Public Key Cryptography

Unlike symmetric key cryptography, we do not find historical use of public-key cryptography. It is a relatively new concept.

Symmetric cryptography was well suited for organizations such as governments, military, and big financial corporations were involved in the classified communication.

With the spread of more unsecure computer networks in last few decades, a genuine need was felt to use cryptography at larger scale. The symmetric key was found to be non-practical due to challenges it faced for key management. This gave rise to the public key cryptosystems.

When the two parties communicate to each other to transfer the intelligible or sensible message, referred to as plaintext, is converted into apparently random nonsense for security purpose referred to as **ciphertext**.

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.	• One algorithm is used for encryption and a related algorithm decryption with pair of keys, one for

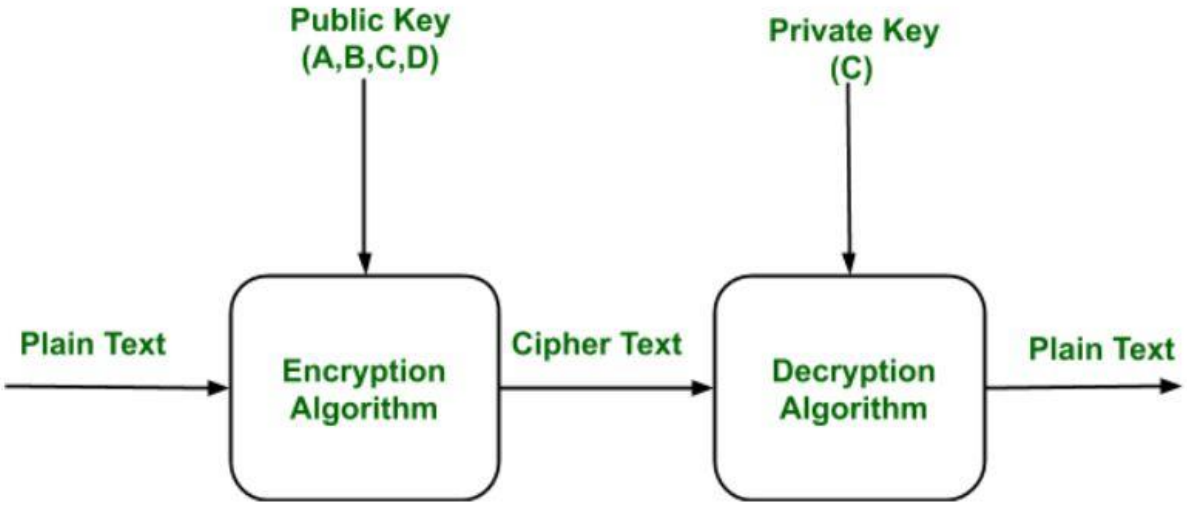
	• The sender and receiver must share the algorithm and key.	encryption and other for decryption. • Receiver and Sender must each have one of the matched pair of keys (not identical) .
Required for Security:	• Key must be kept secret. • If the key is secret, it is very impossible to decipher message. • Knowledge of the algorithm plus samples of ciphertext must be impractical to determine the key.	• One of the two keys must be kept secret. • If one of the key is kept secret, it is very impossible to decipher message. • 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.



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 sender's 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.