

# MATH 314 Fall 2019 - Class Notes

4/6/2020

Scribe: Daniella Diaz

Summary: In class we learned about SAES.

Notes:

Table 1: SAES Sbox

	<b>00</b>	<b>01</b>	<b>10</b>	<b>11</b>
00	1001	0100	1010	1011
01	1101	0001	1000	0101
10	0110	0010	0000	0011
11	1100	1110	1111	0111

Process to get Round Keys is AES (SAES). It is slightly more complicated. Round Keys are generated by a process called Key Expansion.

Key Expansion:

Master Key (16 bits)

0th Round Key ( $K_0$ )

**1st Step:** Break 16 bit master key into two 8 bits.

$$(K_0) = (W_0)(W_1)$$

Now, we have to create more words using rules:

$$(W_2) = g(W_1) \oplus (W_0)$$

$$(W_3) = W_2 \oplus W_1$$

$$(W_4) = g(W_3) \oplus (W_2)$$

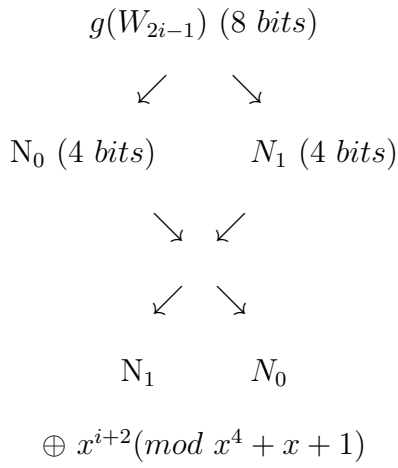
$$(W_5) = W_4 \oplus W_3$$

Remember:

$$(W_{2i}) = g(W_{2i-1}) \oplus (W_{2i-2})$$

$$(W_{2i+1}) = W_{2i} \oplus W_{2i-1}$$

**2nd Step:** Use g-function.



**Note:** if  $i = 1$ ,  $x^3 \rightarrow 1000$   
 if  $i = 2$ ,  $x^4 = x + 1(\text{mod } x^4 + x + 1) \rightarrow 0011$

Concatenate to get output!

## 4 Steps of SAES:

1. **Add Roundkey Step (ARK):**

-XOR with roundkey

2. **Substitute:**

-Break into four 4 bits. Replace each nibble with Sbox entry.

3. **Shift Rows:**

-Write nibbles in a 2x2 matrix filling columns first.

$N_0N_1N_2N_3 \leftarrow 16bits$

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

1st Column- shift 0 times

2nd Column- shift 1 time

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

4. **Mix Columns:**

-Treat matrix entries in  $\mathbb{F}_{16} \text{ (mod } x^4 + x + 1)$  and write this matrix as M.

Then take this encryption matrix:  $E = \begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix}$

Compute  $E * M$ .

Then take the result and write it out as a string of bits (working columns first).

**Example:** SAES Example

**Master Key:** W= 0100 1010 1111 0101

**Plaintext:** P= 0100 1010 1111 0101

**Key Expansion:** Break Masterkey into two equal parts ( $W_0$  and  $W_1$ ).

$W_0 = 0100\ 1010$

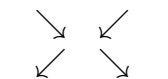
$W_1 = 1111\ 0101$

$W_2 = g(W_1) \oplus W_0$

\* Find  $g(W_1)$  using  $g$  - function

$g(W_1) \rightarrow (i = 1)$

1111 0101



0101 1111

Sbox Sbox

0001 0111

\* Now XOR \*

0001 (from  $N_1$ )

$\oplus$  1000 (from  $x^3$ )

-----

1001

$g(W_1) = 1001\ 0111$

Note: 1001 (from XOR) and 0111 (from  $N_0$ )

$W_2 = g(W_1) \oplus W_0$

10010111

$\oplus$  01001010

-----

11011101 =  $W_2$

$W_3 = W_2 \oplus W_1$

11011101

$\oplus$  11110101

-----

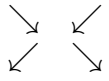
00101000 =  $W_3$

$W_4 = g(W_3) \oplus W_2$

\* Find  $g(W_3)$  using  $g$  - function

$g(W_3) \rightarrow (i = 2)$

0010 1000



1000 0010

*Sbox Sbox*



0110 1010

*\* Now XOR \**

0110 (*from N<sub>1</sub>*)

$\oplus$  0011 (*from x<sup>4</sup>*)

-----

0101

$g(W_3) = 0101\ 1010$

Note: 0101 (from XOR) and 1010 (from  $N_0$ )

01011010

$\oplus$  11011101

-----

10000111 =  $W_4$

$W_5 = W_4 \oplus W_3$

10000111

$\oplus$  00101000

-----

10101111 =  $W_5$

---

$K_0 = (W_0)$  combined with  $(W_1)$

0100 1010 1111 0101

$K_1 = (W_2)$  combined with  $(W_3)$

1101 1101 0010 1000

$K_2 = (W_4)$  combined with  $(W_5)$

1000 0111 1010 1111

$$\begin{aligned} 1000\ 0111\ 0011\ 1011 &= P \\ \oplus 0100\ 1010\ 1111\ 0101 &= K_0 \end{aligned}$$

---


$$1100\ 1101\ 1100\ 1110$$

**Round 1:** Substitute  $\rightarrow$  *Sbox*

$$1100\ 1110\ 1100\ 1111$$

\*Shift Rows:

$$\begin{bmatrix} 1100 & 1100 \\ 1110 & 1111 \end{bmatrix} \rightarrow \begin{bmatrix} 1100 & 1100 \\ 1111 & 1110 \end{bmatrix}$$

\*Convert to  $\mathbb{F}_{16}$ :

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

\*Mix Columns:  $(E * M)$

*a* row  $\rightarrow$

*b* row  $\rightarrow$   $\begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix} = E$

*c* column  $\downarrow$   $x^3 + x^2$

*d* column  $\downarrow$   $x^3 + x^2$

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

$$\begin{bmatrix} ac & ad \\ bc & bd \end{bmatrix} = \text{formula}$$

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

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

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

$$\begin{bmatrix} x^2 + 1 & 1 \\ x^3 + x & x^3 + x + 1 \end{bmatrix} (\text{mod } x^4 + x + 1) = 0101\ 1010\ 0001\ 1011$$

$$\begin{array}{l}
 0101\ 1010\ 0001\ 1011 = \text{Round 1} \\
 \oplus 1101\ 1101\ 0010\ 1000 = K_1
 \end{array}$$

---


$$1000\ 0111\ 0011\ 0011$$

**Round 2:** Substitute  $\rightarrow$  *Sbox*

$$0110\ 0101\ 1011\ 1011$$

\* *ShiftRows* :

$$\begin{bmatrix} 0110 & 1011 \\ 0101 & 1011 \end{bmatrix} \rightarrow \begin{bmatrix} 0110 & 1011 \\ 1011 & 0101 \end{bmatrix}$$

$$\begin{array}{l}
 0110\ 1011\ 1011\ 0101 = \text{Shifted Rows from Round 2} \\
 \oplus 1000\ 0111\ 1010\ 1111 = K_2
 \end{array}$$

---


$$1110\ 1100\ 0001\ 1010$$

$\uparrow$   
*Final Ciphertext*