# MATH 314 - Class Notes

04/18/2017

Scribe: Brittany Galata

**Summary:** During class, we finished SAES and began looking at the difference between Symmetric Key Cryptosystems and Public Key Crytography. We then began RSA.

**Notes:**
Plaintext - ARK1 - Sub - SR - MC - ARK2 - Sub - SR - ARK3
ARK1 = Key0
ARK2 = Key1
ARK3 = Key2 and Ciphertext

Decrypt SAES
Receiver needs to know key
Perform key expansion

- To undo ARK just ARK again
- To undo SR shift backwards
- To undo Sub Step we use inverse S-box

Recall Mix Columns
Multiply on the right by encryption matrix
To undo Mix columns we want to multiply by the inverse matrix $D = E^{-1}$ (Decryption matrix)

Ciphertext - ARK2 - SR Backwards - Inverse Sub - ARK1 - Inverse MC - SR Backwards - Inverse Sub - ARK0
ARK2 = K2
ARK1 = K1
ARK0 = K0 and plaintext

AES
128 Bit Plaintext
128/192/256 bit keys
(Different Key Expansion)
Matrices we 4x4
work over F (one byte)
$(mod x^8 + x^4 + x^3 + x + 1)$
10 rounds
9 are Sub, SR, MC, ARK
last is Sub, SR, ARK
Faster to attack AES using brute force than differential cryptanalysis (7 rounds)
3 extra round to defend against future attacks

Symmetric Key Cryptosystem
Alice - Encrypt - Ciphertext - Decrypt - Bob
Alice and Bob have a shared secret key that is used for both encryption and decryption

Symmetric Key

1. AES
2. DES
3. Hill Cipher
4. Substitution Cipher, etc

Advantages
Very Fast
Very Secure if implanted right (large keys)

Disadvantages
No way to communicate with someone that doesn't already share a key with you
How do you send the first message?

Public Key Cryptography
Two different keys for encryption and decryption
Can't use encryption key to get decryption key
Alice can publish her encryption key public
Anyone can send her a message using encryption key
She keeps decryption key secret
She is the only one who can decrypt messages
Every public key system is based on a one-way function (trapdoor function)
Easy to do one way, really hard to undo

RSA
Trapdoor function: Multiplying integers (factoring integers)
Say p and q are two 100 digit prime numbers
Really easy to multiply them
Compute n=pq
Given n, no one knows a faster way to factor n and find p and q

Recall:
Euler's Theorem if a has gcd 1 with n then $a^{phi(n)} = 1(mod n)$
When working with exponents mod n work mod phi(n) in the exponent

Suppose $n = pq$
$phi(n) = phi(p)phi(q) = (p-1)(q-1)$
Alice picks 2 large primes pq (120ish digits)
She computes $n = pq$
She computes $phi(n) = (p-1)(q-1)$
She picks an encryption exponent e

need $gcd(phi, phi(n)) = 1$
often $e = 65535$
She computes $d = e^{-1}(modphi(n))$
Public Key (n,e)
Secret Decryption Key (p,q,d)
To send m to Alice, Bob computes
$C = M^(phi)(modn)$
He sends C to Alice
To decrypt Alice computes: $C = (m^(phi^(d)))(modn)$
Since $ed = 1mod(phi(n))$
$(m^{phi^d}) = m^{ed} = m^1(modn)$
Alice recovers Bobs message m