MATH 314 Fall 2019 - Class Notes

10/23/2019

Scribe: Jay Romero

Summary : Public Key Cryptography

Public Key Cryptography

- Two different keys for encryption and decryption.
- Knowing the encryption key doesn't mean that one can easily compute the decryption key.
- The key ingredient in Public Key Cryptography is a one-way function (or a trap-door function).
- It is easy to compute in one direction but hard to undo (without extra information).

- Alice can create an encryption key K_p (public key) which she can tell everyone.
- There's a separate decryption key she keeps secret.
- Anyone can use K_p to send Alice a message.
- Without knowing the secret key no one besides Alice can decrypt.

RSA

- Invented in 1970s by Rivest, Shamir, and Adleman.
- It was the First Public Key Crypto System.
- One-way funtion is multiplication/factorization.

Steps for RSA

Alice picks p and q and finds n

- Alice finds two random prime numbers p, q
- She multiplies them $n = p * q$.

Compute $\varphi(n)$ and pick encryption exponent e and decryption exponent d

- Alice then computes $\varphi(n) = (p-1) * (q-1)$
- She picks an encryption exponent e where $gcd(e, \varphi(n)) = 1$
- In practice, $e = 65537$ is often chosen.
- Alice's public key (n, e) which others will use to send her a message.
- Her encryption function is $E(x) \equiv x^e (modn)$
- How does Alice decrypt? She computes $d = e^{-1}(mod\varphi(n))$
- d is Alice's private key which she keeps a secret.
- Her decryption function is $D(y) = y^d(modn)$.

Bob send a message to Alice

- In order for Bob to send a message P to Alice, Bob needs to use the public key information n, e.
- Bob computes $E(P) = P^e(modn) = C$

Alice decrypts Bob's message C

- Alice wants to decrypt the message that Bob sent her.
- She wants to decrypt $C = P^e(modn)$.
- She computes $D(C) \equiv C^d \equiv (\mathrm{P}^e)^d \equiv P(\mod n)$.
- Suppose Eve captures the ciphertext C. She wants to find P.
- Brute force is not an option; it doesn't work.
- To decrypt, Eve needs d where $d = e^{-1}(mod\varphi(n))$. Finding $\varphi(n)$ is as hard as factoring n.