Unit 3: Internet Security & Privacy

Internet Security

Internet security refers to securing communication over the internet. It includes specific security protocols such as:

- Internet Security Protocol (IPSec)
- Secure Socket Layer (SSL)

Internet Security Protocol (IPSec)

It consists of a set of protocols designed by Internet Engineering Task Force (IETF). It provides security at network level and helps to create authenticated and confidential packets for IP layer.

Secure Socket Layer (SSL)

It is a security protocol developed by Netscape Communications Corporation.). It provides security at transport layer. It addresses the following security issues:

- Privacy
- Integrity
- Authentication

Data Encryption

Encryption is a security method in which information is encoded in such a way that only authorized user can read it. It uses encryption algorithm to generate cipher text that can only be read if decrypted.

- Cryptography is a method of storing and transmitting data in a particular form.
- It ensures that only the person for whom the message is intended can read the message.

Step – 1:

At sender side,

- Using an encryption algorithm, the message is converted into an unreadable form.
- The message in unreadable form is called as **cipher text**.

Step – 2:

- The cipher text is sent to the receiver over the communication channel.
- Since the message is encrypted, the attackers can not read the message.

Step – 3:

At receiver side,

- Using a decryption algorithm, the message is again converted into the readable form.
- Then, receiver can read the message.

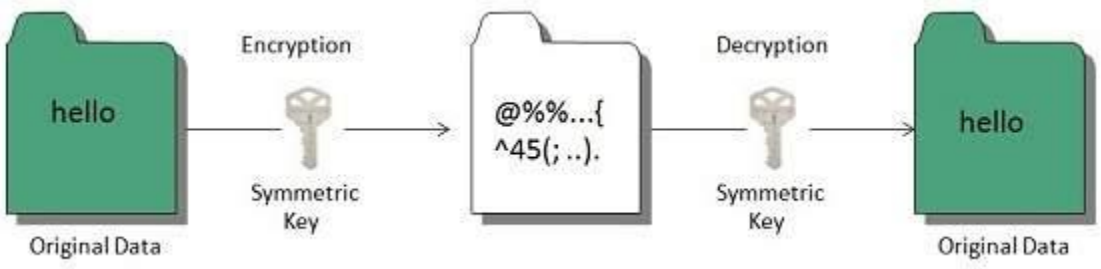
Types of Encryption

There are two types of encryptions schemes as listed below:

- Symmetric Key encryption
- Public Key encryption

Symmetric Key encryption

Symmetric key encryption algorithm uses same cryptographic keys for both encryption and decryption of cipher text.

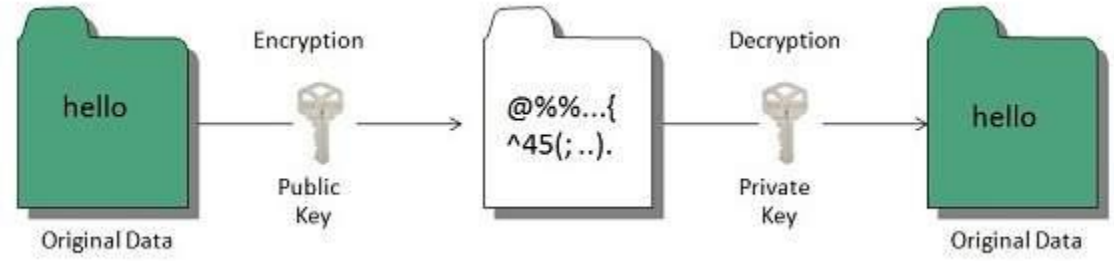


- It is also called as **secret key cryptography**.
- Before starting the communication, sender and receiver shares the secret key.
- This secret key is shared through some external means.

- At sender side, sender encrypts the message using his copy of the key.
- The cipher text is then sent to the receiver over the communication channel.
- At receiver side, receiver decrypts the cipher text using his copy of the key.
- After decryption, the message converts back into readable format.

Public Key encryption

Public key encryption algorithm uses pair of keys, one of which is a secret key and one of which is public. These two keys are mathematically linked with each other.



- It is also called as **Asymmetric key cryptography**.

Step-01:

At sender side,

- Sender encrypts the message using receiver's public key.
- The public key of receiver is publicly available and known to everyone.
- Encryption converts the message into a cipher text.
- This cipher text can be decrypted only using the receiver's private key.

Step-02:

- The cipher text is sent to the receiver over the communication channel.

Step-03:

At receiver side,

- Receiver decrypts the cipher text using his private key.
- The private key of the receiver is known only to the receiver.
- Using the public key, it is not possible for anyone to determine the receiver's private key.

- After decryption, cipher text converts back into a readable format.

