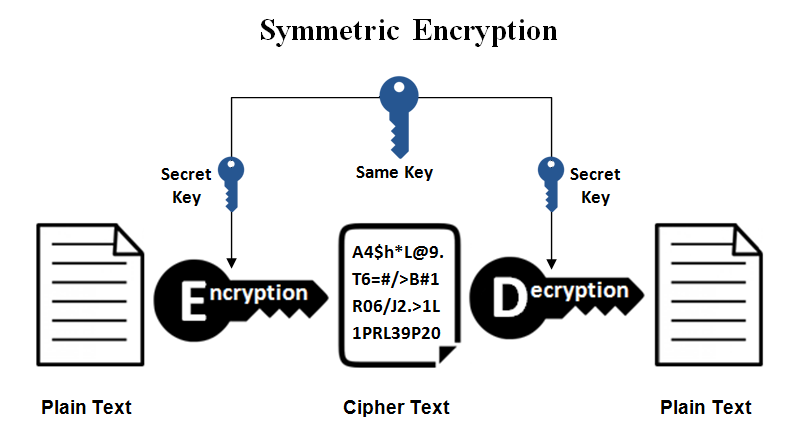
9/25/2018:

From 9.30 to 11.20 (1h50m)

Symmetric key: known as Private key cryptography

- We use the same key to encrypt and decrypt the data.

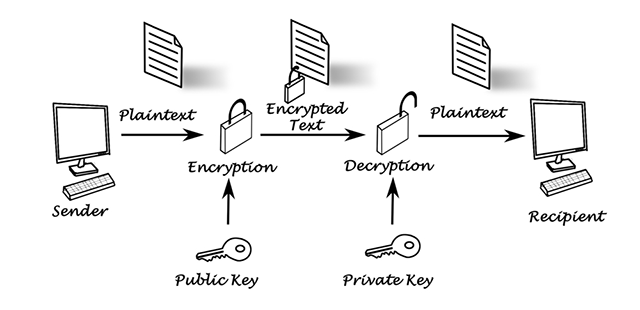


- The advantage of using symmetric key is that it is fast because we only need to know the key using for encryption and decryption.

- The disadvantage of using symmetric key is that the data is not so secured once the attacker gets the key.

Asymmetric key: Known as Public key cryptography

- Instead of using one single key to encrypt and decrypt as symmetric key, we use a key pair including Private key and Public key.



- We use public key to encrypt the data and we use the private key to decrypt the data.

- The public key will be broadcast to the network and everyone in the network will know it.

- However, the private key will be securely kept to make sure nobody knows about it.

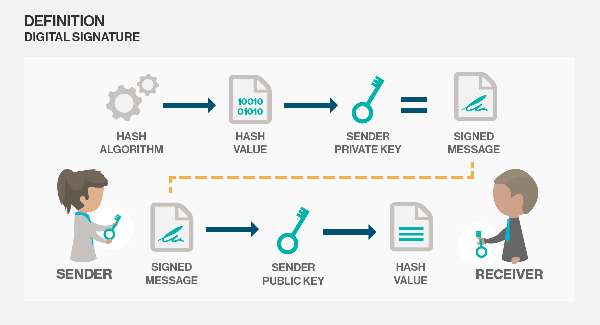
- Pros: it is much more secure than symmetric key because once the attacker got the public, he still can’t decrypt the data, unless he has the private key.

- Cons: it consumes time for working due to the complicated underlying mathematical system in order to secure the data.

Digital Signature: Known as Signing Certificate

- It is an electronic, encrypted, stamp of authentication on digital information such as email, files, documents.

- We use digital signature to make sure the data is integrity and non-repudiation.



- We use a key pair just like Asymmetric key. However, instead of keeping private key for your own, now you will use the private key to sign the data. And then signed document is sent to the receivers, they will use your public key to open the signed document.

