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 X^2+1

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

1011 Y^3+Y+1

Affine transformation

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

Output nibble

0001

16-bit block (4 nibbles) $N_0 N_1 N_2 N_3$

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

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

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

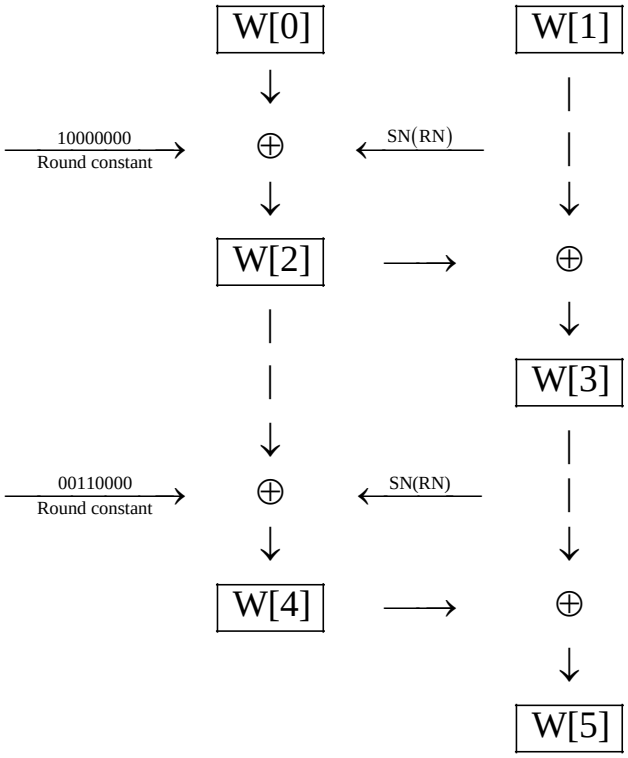
$$\begin{bmatrix} b_0 \oplus b_6 & b_1 \oplus b_4 \oplus b_7 & b_2 \oplus b_4 \oplus b_5 & b_3 \oplus b_5 & c_0 \oplus c_6 & c_1 \oplus c_4 \oplus c_7 & c_2 \oplus c_4 \oplus c_5 & c_3 \oplus c_5 \\ b_2 \oplus b_4 & b_0 \oplus b_3 \oplus b_5 & b_0 \oplus b_1 \oplus b_6 & b_1 \oplus b_7 & c_2 \oplus c_4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

The transformation is

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

Key Schedule

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



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 $\underbrace{1010\quad 0111}_{W[0]}\quad \underbrace{0011\quad 1011}_{W[1]}$

W[0]	=	1010		0111
W[1]	=	0011		1011
RN			╳	
		1011		0011
SN		↓		↓
		0011		1011
			⊕	
Round constant		1000		0000
		1011		1011
			⊕	
W[0]		1010		0111
W[2]	=	0001		1100
			⊕	
W[1]		0011		1011
W[3]	=	0010		0111

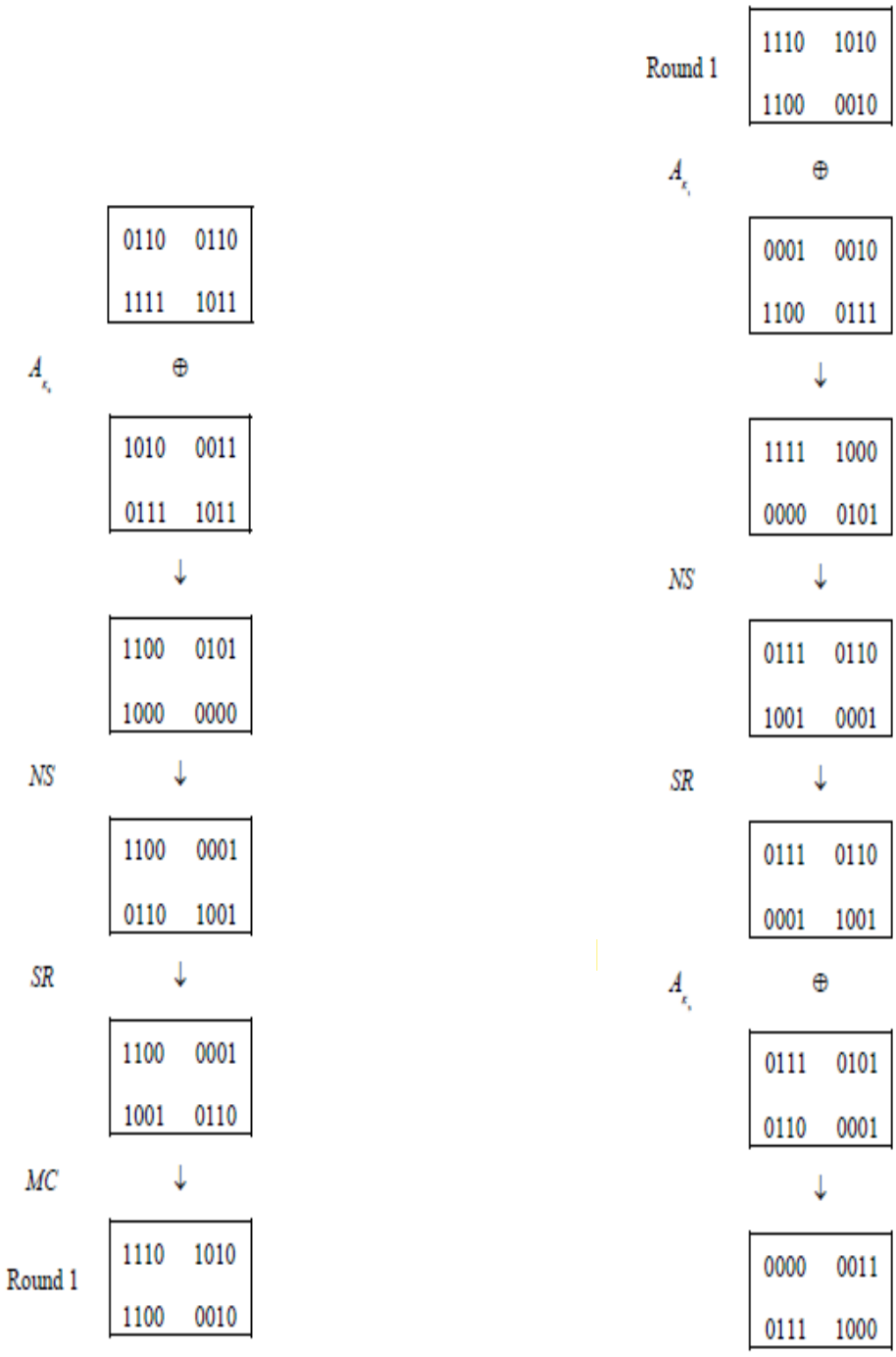
W[3]	=	0010	0111
RN			╳
		0111	0010
SN		↓	↓
		0101	1010
			⊕
Round constant		0011	0000
		0110	1010
			⊕
W[2]		0001	1100
W[4]	=	0111	0110
			⊕
W[3]		0010	0111
W[5]	=	0101	0001

K_0 = 1010 0111 0011 1011
K_1 = 0001 1100 0010 0111
K_2 = 0111 0110 0101 0001

Encipher

plaintext ok

o		k	
0110	1111	0110	1011
N_0	N_1	N_2	N_3



CIPHERTEXT 0000 0111 0011 1000