MATH 314 Fall 2019 - Class Notes

10/23/2019

Scribe: Samuel Alemayehu

Summary: Todays topic covered are public key cryptography encryption and decryption using RSA

Public Key Cryptography

Contrasts with symmetric Key Cryptography(Alice and Bob both Know the some Secret key)

Public Key Cryptography there is different encryption and decryption key. and figuring out the encryption key from the encryption key is hard to do.To do this we need a one way(or trap door) function: something easy to compute in one direction but hard to reverse (without extra information)

RSA First Public Key Cryptosystem

Inverted by Riverst Shamir and Adleman

One way function used in RSA is Factory/multiplication

Finding two large Prime number, p and a and multiply is easy

multiply pq=n If all you know is the integer n finding p and q is hard How dow we use this in RSA?

suppose Alice Finds large p and q and n=pq she also compute $\varphi(n)$

$\varphi(n) = (p-1)(q-1)$

she picks an encryption exponent e where $\gcd(e, \varphi(n)) = 1$

usually e=65537

=2^{16+1}

Encryption Function E(x)= X^e($\mod n$)

To decrypt we need to find d=e^{-1}($\mod \varphi(n)$)

Alice computes d=e^{-1}($\mod n$)

Decryption function is D(y)= y^d($\mod n$)

Alice makes numbers(n,e) public this is her public key she keeps(Also p,q,$\varphi(n)$)

but she can use(n,e) to send Alice a message. Suppose Bob uses this to send her a message P He computes C=p^c($\mod n$)

He Sends C to Alice

Alice decrypts it using C$^d = p^{e^d} = p^1$($\mod n$)

What if Eve Captures C?

Brute Force does not work because the number are two big.

She needs to find d to decrypt the message

Since d=e^{-1}($\mod \varphi(n)$)

She needs to know $\varphi(n)$

but the only fast way to do this is to know p and q.