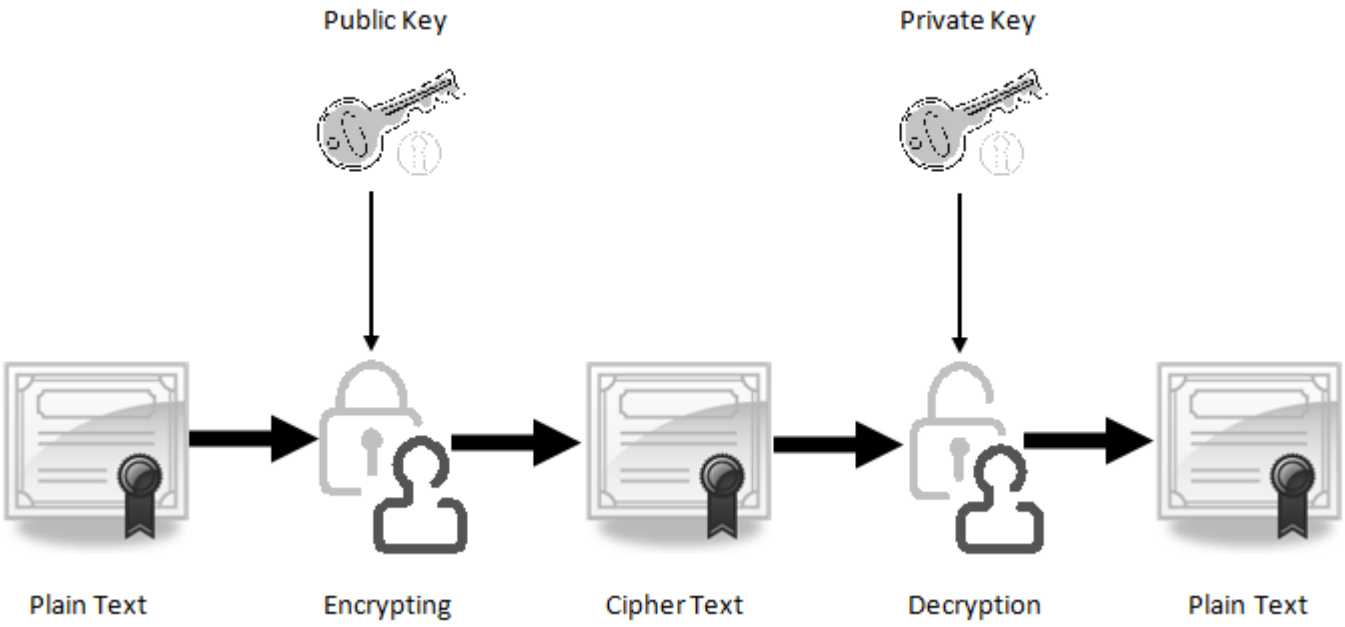
Experiment No. 16
A. Generate public and private key pair

Theoretical Background

What is a Public and Private Key Pair?

Private Key and public key are a part of encryption that encodes the information. Both keys work in two encryption systems called symmetric and asymmetric. Symmetric encryption (private-key encryption or secret-key encryption) utilize the same key for encryption and decryption. Asymmetric encryption utilizes a pair of keys like public and private key for better security where a message sender encrypts the message with the public key and the receiver decrypts it with his/her private key.

Public and Private key pair helps to encrypt information that ensures data is protected during transmission.



Public Key:

Public key uses asymmetric algorithms that convert messages into an unreadable format. A person who has a public key can encrypt the message intended for a specific receiver. The receiver with the private key can only decode the message, which is encrypted by the public key. The key is available via the public accessible directory.

Private Key:

The private key is a secret key that is used to decrypt the message and the party knows it that exchange message. In the traditional method, a secret key is shared within communicators to enable encryption and

decryption the message, but if the key is lost, the system becomes void. To avoid this weakness, PKI (public key infrastructure) came into force where a public key is used along with the private key. PKI enables internet users to exchange information in a secure way with the use of a public and private key.

Key Size and Algorithms:

There are RSA, DSA, ECC (Elliptic Curve Cryptography) algorithms that are used to create a public and private key in public key cryptography (Asymmetric encryption). Due to security reason, the latest CA/Browser forum and IST advises to use 2048-bit RSA key. The key size (bit-length) of a public and private key pair decides how easily the key can be exploited with a brute force attack. The more computing power increases, it requires more strong keys to secure transmitting data.

The Public Key is what its name suggests - Public. It is made available to everyone via a publicly accessible repository or directory. On the other hand, the Private Key must remain confidential to its respective owner.

Because the key pair is mathematically related, whatever is encrypted with a Public Key may only be decrypted by its corresponding Private Key and vice versa.

For example, if Bob wants to send sensitive data to Alice, and wants to be sure that only Alice may be able to read it, he will encrypt the data with Alice's Public Key. Only Alice has access to her corresponding Private Key and as a result is the only person with the capability of decrypting the encrypted data back into its original form.

As only Alice has access to her Private Key, it is possible that only Alice can decrypt the encrypted data. Even if someone else gains access to the encrypted data, it will remain confidential as they should not have access to Alice's Private Key.

Conclusion

We have conclude that Generate public and private key pair successfully.

Exercise

1. What is a private key?
2. What is a public key?
3. What is Key Size and Algorithms?

Answers

Marks obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total(25)**	