Public Key Cryptography (PKC)

- Public key cryptography (PKC) is an encryption technique that uses a paired public and private key (or asymmetric key) algorithm for secure data communication.
- A message sender uses a recipient's public key to encrypt a message.
- To decrypt the sender's message, only the recipient's private key may be used.
- The two types of PKC algorithms are RSA, which is an acronym named after this algorithm's inventors: Rivest, Shamir and Adelman, and Digital Signature Algorithm (DSA).
- PKC encryption evolved to meet the growing secure communication demands of multiple sectors and industries, such as the military.
- PKC is also known as public key encryption, asymmetric encryption, asymmetric cryptography, asymmetric cipher, and asymmetric key encryption and Diffie-Hellman encryption.

Public Key Cryptography (PKC)??

PKC is a cryptographic algorithm and cryptosystem component implemented by a variety of internet standards, including Transport Layer Security (TLS), Pretty Good Privacy (PGP), GNU Privacy Guard (GPG), Secure Socket Layer (SSL) and Hypertext Transfer Protocol (HTTP) websites.

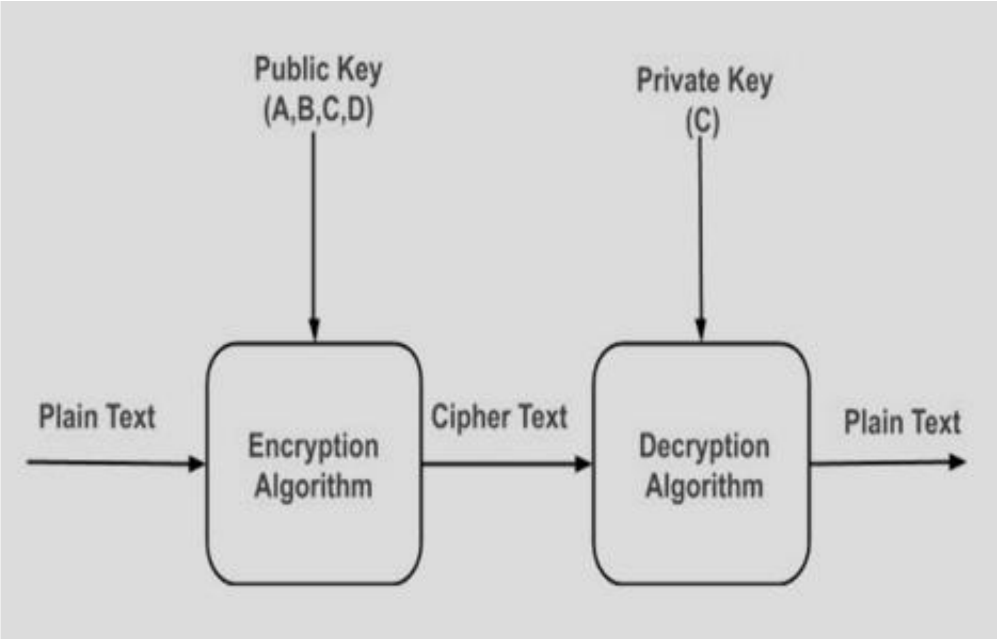
PKC facilitates secure communication through an insecure channel, which allows a message to be read by the intended recipient only. For example, A uses B's public key to encrypt a message to B, which can be decrypted using B's unique private key.

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 key (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:

- **PlainText:**
  This is the message which is readable or understandable. This message is given to the Encryption algorithm as an input.
- **CipherText:**
  The cipher text is produced as an output of Encryption algorithm. We cannot simply understand this message.
- **EncryptionAlgorithm:**
  The encryption algorithm is used to convert plain text into cipher text.
- **DecryptionAlgorithm:**
  It accepts the cipher text as input and the matching key (Private Key or Public key) and produces the original plain text
- **PublicandPrivateKey:**
  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:

- Confidentiality can be achieved using Public Key Encryption. In this the Plain text is encrypted using receiver public key. This will ensures that no one other than receiver private key can decrypt the cipher text.
- 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 pubic key only.

- This algorithm can use in both Key-management and securely transmission of data.

TASK

Difference between Private key and Public key with an example