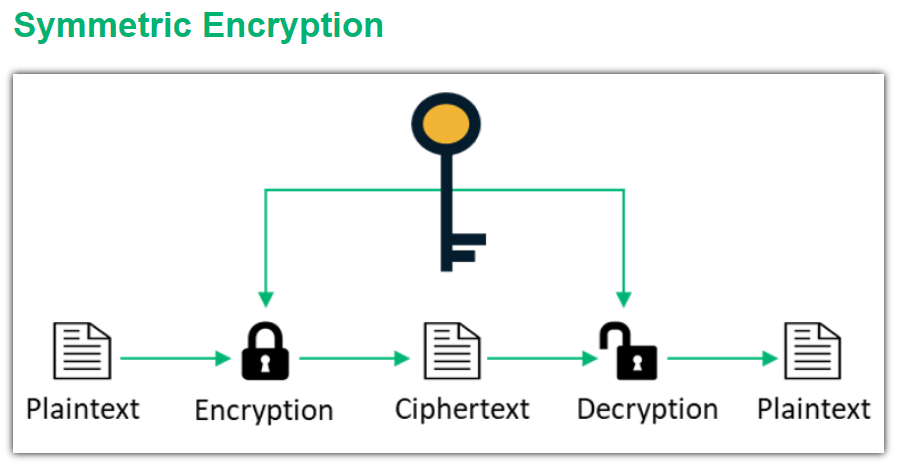
ENCRYPTION: In cryptography, encryption is the process of encoding information. This helps protect the confidentiality of digital data either stored on computer systems or transmitted through a network like the internet

Types:

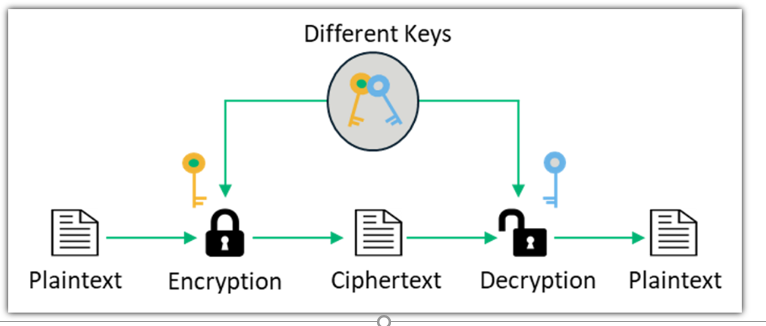
This is pretty direct one with 1 key…

Consider I want to receive data from you.

You locked data with your key and sent it me. But I also need your key to read data. But how will you send key? :P

**This is the limitation of Symmetric encryption.**





So, another encryption was introduced called **Asymmetric encryption**. (**Public key cryptography/ encryption**)

Consider now we use this, then I do following steps:

1. I will get 2 keys(privatekey, publickey). These keys are such that data locked by one key can only be unlocked with another key.
2. I will give you my publickey and ask you to lock data with that key. It’s okay whoever gets this key.
3. Now, whatever data you send, I will unlock(decrypt) with my private key.

The first step here is called “key pair generation”. RSA algorithm is used to generate keypair.

The [**SSH protocol**](https://www.ssh.com/ssh/protocol/) uses public key cryptography (asymmetric encryption) for authenticating hosts and users. The authentication keys, called [**SSH keys**](https://www.ssh.com/ssh/key/), are created using the keygen program.

ssh-keygen

**The issue here is that someone else** (attacker) might give you a public key telling its mine. Then the data that you gave will be accessible by the attacker. He will decrypt using his privatekey.

**So Certificates come into picture.**

What I will do is…instead of giving key directly… I get a certificate issued to me (with details on my public key and my name). Then I give it to you. Now you can verify my certificate and know that it’s my public key. To send me data you use that key. A certificate bind the public key to the owner/server.

Since you are sending me data, I would also want to know that it’s you who is sending.. you can also generate key pair, get a certificate from public key. Send me certificate.