Key Management in Cryptography

- Cryptography is the science of secret writing with the intention of keeping the data secret. Cryptography is classified into symmetric cryptography, asymmetric cryptography and hashing.

- Private Key:
  In Private key, the same key (secret key) is used for encryption and decryption. In this key is symmetric because the only key is copy or share by another party to decrypt the cipher text. It is faster than the public key cryptography.
- Public Key:
  In Public key, two keys are used one key is used for encryption and another key is used for decryption. One key (public key) is used for encrypt the plain text to convert it into cipher text and another key (private key) is used by receiver to decrypt the cipher text to read the message.

SNo	**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.

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 ciphertext.

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.

Once the ciphertext is produced, it may be transmitted.

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

1.The Encryption algorithm

2.Secrecy of the key

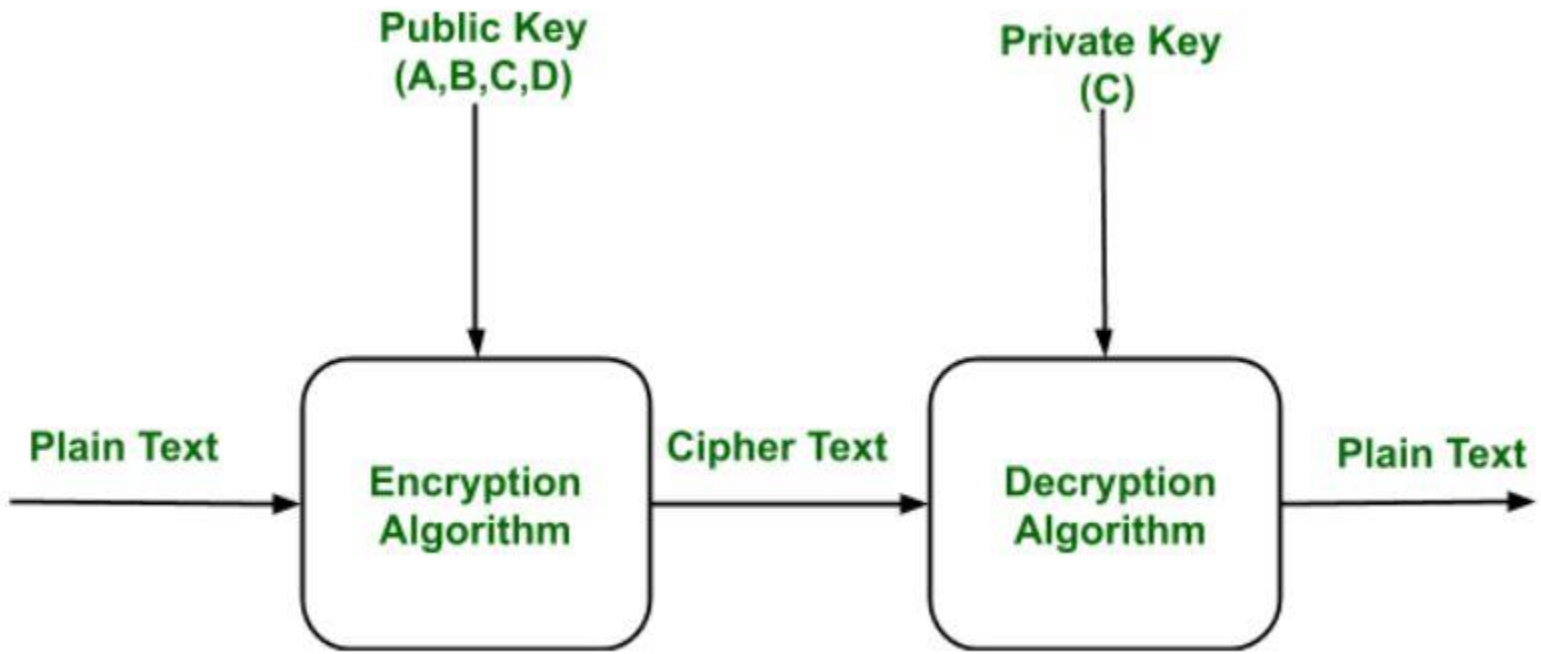
- The algorithm will produce a different output depending on the specific key being used at the time. Changing the key changes the output of the algorithm.
  Once the ciphertext is produced, it may be transmitted. Upon reception, the ciphertext can be transformed back to the original plaintext by using 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.
  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 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.


Public Key
(A,B,C,D)
Private Key
(C)
Plain Text
Encryption
Algorithm
Cipher Text
Decryption
Algorithm
Plain Text

Easy Key Management in Cryptography

Key Management:
In cryptography it is a very tedious task to distribute the public and private key between sender and receiver. If key is known to the third party (forger/eavesdropper) then the whole security mechanism becomes worthless. So, there comes the need to secure the exchange of keys.

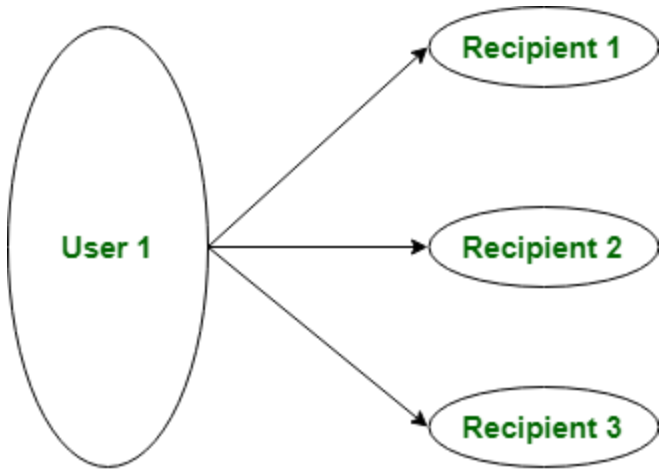
- There are 2 aspects for Key Management:

1. Distribution of public keys.
2. Use of public-key encryption to distribute secret.

- **Distribution of Public Key:**
- Public key can be distributed in 4 ways:
- Public announcement,
- Publicly available directory,
- Public-key authority, and
- Public-key certificates. These are explained in following slides.

1. Public Announcement:

Here the public key is broadcasted to everyone. Major weakness of this method is forgery. Anyone can create a key claiming to be someone else and broadcast it. Until forgery is discovered can masquerade as claimed user.



Public Key Announcement

2. Publicly Available Directory:

In this type, the public key is stored at a public directory. Directories are trusted here, with properties like Participant Registration, access and allow to modify values at any time, contains entries like {name, public-key}.Directories can be accessed electronically still vulnerable to forgery or tampering.

3. **Public Key Authority:**

It is similar to the directory but, improve security by tightening control over distribution of keys from directory. It requires users to know public key for the directory. Whenever the keys are needed, a real-time access to directory is made by the user to obtain any desired public key securely.

- 4. **Public Certification:**

This time authority provides a certificate (which binds identity to the public key) to allow key exchange without real-time access to the public authority each time. The certificate is accompanied with some other info such as period of validity, rights of use etc. All of this content is signed by the trusted Public-Key or Certificate Authority (CA) and it can be verified by anyone possessing the authority’s public-key.

Thank You