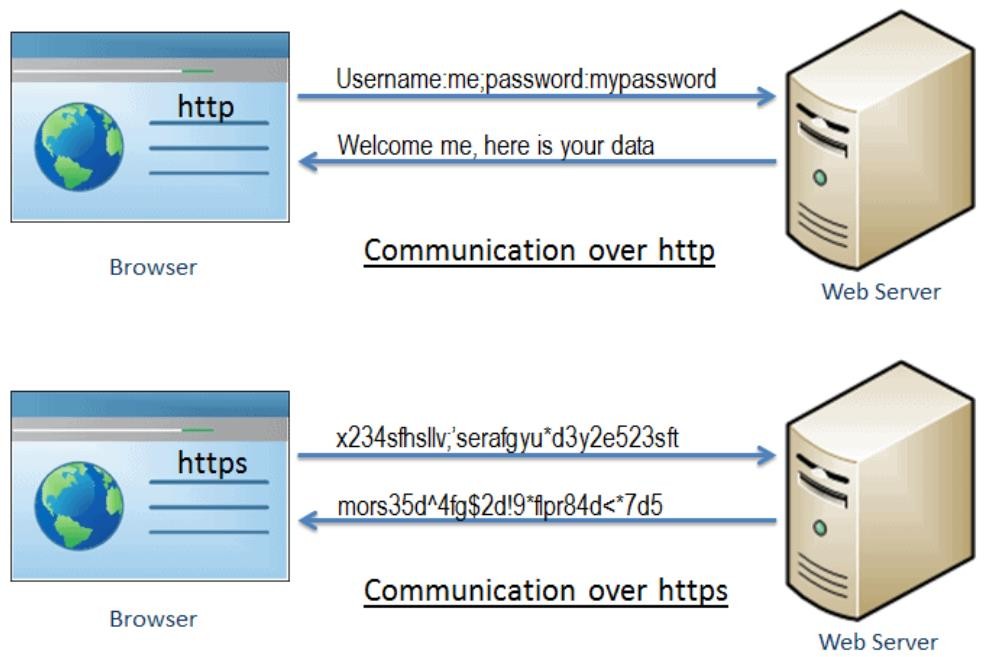
# What is https?

HTTPS stands for Hyper Text Transfer Protocol Secure. It is a protocol for securing the communication between two systems e.g. the browser and the web server.

The following figure illustrates the difference between communication over http and https:



As you can see in the above figure, http transfers data between the browser and the web server in the hypertext format, whereas https transfers data in the encrypted format. Thus, https prevents hackers from reading and modifying the data during the transfer between the browser and the web server. Even if hackers manage to intercept the communication, they will not be able to use it because the message is encrypted.

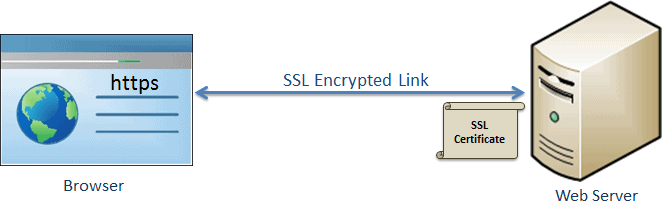
Port no Http:80 and Port no Https:443.

HTTPS established an encrypted link between the browser and the web server using the Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocols. TLS is the new version of SSL.

# Secure Socket Layer (SSL)

SSL is the standard security technology for establishing an encrypted link between the two systems. These can be browser to server, server to server or client to server. Basically, SSL ensures that the data transfer between the two systems remains encrypted and private.

The https is essentially http over SSL. SSL establishes an encrypted link using an SSL certificate which is also known as a digital certificate.



SSL

# http vs https

|  |  |
| --- | --- |
| http | https |
| Transfers data in hypertext (structured text) format | Transfers data in encrypted format |
| Uses port 80 by default | Uses port 443 by default |
| Not secure | Secured using SSL technology |
| Starts with http:// | Starts with https:// |

# [Virtual Private Network (VPN)](https://www.geeksforgeeks.org/virtual-private-network-vpn-introduction/)

VPN stands for [Virtual Private Network (VPN)](https://www.geeksforgeeks.org/virtual-private-network-vpn-introduction/), that allows a user to connect to a private network over the Internet securely and privately. VPN creates an encrypted connection that is called VPN tunnel, and all Internet traffic and communication is passed through this secure tunnel.

Virtual Private Network (VPN) is basically of 2 types:

## RemoteAccessVPN:

Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely. The connection between the user and the private network occurs through the Internet and the connection is secure and private. Remote Access VPN is useful for home users and business users both.

