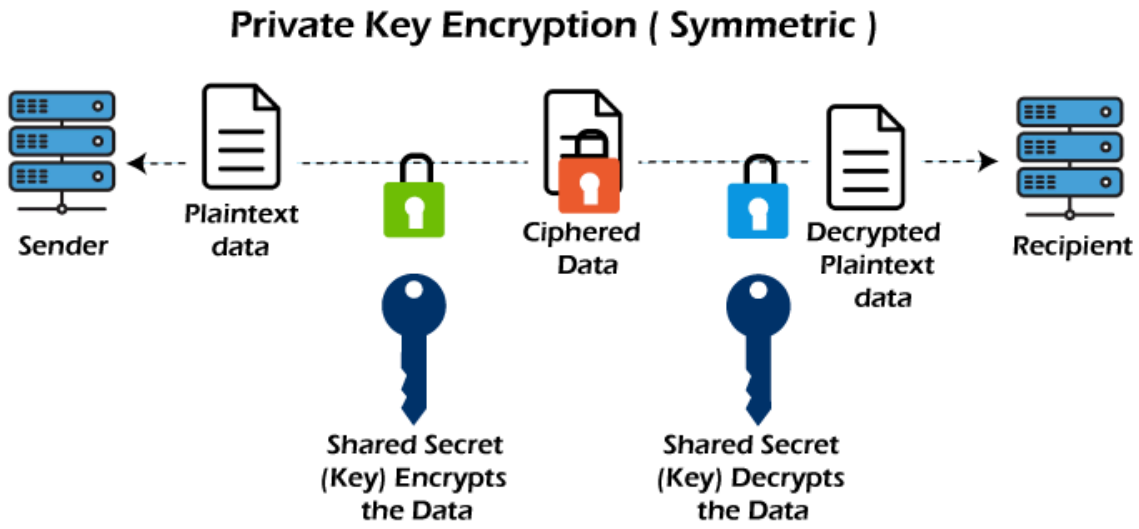
Public Key and Private Key

Private Key:

In Private key, the same key (secret key) is used for encryption and decryption. This key is symmetric because the only key is copy or share by another party to decrypt the ciphertext. It is faster than public key cryptography.

The sender uses the secret key and encryption algorithm for encryption, whereas for decryption, the receiver uses this key and decryption algorithm.

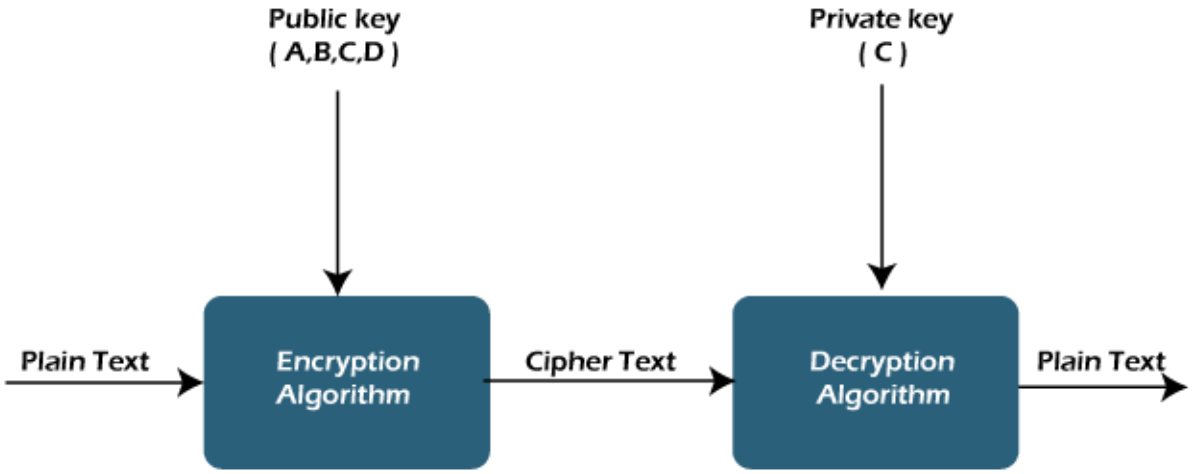
In the Secret Key Encryption/Decryption technique, the algorithm used for encryption is the inverse of the algorithm used for decryption. It means that if the combination of addition and multiplication is used in the encryption algorithm, then the decryption algorithm will use the combination of subtraction and division.



Public Key:

In Public key, two keys are used one key is used for encryption and another key is used for decryption. One key (public key) is used for encrypt the plain text to convert it into cipher text and another key (private key) is used by receiver to decrypt the cipher text to read the message.

The private key is given to the receiver while the public key is provided to the public. Public Key Cryptography is also known as asymmetric cryptography.



Difference between Private key and Public key

Private Key	**Public Key**
Private key is faster than public key.	It is slower than private key.
In this, the same key (secret key) and algorithm is used to encrypt and decrypt the message.	In public key cryptography, two keys are used, one key is used for encryption and while the other is used for decryption.
In private key cryptography, the key is kept as a secret.	In public key cryptography, one of the two keys is kept as a secret.
Private key is **Symmetrical** because there is only one key that is called secret key.	Public key is **Asymmetrical** because there are two types of key: private and public key.
In this cryptography, sender and receiver need to share the same key.	In this cryptography, sender and receiver do not need to share the same key.
In this cryptography, the key is private.	In cryptography, public keys can be public and private keys are private.