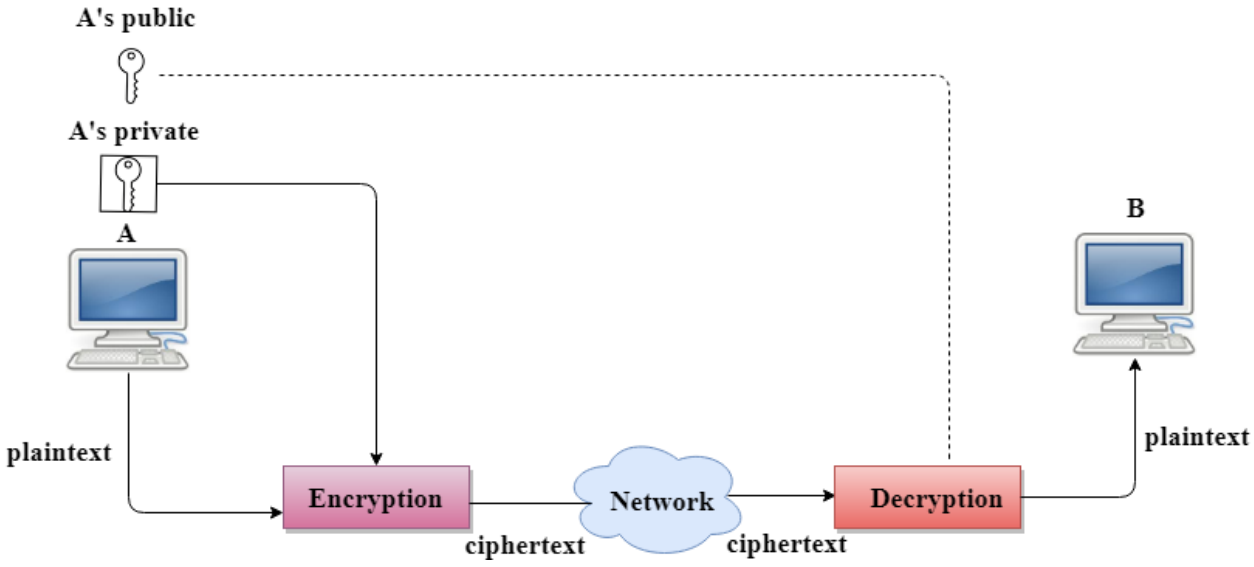
Digital Signature

Digital signatures allow us to verify the author, date and time of signatures, authenticate the message contents. It also includes authentication function for additional capabilities.

A digital signature should not only be tied to the signing user, but also to the message.

Signing the Whole Document

- In Digital Signature, a public key encryption technique is used to sign a document. However, the roles of a public key and private key are different here. The sender uses a private key to encrypt the message while the receiver uses the public key of the sender to decrypt the message.
- In Digital Signature, the private key is used for encryption while the public key is used for decryption.



Applications

There are several reasons to implement digital signatures to communications:

Authentication

Digital signatures help to authenticate the sources of messages. For example, if a bank's branch office sends a message to central office, requesting for change in balance of an account. If the central office could not authenticate that message is sent from an authorized source, acting of such request could be a grave mistake.

Integrity

Once the message is signed, any change in the message would invalidate the signature.

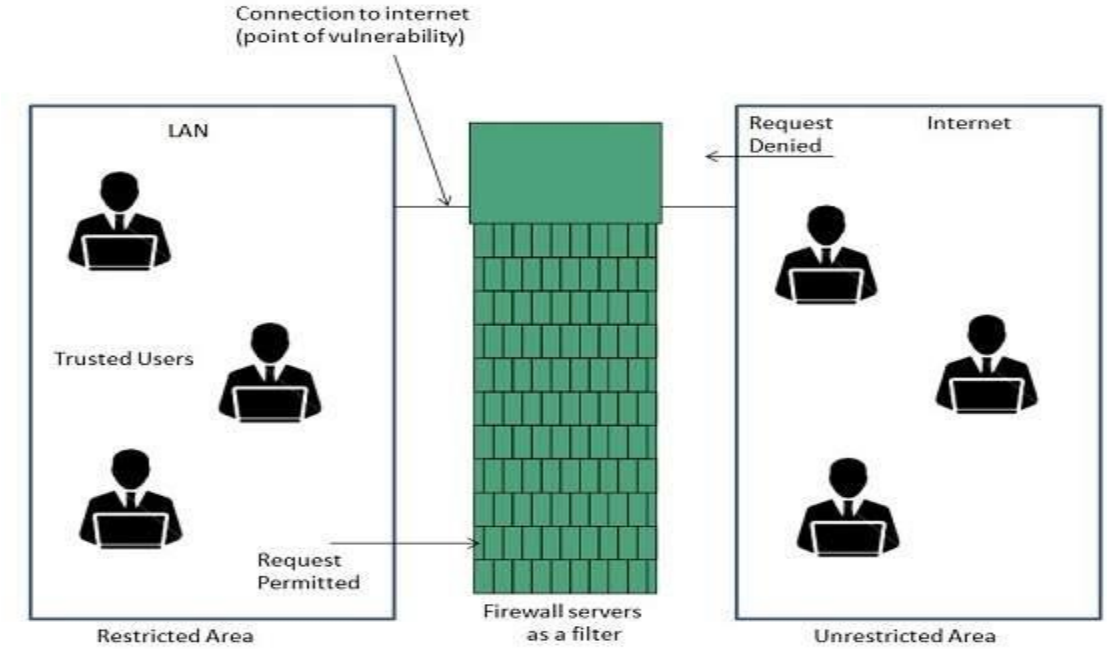
Non-repudiation

By this property, any entity that has signed some information cannot at a later time deny having signed it.

Firewall Security

Firewall is a barrier between Local Area Network (LAN) and the Internet. It allows keeping private resources confidential and minimizes the security risks. It controls network traffic, in both directions.

The following diagram depicts a sample firewall between LAN and the internet. The connection between the two is the point of vulnerability. Both hardware and the software can be used at this point to filter network traffic.



Created By:
Prof. Chirag Prajapati – SDJ International College, Surat.

There are two types of Firewall system: One works by using filters at the network layer and the other works by using proxy servers at the user, application, or network layer.

- Firewall management must be addressed by both system managers and the network managers.
- The amount of filtering a firewall varies. For the same firewall, the amount of filtering may be different in different directions.