Week 1
Part 2

Lecture 2

Encryption and Decryption

A social security number looks like this 111-22-3333
Encryption is a mathematical operation that takes the social security number. The information that we are trying to transmit over the internet, we call it plain text because, it is a plain text and there is nothing applied to it as of now. The moment we apply encryption, this will convert into something completely different, completely random.

Encrypt(111-22-3333) → Xa2MO1D9astLaSdnoP

[we use a key to encrypt]

[Encryption is basically a mathematical process that is capable of taking anything that is in plain text and converts it into something completely different]

Decrypt(Xa2MO1D9astLaSdnoP) → 111-22-3333

[we use the same key to decrypt]

If anyone else knows the value of this secret key then they will also be able to decrypt the encrypted document and breach confidentiality.

One major weakness of encryption is, the whole process of encryption relies on the secrecy of the same key.

Encryption is a two-way function because, whatever we are encrypting, the same encrypted thing can be decrypted back to get back the original plain text.

There are two major types of encryption,

1. Symmetric
2. Asymmetric

symmetric encryption is the one like before, we use same key for both encryption and decryption.

The major problem of symmetric encryption is that the whole system relies on the key being secret, if the key goes into a wrong hand, then they can access the information by decrypting it. There has to be a good way to exchang the key in a secured fashion. There are many cryptographic algorithms to do so.

Asymmetric encryption is also known as public key encryption.

The main difference between symmetric and asymmetric encryption is, in symmetric encryption there is one key but, in asymmetric encryption there are two keys, we call them a pair of keys. One of them is a private key and another

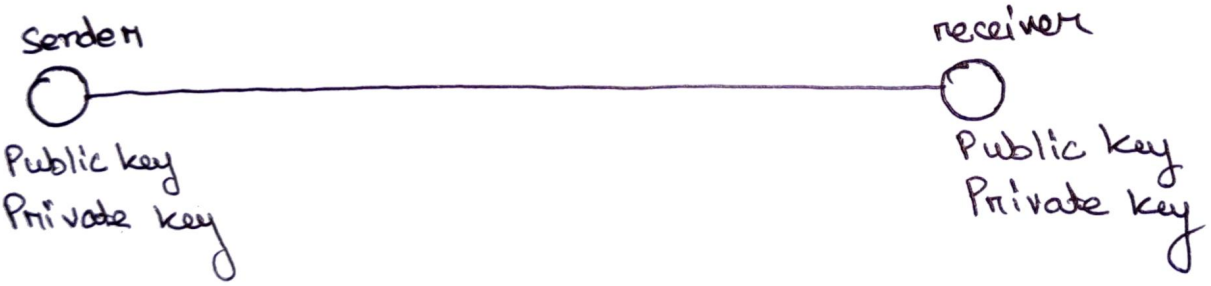
is Public key.

There are 3 very important properties of Private and Public keys in asymmetric encryption:

① Private and Public keys are mathematically linked together.

② Private key is not shared, Public key is shared with everyone.

③ It's mathematically impossible to DERIVE the Private key from the public key.



Private key is shared with nobody.
Public key is shared with everybody.

Now, about performance, Symmetric encryption is faster than asymmetric encryption because, we use the same key but in Asymmetric encryption there is a pair of key (Private and Public) mathematically linked together. when we need security mode, we will use asymmetric encryption and when we need performance mode we use Symmetric encryption.

In asymmetric encryption we have two major types of operation:

① Encryption
② Digital Signature

They are closely related but have different applications having different purposes!