## SitetoSiteVPN:

A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies. Companies or organizations, with branch offices in different locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.

# Telnet

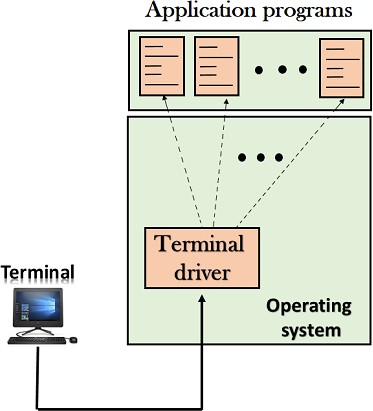
* The main task of the internet is to provide services to users. For example, users want to run different application programs at the remote site and transfers a result to the local site. This requires a client-server program such as FTP, SMTP. But this would not allow us to create a specific program for each demand.
* The better solution is to provide a general client-server program that lets the user access any application program on a remote computer. Therefore, a program that allows a user

to log on to a remote computer. A popular client-server program Telnet is used to meet such demands. Telnet is an abbreviation for **Terminal Network**.

* Telnet provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side.

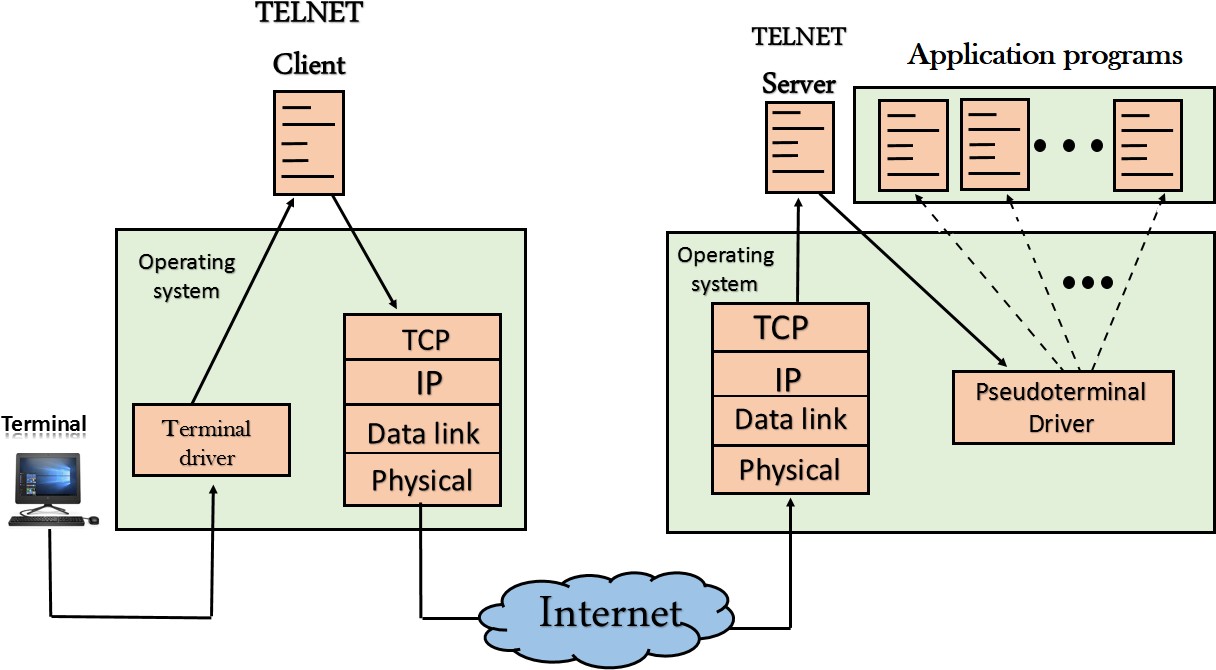
There are two types of login:

# Local Login



* + When a user logs into a local computer, then it is known as local login.

# Remote login



* + When the user wants to access an application program on a remote computer, then the user must perform remote login.

Simple Mail Transfer Protocol (SMTP)

Email is emerging as one of the most valuable services on the internet today. Most internet systems use SMTP as a method to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) are used to retrieve those emails at the receiver’s side.

## Fundamentals

SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is an always-on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection through port 25. After successfully establishing a TCP connection the client process sends the mail instantly.

