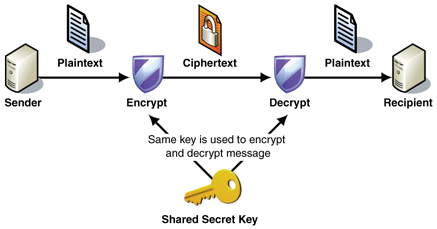
**SYMMETRIC AND ASYMMETRIC KEY ENCRYPTION**

SYMMETRIC KEY ENCRYPTION

Uses the same key to encrypt and decrypt data.



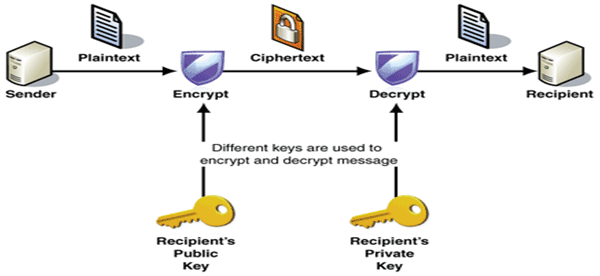
First, the sender encrypts the data using the key and sends the message through the channel.

The receiver cannot read the message as he/she doesn’t have the key.

The sender uses the same channel to send the key to the receiver, hacker can steal the key and decrypt the message.

People normally convey the key via a secure medium (e.g. telephone) but symmetric key encryption is not reliable and safe and is vulnerable to hackers.

ASYMMETRIC KEY ENCRYPTION



Here, a person has a public and a private key.

Suppose Alice and Bob are communicating with each other.

Alice

da : Private key

ea : Public key

Bob

db : Private key

eb : Public key

Now, public keys are only used for encryption of message.

Private keys are only used for decryption of message.

The public key of a person is known to everyone.

Private key is only known to that person.

Suppose Alice encrypts her message, say la using Bob’s public key (eb).

Bob decrypts the message using his private key, db.

If a hacker intercepts the message, he/she cannot read it as only Bob has the key db.

Similarly, if Bob encrypts a message using Alice’s public key (ea), only the private key da can decrypt the message.

Since everyone knows the key for encrypting the message, is it possible to figure out what the private key is?

The mathematics behind it is quite complex.

The basic idea is that when the data is encrypted using the public key, it is done in a way where there is a large number of possible solutions available. In order to decrypt the data, you would need to test every single solution until you find the right one. The process could take 100 years. The private key adds enough information to the puzzle such that there is only one solution.

* Asymmetric key encryption is slower compared to symmetric key encryption.
* Asymmetric key encryption is safer than symmetric key encryption.