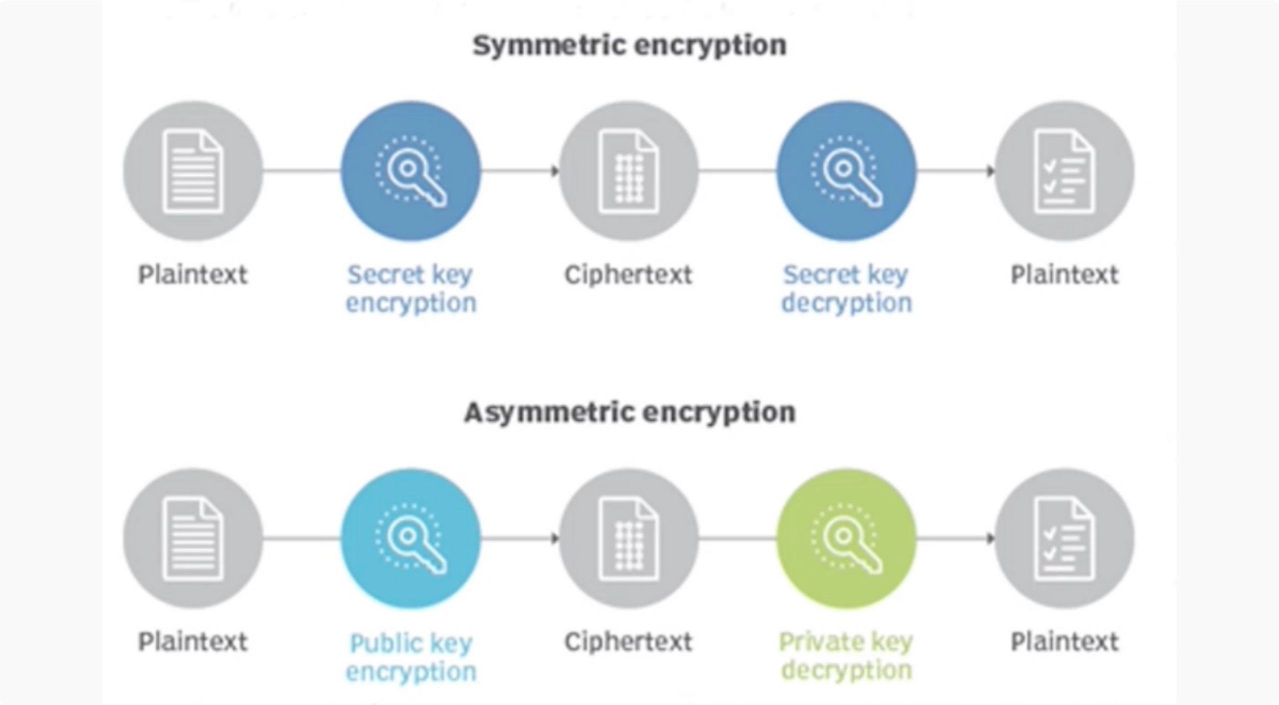
Lecture 5 🎍

> **Class**: Practical Cryptography and PKI
>
> **Date**: 13.14 AM , 11 Nov
>
> **Author**: Lasal Hettiarachchi

Key learnings:

- How Encryption , Hash fucnctions, digital signatures are used together in actual security
- How internet works on a security standpoint

Asymmetric Key encryption

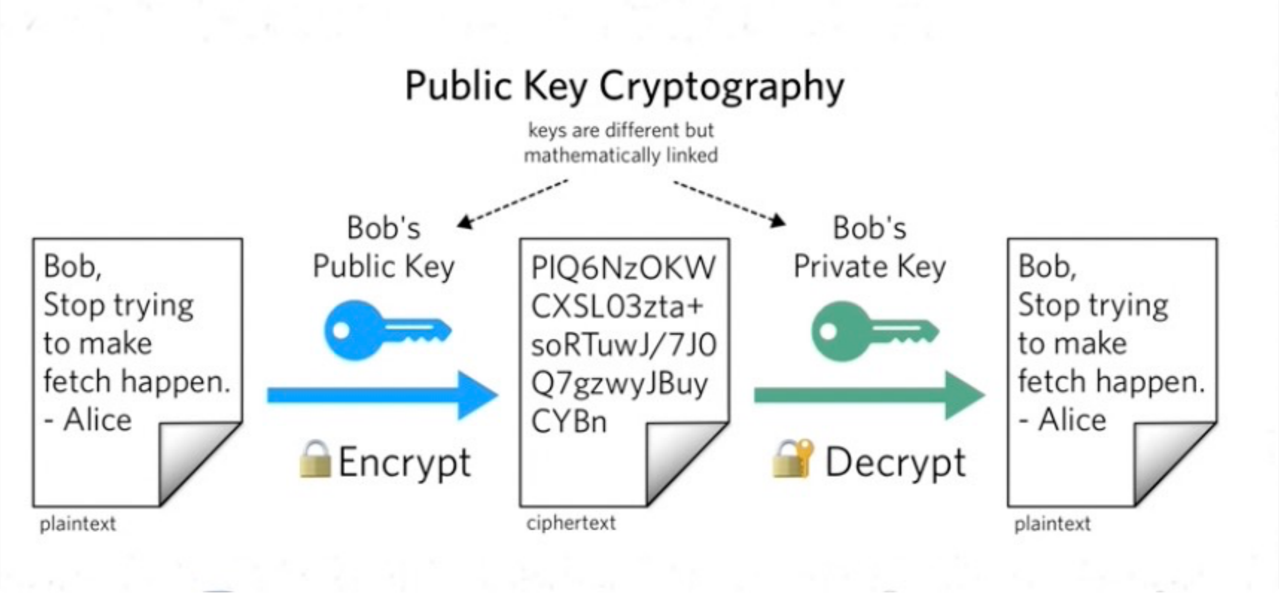


Key Generation

- High complex mathematics functions therefore time consuming
- Pseudo Random Number Generation is important in cryptography

