# Public Key Encryption

Public key cryptography provides a secure way to exchange information and authenticate users by using pairs of keys. The public key is used for encryption and signature verification, while the private key is used for decryption and signing. When the two parties communicate with each other to transfer the intelligible or sensible message, referred to as plaintext, is converted into apparently random unreadable for security purposes referred to as **ciphertext**.

## What is Public Key Cryptography?

Public key cryptography is a method of secure communication that uses a pair of keys, a public key, which anyone can use to encrypt messages or verify signatures, and a private key, which is kept secret and used to decrypt messages or sign documents. This system ensures that only the intended recipient can read an encrypted message and that a signed message truly comes from the claimed sender. Public key cryptography is essential for secure internet communications, allowing for confidential messaging, authentication of identities, and verification of data integrity.

## What is a Cryptographic Key?

A cryptographic key is a piece of information used by cryptographic algorithms to encrypt or decrypt data, authenticate identities, or generate digital signatures. It serves as a parameter to control cryptographic operations, ensuring the security and privacy of digital communications and transactions.

## How Does TLS/SSL Use Public Key Cryptography?

TLS/SSL uses public key cryptography to keep our internet connections secure. It does this in two main ways:

1. **Encryption**: When you visit a secure website (HTTPS), TLS/SSL helps encrypt data exchanged between your browser and the website's server. It uses a combination of public and private keys to create a secure connection. Your browser and the server agree on a secret key for this session, which keeps your data safe from eavesdroppers.
2. **Authentication**: TLS/SSL verifies the identity of websites. When you connect to a site, it presents a digital certificate signed by a trusted authority. Your browser checks this certificate to ensure you're really connecting to the right site and not a fake one trying to steal your information.

By using public key cryptography, TLS/SSL protects our privacy online and ensures that the websites we visit are genuine and trustworthy.

**Encryption**

The process of changing the plaintext into the ciphertext is referred to as **encryption.**

The encryption process consists of an algorithm and a key. The key is a value independent of the plaintext.

**The security of conventional encryption depends on the major two factors**

1. The Encryption algorithm
2. Secrecy of the key

Once the ciphertext is produced, it may be transmitted. The Encryption algorithm will produce a different output depending on the specific key being used at the time. Changing the key changes the output of the algorithm.

Once the ciphertext is produced, it may be transmitted. Upon reception, the ciphertext can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption.

**Decryption**

The process of changing the ciphertext to the plaintext that process is known as **decryption**.

**Public Key Encryption :** Asymmetric is a form of Cryptosystem in which encryption and decryption are performed using different keys-Public key (known to everyone) and Private key (Secret key). This is known as **Public Key Encryption.**

**Difference Between Encryption and Public-Key Encryption**

| **Basis** | **Encryption** | **Public-Key Encryption** |
|---|---|---|
| Required for Work | • Same algorithm with the same key is used for encryption and decryption.<br>• The sender and receiver must share the algorithm and key. | • One algorithm is used for encryption and a related algorithm decryption with pair of keys, one for encryption and other for decryption.<br>• Receiver and Sender must each |

