MATH 314 - Class Notes

10/25/2016

Scribe: Lougrant Fernandez

Summary: Today in class we covered the Advanced Encryption Standard(AES).

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

- bullets

1. lists

or **other** formatting *commands.* Make sure to write $e^{qu}a + i \circ \mathbb{N}s$ in math mode.

Examples: If including plaintext or ciphertext or other data it is often helpful to write them using `typewriter text`.

AES is the current standard for encryption.

Simplified AES

- Key: 16 bits
- Block Size: 16 bits
- 2 rounds

Plain Text $\rightarrow$ Add Round Key $\rightarrow$ Round 1 $\rightarrow$ Round 2

Round 1
Substitution $\rightarrow$ Shift Rows $\rightarrow$ Mix Columns $\rightarrow$ Add Round Key

Round 2
Repeat round 1 but skip mix columns.

Unlike DES, AES is not a Feistel Cipher.
Benefit: Bits get diffused much faster.

S-Box: SAES

- Take in 4 bits
- Output 4 bits

Values come from a simple rule.

Take the input $b_0b_1b_2b_3s$
and write as polynomial
$\mathrm{b}_0x^3 + b_1x^2 + b_2x + b_3$

Treat this as an element of $\mathrm{F}_(2^4)$

In $\mathbb{F}_{16} = \mathbb{F}_{2^4}$
we work modulo the irreducible polynomial: $\mathrm{x}^4 + x + 1$

Compute: $(\mathrm{b}_0x^3 + b_1x^2 + b_2x + b_3)^-1$
$= C_0x^3 + C_1x^2 + C_2x + C_3$

$$\begin{pmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

output of S Boxes

<u>Ex:</u> Compute output of S-Box for 1001

Write as polynomial
$\mathrm{x}^3 + 1$

Find Inverse (Euclidean Algorithm)
x

Compute

$$MC = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} output from S - Box$$

<u>S-Box for SAES</u>

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

<u>Key Expansion</u>
Get roundkeys from master key K

Break K into two pieces(W_0, W_1)

$\mathrm{W}_2 = g(W_1) \oplus W_0$
$W_3 = W_2 \oplus W_1$
$W_4 = g(W_1) \oplus W_2$

$W_5 = W_4 \oplus W_3$

Round Keys

$\text{K}_0 = W_0 W_1$
$K_1 = W_2 W_3$
$K_2 = W_4 W_5$

g

Split W into N_0 and N_1
Swap N_0 and N_1
Run through S-Boxes
XOR new N_1 with the polynomial x^{i+2} mod $x^4 + x + 1$
Append new N_0 to the output of the previous step to get final result

In g, i is the round that the word is being computed for

Arrange our bits into a 2x2 matrix 4 bits each
$\begin{pmatrix} In_0 & In_1 \\ In_2 & In_3 \end{pmatrix}$

Substitution Step

Feed $In_0 In_1 In_2 In_3$ into the s-box and replace with the outputs

Get out: $\begin{pmatrix} S_{00} & S_{01} \\ S_{10} & S_{11} \end{pmatrix}$

Shift Rows

Take the elements of matrix in row i and rotate them i position left.
$\begin{pmatrix} S_{00} & S_{01} \\ S_{10} & S_{11} \end{pmatrix}$
In AES shifts to: $\begin{pmatrix} S_{00} & S_{01} \\ S_{11} & S_{10} \end{pmatrix}$

Mix Column

Treat entries of m as polynomials in $\mathbb{F}_{16}$
Multiply times the Matrix E.

$$E = \begin{pmatrix} 1 & X^2 \\ X^2 & 1 \end{pmatrix}$$

output of Mix Column is matrix ME. Treat entries as vector again.

Example: Use SAES to encrypt
P = 1101 0111 0010 1000
K = 0100 1010 1111 0101

$W_0 = 01001010$
$W_1 = 11110101$

$W_2 = g(W_1) \oplus W_0$

$g(W_1)$ = swap 1111 0101
get: 0101 1111
S-Box: 0001 0111
XOR 0001 with $x^3$1000
get : 10010111
W_2 = 1001 0111 $\oplus$01001010 = 11011101

$W_3 = W_2 \oplus W_1$
$= 11011101 \oplus 11110101 = 00101000$

$W_4 = g(W_3) \oplus W_2$
$= 01011010 \oplus 11011101 = 10000111$

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

We now have all of our round Keys!
$W_0 = 01001010$
$W_1 = 11110101$
$W_2 = 11011101$
$W_3 = 00101000$
$W_4 = 10000111$
$W_5 = 10101111$

P + K = output of initial add round key. Input this to round 1.
$1101011100101000 \oplus 010010101110101 = 1001110111011101$