How it works

- When someone wants to recieve a message they will generate a combination of public key private key
- The reciever then shares the public key
- Then the sender encrypts the message using the public key
- The receiver can decrypt the message using the private key of them



Public Key Cryptography
keys are different but mathematically linked
Bob's Public Key
Bob's Private Key
Bob, Stop trying to make fetch happen. - Alice
plaintext
Encrypt
PIQ6NzOKW CXSL03zta+ soRTuwJ/7J0 Q7gzwyJBuy CYBn
ciphertext
Decrypt
Bob, Stop trying to make fetch happen. - Alice
plaintext

- When someone wants to send an encrypted message, they can pull the intended recipient's public key from a public directory.
- They then use it to encrypt the message before sending it.
- The recipient of the message can then decrypt the message using their related private key.
- As the private key is only with receiver only he can read the message

Advantages of asymmetric key encryption

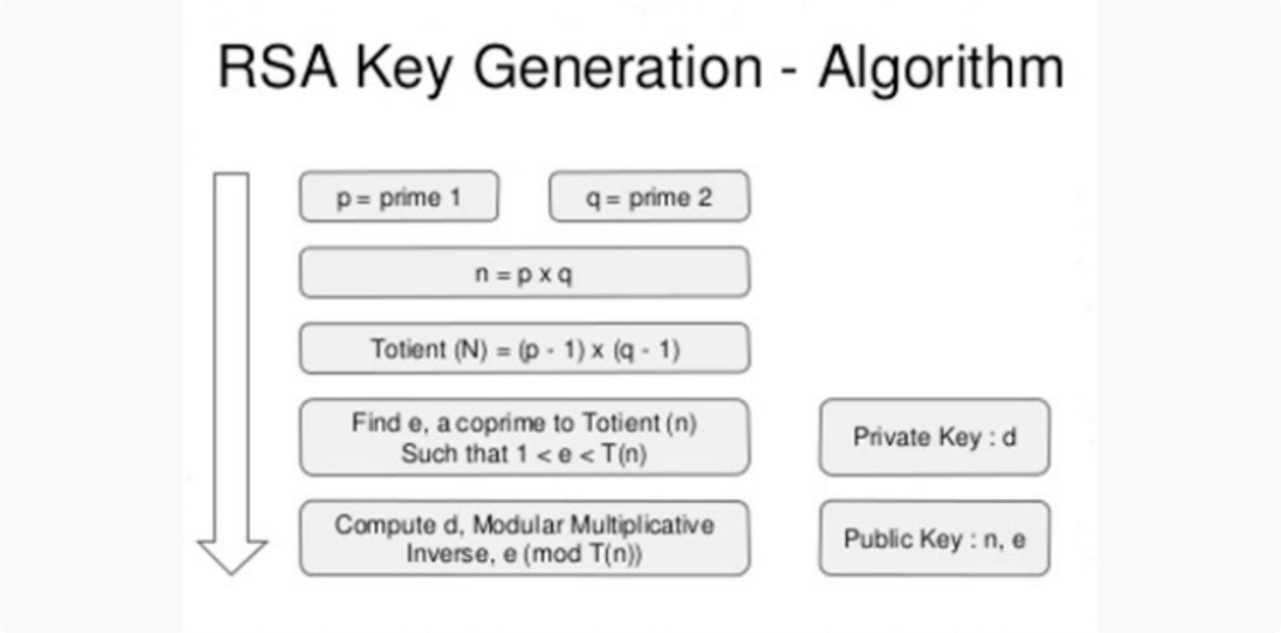
- No need to have another secure mechanism to share the key
- The use of digital signatures is enabled so that a recipient can verify that a message comes from a particular sender.
- It allows for non-repudiation so the sender can't deny sending a message.

disadvantages of asymmetric key encryption

- Overhead compared to symmentric
- not appropriate for decryption of bulk messages
- If an individual loses his private key, he can't decrypt the messages he receives.
- Since the public keys aren't authenticated, no one really knows if a public key belongs to the person specified. Consequently, users must verify that their public keys belong to them.
- If a hacker identifies a person's private key, the attacker can read all of that individual's messages.

RSA

- Support both public key encryption and digital signature
- Security relies on assumption that factorization of large primes is hard



RSA Key Generation - Algorithm

p = prime 1

q = prime 2

n = p x q

Totient (N) = (p - 1) x (q - 1)

Find e, a coprime to Totient (n)
Such that 1 < e < T(n)

Compute d, Modular Multiplicative
Inverse, e (mod T(n))

Private Key : d

Public Key : n, e

Attacks against RSA

- If the keys are not longer enough or the random numbers are not primes factorization attacks can be easily mounted
- Timing attacks use knowledge of the hardware used to measure decryption times for known cypher texts and then deduce

(Using other information about the physical hardware wheb decrypting to deduce the key)

- Rainbow table - a modified version of brute force attacks

Public key infrastructure

(How do I know the public key of Amarzon is from amarzon themselves)