Cryptography

To send a message we encrypt the message at the sending point and decrypt it at the receiver point to protect it from hackers.

There are two types of cryptography

1. Symmetric key cryptography
2. Asymmetric key cryptography

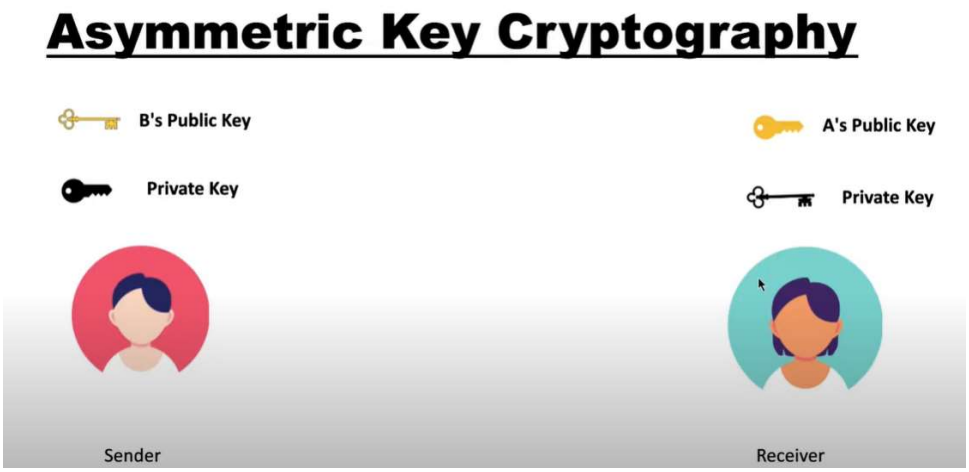
1. Symmetric key cryptography

In this type of cryptography, we encrypt the message with the help of a key and decrypt it with that same key. That key is sent with the message which simply means still it can be hacked.

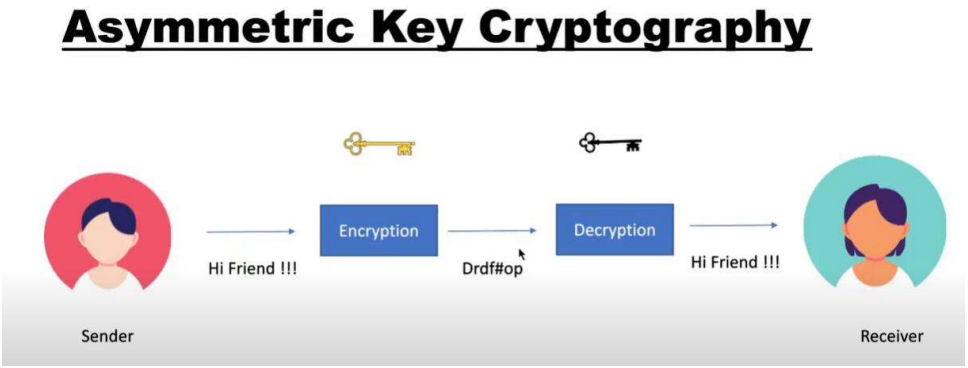
2. Asymmetric key cryptography

In this type of cryptography every user has two keys

1. Public key
2. Private key



As the names state public key means the user address or the key which is available/visible to the public and private key mean which is only available to you.



Any data encrypted with X person's public key can only be decrypted by X person's private key and vice versa. So, the sender will encrypt the data with receiver's public key and the receiver will decrypt it with his private key.