inverse of 0101 modulo $X^4 + X + 1$

$$1011 \quad Y^3 + Y + 1$$

Affine transformation

$$(Y^3 + Y^2 + 1)(Y^3 + Y + 1) + (Y^3 + 1) \bmod (Y^4 + 1) = 1$$

Output nibble

$$0001$$

16-bit block (4 nibbles) $N_0N_1N_2N_3$

$$\begin{bmatrix} N_0 & N_2 \\ N_1 & N_3 \end{bmatrix}$$

Encryption operations

Nibble Substitution NS

$$\begin{bmatrix} S(N_0) & S(N_2) \\ S(N_1) & S(N_3) \end{bmatrix}$$

Shift Row SR

$$\begin{bmatrix} N_0 & N_2 \\ N_3 & N_1 \end{bmatrix}$$

Mix Columns MC

$$\begin{bmatrix} b_0b_1b_2b_3 & c_0c_1c_2c_3 \\ b_4b_5b_6b_7 & c_4c_5c_6c_7 \end{bmatrix} \text{ becomes}$$

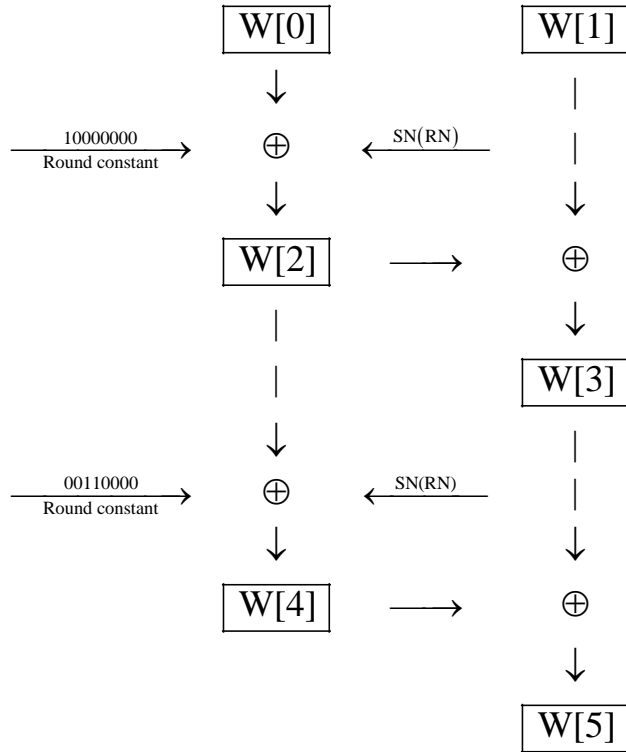
$$\begin{bmatrix} b_0 \oplus b_6 & b_1 \oplus b_4 \oplus b_7 & b_2 \oplus b_4 \oplus b_5 & b_3 \oplus b_5 & c_0 \oplus c_6 & c_1 \oplus c_4 \oplus c_7 & c_2 \oplus c_4 \oplus c_5 & c_3 \oplus c_5 \\ b_7 \oplus b_4 & b_0 \oplus b_3 \oplus b_5 & b_0 \oplus b_1 \oplus b_6 & b_1 \oplus b_7 & c_7 \oplus c_4 & c_0 \oplus c_3 \oplus c_5 & c_0 \oplus c_1 \oplus c_6 & c_1 \oplus c_7 \end{bmatrix}$$

The transformation is

$$\begin{bmatrix} N_0 & N_2 \\ N_1 & N_3 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix} \begin{bmatrix} N_0 & N_2 \\ N_1 & N_3 \end{bmatrix} \text{ mod}(x^4 + x + 1)$$

Key Schedule

16 bits of user-supplied key $\underbrace{k_0k_1k_2k_3 \quad k_4k_5k_6k_7}_{W[0]} \quad \underbrace{k_8k_9k_{10}k_{11} \quad k_{12}k_{13}k_{14}k_{15}}_{W[1]}$



$$K_0 = W[0] W[1]$$

$$K_1 = W[2] W[3]$$

$$K_2 = W[4] W[5]$$

Key Schedule

16 bits of user-supplied key $\underbrace{1010\ 0111}_{w[0]}\ \underbrace{0011\ 1011}_{w[1]}$

$$\begin{array}{rcl}
 W[0] & = & 1010\quad 0111 \\
 W[1] & = & 0011\quad 1011 \\
 RN & & \times \\
 & & 1011\quad 0011 \\
 SN & & \downarrow\quad \downarrow \\
 & & 0011\quad 1011 \\
 & & \oplus \\
 \text{Round constant} & & \underline{1000}\quad \underline{0000} \\
 & & 1011\quad 1011 \\
 & & \oplus \\
 W[0] & & \underline{1010}\quad \underline{0111} \\
 W[2] & = & 0001\quad 1100 \\
 & & \oplus \\
 W[1] & & \underline{0011}\quad \underline{1011} \\
 W[3] & = & 0010\quad 0111
 \end{array}$$

