MATH 314 Spring 2018 - Class Notes

10/29/2018

Scribe: Devon Emanuel

Summary : SAES Example, AES Recap, and Public Key Cryptography Introduction.

Notes: Include detailed notes from the lecture or class activities. Format your notes nicely using latex such as

SAES

SAES SBOX

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

Example:

Master Key: 0100 1010 1111 0101
Encrypt Plaintext: 1101 0111 0010 1000

Key Expansion (Determine Roundkeys)
$W_0 = 01001010$
$W_1 = 11110101$
$W_2 = W_0 \oplus g(W_i)$
$g(W_i)$

1101 1101 (swap)
1101 1101
Sbox 0001 0111

$x^{i+2}\ mod(x^4 + x + 1)$
$X^3 = 1000$
$0001 \oplus 1000 = 1001$

1001 0111

$W_2 = 01001010 \oplus 11010111 = 11011101$
$W_3 = W_2 \oplus W_1 = 11011101 \oplus 11110101 = 00101000$
$W_4 = W_2 \oplus g(W_3) = 11011101 \oplus 11110101 = 00101000$
$g(W_3)$

0010 1000 (swap)
1000 0010
Sbox 0110 1010

$x^{i+2} mod(x^4 + x + 1)$
$x^4 = 0011$
$0110 \oplus 0011$

0101 1010

$W_5 = W_3 \oplus W_4 = 00101000 \oplus 10000111 = 10101111$

$RK1$ =W_2 + W_3 =1101 1101 0010 1000
RK2 = W_4 + W_5 =1000 0111 1010 1111
Plaintext = 1101 0111 0010 1000

SAES
Plaintext

ARK_0

Substitute
Shift Rows
Mix Columns
ARK_1

Substitute
Shift Rows
ARK_2

1101 0111 0010 1000 (Plaintext) $\oplus$ 0100 1010 1111 0101 ($AR\mathrm{K}_0$) = 1001 1101 1101 1101
(Substitute Test Box) - 0010 1110 1110 1110

$$\left|\begin{array}{cc} 0010 & 1110 \\ 1110 & 1110 \end{array}\right|$$

Shift Rows / Swap the bottom two values (By coincidence, they are the same)

$$\left|\begin{array}{cc} 0010 & 1110 \\ 1110 & 1110 \end{array}\right|$$

M=$\left|\begin{array}{cc} \mathrm{x} & \mathrm{x}^3 + x^2 + x \\ \mathrm{x}^3 + x^2 + x & \mathrm{x}^3 + x^2 + x \end{array}\right|$

$$\text{E}=\begin{vmatrix} 1 & \text{x}^2 \\ x^2 & 1 \end{vmatrix}$$

$$\begin{vmatrix} 1 & \text{x}^2 \\ x^2 & 1 \end{vmatrix} \begin{vmatrix} \text{x} & \text{x}^3+x^2+x \\ \text{x}^3+x^2+x & \text{x}^3+x^2+x \end{vmatrix}$$

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

$$\text{x}^4+x+1 \overline{\left| \begin{array}{r} \text{x+1} \\ \text{x}^5+x^4+x^3+x \end{array} \right.} \text{ Remainder } = \text{x}^3+x^2+x+1$$

$$\text{x}^4+x+1 \overline{\left| \begin{array}{r} \text{x+1} \\ \text{x}^5+x^4+x^2+x \end{array} \right.} \text{ Remainder } = \text{x}+1$$

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

1111 0110 0011 0011 $\oplus$ RK1: 1101 1101 0010 1000 = 0010 1011 0001 1011
Output Round 1 = 0010 1011 0001 1011
Substitute Sbox: 1010 0011 0100 0011

$$\begin{vmatrix} 1010 & 0100 \\ 0011 & 0011 \end{vmatrix}$$ Shift Rows (Again, they happen to be the same)

1010 0011 0100 0011 $\oplus$ RK2: 1000 0111 1010 1111
Ciphertext: 0010 0100 1110 1100

AES

- Symmetric key algorithm - Both sides agree on a key
- 10 rounds
- 128 bit plaintexts
- 128, 196, 256 - bit keys
- Arithmetic happens over F_{256}
- Considered to be secure against any current attacks

Problem: How do we transmit the master key?

Public Key Cryptography

- First developed in the 1970's
- Idea: Alice can produce a "public key" that she can tell anybody
- Anybody can use this public key to send Alice a message
- Alice also has a "private key" that is required to decrypt these messages
- Key ingredient in any public key system is a hard math problem to get from public key to private one