MATH 314 Spring 2018 - Class Notes

4/9/2019

Scribe: Angela Gurfolino

Summary: Today we finished the second half of simplified AES starting with round 1 shift rows

Notes: Encrypt P = 1000 0111 0011 1011 with
$K_0 = 0100101011110101, K_1 = 1101110100101000, K_2 = 1000011110101111$

Round 1:

Shift Rows

$$M = \begin{bmatrix} 1101 & 1100 \\ 1111 & 1110 \end{bmatrix}$$

Mix Columns

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

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

The next step is to add Round Key 1. We do this by going down columns. First, we change the numbers in the matrix.
$x^2 + 1 = 0101$
$x^3 + x = 1010$
$1 = 0001$
$x^3 + x + 1 = 1011$

We then XOR these numbers with Round key 1.
$0101101000011011 \oplus 1101110100101000 = 1000011100111000$

This is the end of Round 1.

Round 2 skips the mix columns step. The last round of AES never uses mix columns and since we are using simplified AES, the second round is the last round.
Round 2:

Substitute
We substitute the previous rounds final key into the S-box.

1000 0111 0011 0011
Substitutes in the S-box to:
0110 0101 1011 1011

Now we shift rows:

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

The top row is shifted 0 times and the bottom row is shifted once.
We skip the mix columns step.
Now we XOR this matrix (by column) with round key 2.

$0110101110110101 \oplus 1000011110101111 = 1110110000011010$
Our final cipher text is 1110110000011010

SAES Encryption
↓
ARK0
↓
Substitute
↓
Shift rows
↓
Mix columns
↓
ARK1
↓
Substitution
Shift rows
↓
ARK2
↓
Cipher text

How do we decrypt this?
We work backwards from the encryption!

SAES Decryption
Cipher text
↓
ARK2
↓
Inverse shift rows
↓
Inverse substitution
↓
ARK1
↓
Inverse mix columns
↓
Reverse shift rows
↓
Inverse substitution
↓
ARK0
↓
Plain text

Public Key Cryptography
The idea was first presented in 1976 but no algorithm was known for it at the time.

Idea: Alice is going to have 2 different keys.
Encryption key: k_e
Decryption key: k_d

The encryption key can be used to encrypt a message, but not to decrypt it (without a lot of work).
In order to decrypt quickly, one needs the decryption key.
The decryption key is secret, the encryption key is public knowledge.

Mathematically this sort of encryption function is called a one way function.
It is easy to compute, difficult to reverse.
It is easy to reverse if you have extra knowledge called a trapdoor.

The first example of a public key cryptosystem was RSA. RSA stands for the initials of its inventors: Rivest, Shamir, and Adleman.Trapdoor: integer factorization.

If you have two big prime numbers pq, you can easily multiply them together.
Instead if you have a big number n and you need to find p and q with p*q=n, this is hard.
How do we use this to make a secure cryptosystem?

Alice picks p and q randomly.*This needs to be done in a way that nobody can predict her choice.* Both p and q are prime. She multiplies them to get n = pq. She also picks an exponent e. gcd(e,p-1) = gcd(e,q-1) = 1
In practice e = 65537 is often used.
Alice's public Encrption key: $\mathrm{k}_e(n, e)$
Bob wants to send Alice a message, m.
m is an integer ¡ n
Bob encrypts m using c = $\mathrm{m}^e (mod\, n)$
E(m) = $\mathrm{m}^e (mod\, n)$
Alice wants to decrypt c to find m.
c = $\mathrm{m}^e (mod\, n)$
She needs to undo raising something to the e power.
Basic principle: (Euler's theorem)
When working with mod n the exponents work mod $\varphi(n)$.
Alice needs d = $\mathrm{e}^{-1} (mod\, \varphi(n))$
Need to compute: $\varphi(n) = \varphi(pq) = (p-1)(q-1)$
The only way to compute $\varphi(n)$
is to know p and q but factoring n is supposed to be hard!
Alice computes d $\equiv e^{-1} \, mod\, \varphi(n)$
Her decryption key is d $\mathrm{k}_d = d$
Alice's Decrpytion function:
$\mathrm{D}_k(c) = c^d \, (mod\, n) \equiv (m^e)^d \equiv m^{1 \, mod\, \varphi(n)} \equiv m (mod\, n)$
Numbers with exactly two prime factors n = pq are called semiprimes. In practice, you want p $\sim 80\, ish\, digits$
and q $\sim 81 - 82\, ish\, digits.$
n $\sim 160\, digits.$