$$\begin{array}{rcl}
W[3] & = & 0010 \quad 0111 \\
RN & & \quad \quad \times \\
& & 0111 \quad 0010 \\
SN & & \downarrow \quad \downarrow \\
& & 0101 \quad 1010 \\
& & \quad \quad \oplus \\
\text{Round constant} & & \underline{0011} \quad \underline{0000} \\
& & 0110 \quad 1010 \\
& & \quad \quad \oplus \\
W[2] & & \underline{0001} \quad \underline{1100} \\
W[4] & = & 0111 \quad 0110 \\
& & \quad \quad \oplus \\
W[3] & & \underline{0010} \quad \underline{0111} \\
W[5] & = & 0101 \quad 0001
\end{array}$$

$$\begin{array}{l}
K_0 = 1010 \ 0111 \ 0011 \ 1011 \\
K_1 = 0001 \ 1100 \ 0010 \ 0111 \\
K_2 = 0111 \ 0110 \ 0101 \ 0001
\end{array}$$

Encipher

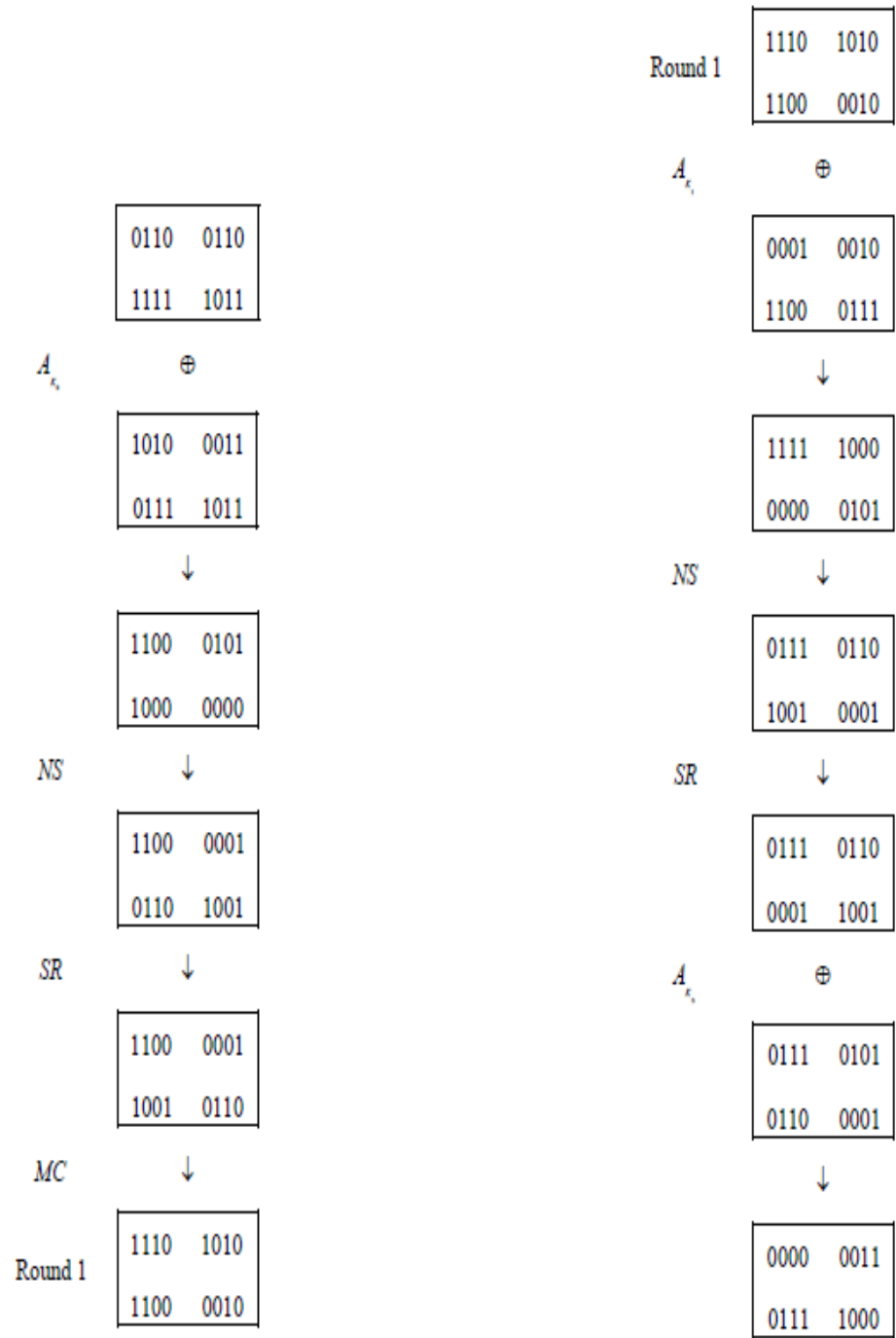


plaintext ok

o k

0110 1111 0110 1011

N_0 N_1 N_2 N_3



CIPHERTEXT 0000 0111 0011 1000