Principle of Public key cryptosystem

- There are **two** basic principles of any cryptosystem i.e. **confidentiality** and **authenticity.**
- **In symmetric cryptography**, the problem associated with confidentiality is that we all know in symmetric cryptography a secret key is used to encrypt as well as decrypt the message. So, this key must be shared by both the communicating parties by any means or they must rely on a third party for the distribution of the key i.e. key distribution centre. But relying on a third party again risk the secrecy of the secret key.
- Symmetric key also had an issue with authentication. The public key cryptosystem is successful in achieving both these principles
- Asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys- one public key and one private key
- Also known as public-key encryption
- It uses mathematical functions rather than substitution and permutation
- More secure from cryptanalysis than the symmetric encryption
- **Asymmetric keys** ¬
  Two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification
  - **Public key certificate** ¬
    A digital document issued and digitally signed by the private key of a Certification authority that fixes the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the corresponding private key.
- **Public key cryptographic algorithm** ¬
  A cryptographic algorithm that uses two related keys, a public key and a private key
  - **Public key infrastructure** ¬
    A set of policies, processes, server platform, software and workstations used for the purpose of controlling certificates and public- private key pairs, including the ability to issue, maintain, and cancel public certificate

- **To achieve both confidentiality and authenticity the public key algorithm has to be applied**.

Public key Cryptosystem

Any public key cryptographic algorithm has **six elements** as follow:

1. **Plain Text**
   This is a readable message which is given as input to the algorithm. In a public key algorithm, the plain text is encrypted in blocks.
2. **Encryption Algorithm**
   The encryption algorithm is implemented on the plain text which performs several transformations on plain text.
3. **Public and Private keys**
   These are the set of keys among which if one is used for encryption the other would be used for decryption. The transformation of plain text by encryption algorithm depends on the key chosen from the set to encrypt the plain text.
4. **Cipher Text**
   This is the output of encryption algorithm. The generated cipher text totally depends on the key selected from the set of the public and private key. Both of these keys, one at a time with plain text would produce different cipher texts.
5. **Decryption Algorithm**
   This would accept the output of the encryption algorithm i.e. the cipher text and will apply the related key to produce the original plain text.

NOTE 1:

Steps in public key cryptography.

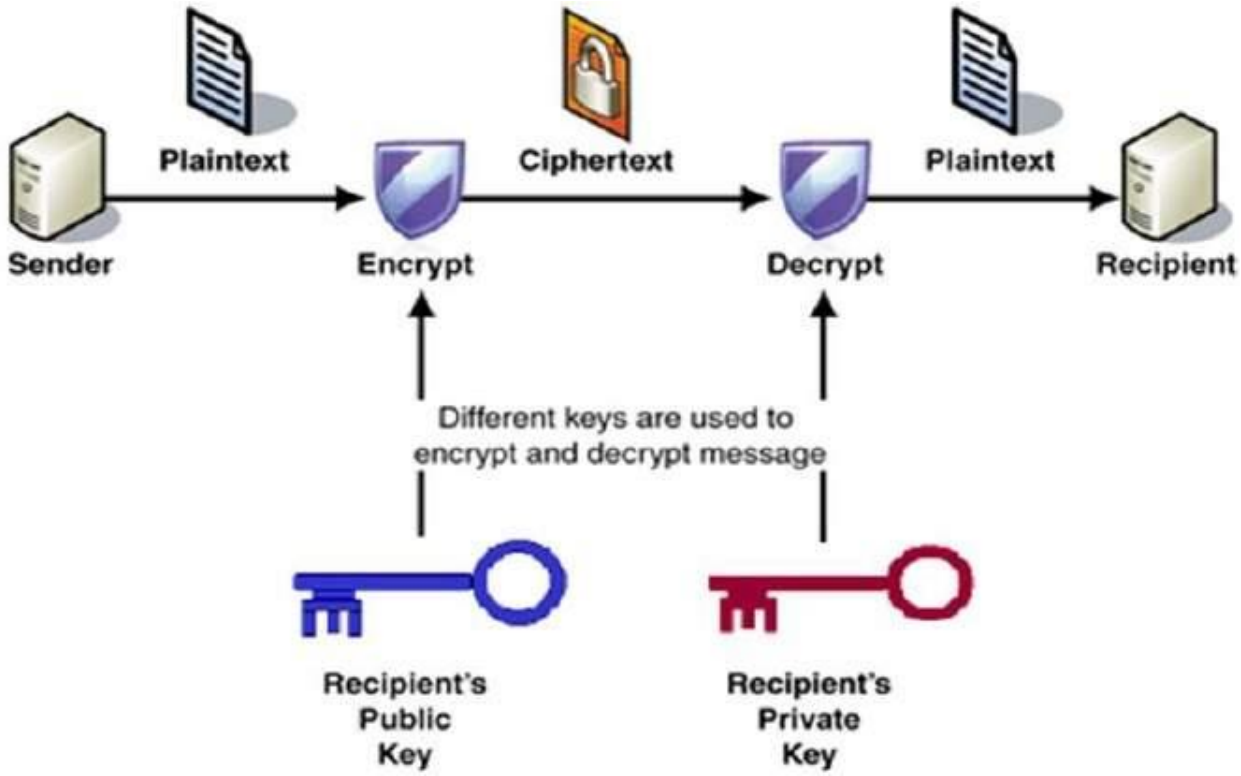
Step 1. Each user has to generate two keys one of which will be used for encryption and other for decryption of messages.

Step 2. Each user has a pair of keys, among which one has to be made public by each user. And the other has to be kept secret.

Step 3. If a user has to send a message to a particular receiver then the sender must encrypt the message using the intended receivers public key and then send the encrypted message to the receiver.

Step 4. On receiving the message, the receiver has to decrypt the message using his private key.

In public key cryptography, there is no need for key distribution as we have seen in symmetric key cryptography. As long as this private key is kept secret no one can interpret the message. In future, the user can change its private key and publish its related public key in order to replace the old public key.



NOTE 2:

- Public key cryptosystem is one which involves two separate keys for encryption and decryption.

- Each user participating in the communication has to generate two keys, one is to be kept secret (private key) and one is to make public (public key).

- Public key cryptosystem can achieve both confidentiality and authenticity.

- The public key cryptosystem is based on invertible mathematics so it has too much of computation.

- Large key size reduces the probability of brute force attack in public key cryptosystem

- Examples of public key cryptosystem are RSA, Diffie-Hellman, DSS and Elliptic curve.

Difference between Conventional and Public-Key Encryption

NOTE:

Conventional Encryption	**Public-Key Encryption**
Needed to Work:	Needed to Work:
1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key.	1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one).
Needed for Security:	Needed for Security:
1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

TASK :

Difference between Symmetric and Asymmetric key Cryptosystems

Write note on “Public Key Cryptography Requirements”