MATH 314 - Class Notes

10/27/2015

Scribe: Jacob Larochelle

Summary: Finished the steps for sAES.

Notes: Picking up where we left off in the last class, we finish the remaining steps of sAES begining with round one.

Round One:

- Substitute from sbox

1001 1101 1101 1101 -becomes 0010 1110 1110 1110

- Shift Rows

turn the above binary into a matrix and shift row N by N positions

$\begin{pmatrix} 0010 & 1110 \\ 1110 & 1110 \end{pmatrix}$

stays the same due to repeated numbers

- Mix Columns in the field 16

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

and reduce mod x^4+x+1

$$= \begin{pmatrix} 1111 & 0110 \\ 0011 & 0011 \end{pmatrix}$$

- Add round key

1111 0110 0011 0011 xor 1101 1101 0010 1000 = 0010 1011 0001 1011

Round Two:

- Substitute from sbox

0010 1011 0001 1011 -becomes 1010 0011 0100 0011

- Shift Rows

turn the above binary into a matrix and shift row N by N positions

$\begin{pmatrix} 1010 & 0100 \\ 0011 & 0011 \end{pmatrix}$

stays the same due to repeated numbers

- Add round key

1010 0011 0100 0011 xor 1101 1101 0010 1000 = 0010 0100 1110 1100

0010 0100 1110 1100 is our final cipher text

Decryption:
We briefly addressed the decryption of AES and concluded that all the steps can be performed in reversed except mix column which is easily dealt with by the use of a decryption matrix that is the inverse of the encryption matrix.

AES Differences:

- 128 bit plaintext
- Versions with 128/192/256 bit keys
- Write 4x4 matrices with 8 bits in each position
- Work over a field 256 elements
- Modulo $x^8 + x^4 + x^3 + x + 1$
- Differential cryptanalysis is only effective against AES with 7 rounds, AES is extra safe using 10 rounds
- Fastest way to attack is brute force, 2^{256} possible keys

Symetric Encryption Methods:

- Fast
- Very secure, eve must figure out key
- Downside- both parties must communicate a key preemptively
- Solution- public key cryptography

Public key:

- 2 keys, public and secure
- knowing one key does not help in finding the second