**Public Key Encryption:**

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 cipher-text. Encryption: The process of changing the plaintext into the cipher-text 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:

**The Encryption algorithm :** Secrecy of the key Once the Cipher-Text 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 Cipher-Text is produced, it may be transmitted. Upon reception, the Cipher-Text 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 Cipher-Text 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.

**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.