Public and Secret Key Encryption

Public key encryption, or public key cryptography, is a method of encrypting data with two different keys and making one of the keys, the public key, available for anyone to use. The other key is known as the **private key**. Data encrypted with the public key can only be decrypted with the private key, and data encrypted with the private key can only be decrypted with the public key. Public key encryption is also known as asymmetric encryption. It is widely used, especially for TLS/SSL, which makes HTTPS possible.

In such a system, any person can encrypt a message using the receiver's *public key*, but that encrypted message can only be decrypted with the receiver's *private key*.

Robust authentication is also possible. A sender can combine a message with a private key to create a short *digital signature* on the message. Anyone with the sender's corresponding public key can combine the same message and the supposed digital signature associated with it to verify whether the signature was valid, i.e. made by the owner of the corresponding private key.

Public key algorithms are fundamental security ingredients in modern cryptosystems, applications and protocols assuring the confidentiality, authenticity and non-reputability of electronic communications and data storage. They underpin various Internet standards, such as Transport Layer Security (TLS), S/MIME, PGP, and GPG. Some public key algorithms provide key distribution and secrecy (e.g., Diffie–Hellman key exchange), some provide digital signatures (e.g., Digital Signature Algorithm), and some provide both (e.g., RSA).

Private Key vs. Public Key

S.NO	Private Key	Public Key
1.	Private key is faster than public key.	It is slower than private key.
2.	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.
3.	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.
4.	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.
5.	In this cryptography, sender and receiver need to share the same key.	In this cryptography, sender and receiver does not need to share the same key.
6.	In this cryptography, the key is private.	In this cryptography, public key can be public and private key is private.