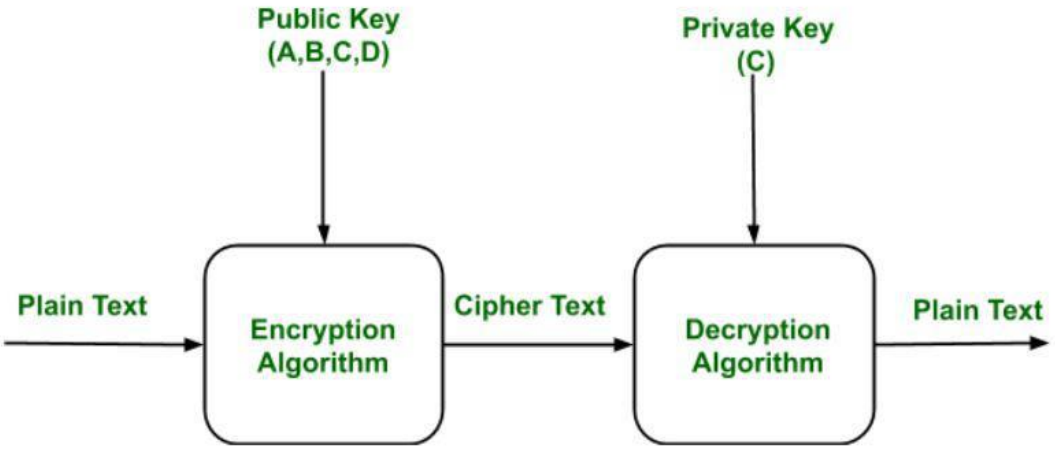
| Basis | Encryption | Public-Key Encryption |
|---|---|---|
| | | have one of the matched pair of keys (not identical) . |
| Required for Security | • Key must be kept secret.<br>• If the key is secret, it is very impossible to decipher message.<br>• Knowledge of the algorithm plus samples of ciphertext must be impractical to determine the key. | • One of the two keys must be kept secret.<br>• If one of the key is kept secret, it is very impossible to decipher message.<br>• Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be impractical to determine the other key. |

**Characteristics of Public Encryption key**

- Public key Encryption is important because it is infeasible to determine the decryption key given only the knowledge of the cryptographic algorithm and encryption key.
- Either of the two keys (Public and Private key) can be used for encryption with other key used for decryption.
- Due to Public key cryptosystem, public keys can be freely shared, allowing users an easy and convenient method for encrypting content and verifying digital signatures, and private keys can be kept secret, ensuring only the owners of the private keys can decrypt content and create digital signatures.
- The most widely used public-key cryptosystem is RSA (Rivest–Shamir–Adleman). The difficulty of finding the prime factors of a composite number is the backbone of RSA.

**Example:**

Public keys of every user are present in the Public key Register. If B wants to send a confidential message to C, then B encrypt the message using C Public key. When C receives the message from B then C can decrypt it using its own Private key. No other recipient other than C can decrypt the message because only C know C's private key.




*Public Key Encryption*

**Components of Public Key Encryption**

- **Plain Text:** This is the message which is readable or understandable. This message is given to the Encryption algorithm as an input.
- **Cipher Text:** The cipher text is produced as an output of Encryption algorithm. We cannot simply understand this message.
- **Encryption Algorithm:** The encryption algorithm is used to convert plain text into cipher text.
- **Decryption Algorithm:** It accepts the cipher text as input and the matching key (Private Key or Public key) and produces the original plain text
- **Public and Private Key:** One key either Private key (Secret key) or Public Key (known to everyone) is used for encryption and other is used for decryption

**Weakness of the Public Key Encryption**

- Public key Encryption is vulnerable to Brute-force attack.
- This algorithm also fails when the user lost his private key, then the Public key Encryption becomes the most vulnerable algorithm.
- Public Key Encryption also is weak towards man in the middle attack. In this attack a third party can disrupt the public key communication and then modify the public keys.
- If user private key used for certificate creation higher in the PKI (Public Key Infrastructure) server hierarchy is compromised, or accidentally disclosed, then a "man-in-the-middle attack" is also possible, making any subordinate

certificate wholly insecure. This is also the weakness of public key Encryption.

**Applications of the Public Key Encryption**

- **Encryption/Decryption:** Confidentiality can be achieved using Public Key Encryption. In this the Plain text is encrypted using receiver public key. This will ensure that no one other than receiver private key can decrypt the cipher text.
- **Digital signature:** Digital signature is for senders authentication purpose. In this sender encrypt the plain text using his own private key. This step will make sure the authentication of the sender because receiver can decrypt the cipher text using senders public key only.
- **Key exchange:** This algorithm can use in both Key-management and securely transmission of data.

**Conclusion**

Public key encryption is a powerful method for securing our digital communications. It uses two keys, a public key, which is shared openly, and a private key, which is kept secret. This system allows us to send encrypted messages and verify the authenticity of digital signatures without sharing secret keys beforehand. It's used widely in HTTPS for secure web browsing, email encryption, and digital signatures. Public key encryption keeps our online transactions safe and ensures that our private information remains confidential.