## SMTP Protocol

The SMTP model is of two types:

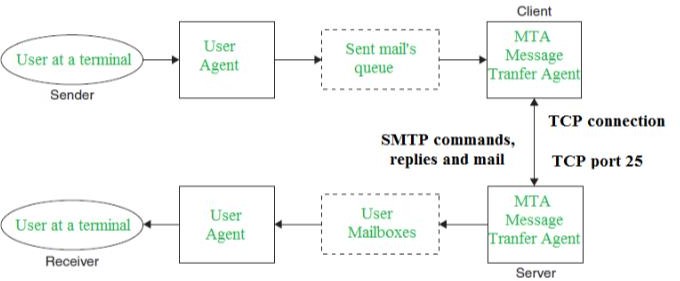
1. End-to-end method
2. Store-and- forward method

The end-to-end model is used to communicate between different organizations whereas the store and forward method is used within an organization. An SMTP client who wants to send the mail will contact the destination’s host SMTP directly, in order to send the mail to the destination. The SMTP server will keep the mail to itself until it is successfully copied to the receiver’s SMTP.

The client SMTP is the one that initiates the session so let us call it client- SMTP and the server SMTP is the one that responds to the session request so let us call it receiver-SMTP. The client- SMTP will start the session and the receiver-SMTP will respond to the request.

Model of SMTP system

In the SMTP model user deals with the user agent (UA), for example, Microsoft Outlook, Netscape, Mozilla, etc. In order to exchange the mail using TCP, MTA is used. The user sending the mail doesn’t have to deal with MTA as it is the responsibility of the system admin to set up a local MTA. The MTA maintains a small queue of mails so that it can schedule repeat delivery of mails in case the receiver is not available. The MTA delivers the mail to the mailboxes and the information can later be downloaded by the user agents.



Both the SMTP-client and SMTP-server should have 2 components:

1. User-agent (UA)
2. Local MTA

### Communication between sender and the receiver:

The sender’s user agent prepares the message and sends it to the MTA. The MTA’s responsibility is to transfer the mail across the network to the receiver’s MTA. To send mails, a system must have a client MTA, and to receive mails, a system must have a server MTA.

.

### RECEIVING EMAIL:

The user agent at the server-side checks the mailboxes at a particular time of intervals. If any information is received, it informs the user about the mail. When the user tries to read the mail it displays a list of emails with a short description of each mail in the mailbox. By selecting any of the mail users can view its contents on the terminal.

# What is DNS?

The domain name system (DNS) is a naming database in which internet [domain](https://www.techtarget.com/whatis/definition/domain) names are located and translated into [Internet Protocol (IP) addresses.](https://www.techtarget.com/whatis/definition/IP-address-Internet-Protocol-Address) The domain name system maps the name people use to locate a website to the IP address that a computer uses to locate that website.

For example, if someone types "example.com" into a web browser, a server behind the scenes maps that name to the corresponding IP address. An IP address is similar in structure to 203.0.113.72.

* 1. **SATELLITE NETWORKS**

# Three Categories of Satellites

Based on the location of the orbit, satellites can be divided into three categOlies: geosta• tionary Earth orbit (GEO), low-Earth-orbit (LEO), and middle-Earth-orbit (MEO). Figure 16.14 shows the taxonomy.

Figure 16.14 *Satellite categories*

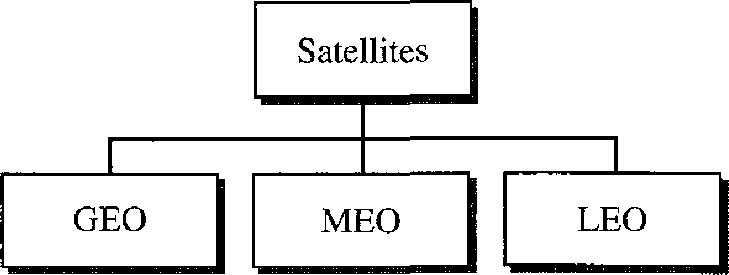


Figure 16.15 shows the satellite altitudes with respect to the surface of the Earth. There is only one orbit, at an altitude of 35,786 kIn for the OEO satellite. MEO satellites are located at altitudes between 5000 and 15,000 kIn. LEO satellites are normally below an altitude of 2000 km.

Figure 16.15 *Satellite orbit altitudes*



Upper Van Allen belt

MEa

Lower Van Allen belt

LEO

Altitude

(km)

35,786

# GEO Satellites

A satellite that moves faster or slower than the Earth's rotation is useful only for short periods. To ensure constant communication, the satellite must move at the same speed as the Earth so that it seems to remain fixed above a certain spot. Such satellites are called *geostationary.*

Because orbital speed is based on the distance from the planet, only one orbit can be geostationary. This orbit occurs at the equatorial plane and is approximately 36,00Km approx.(22,000 mi) from the surface of the Earth.

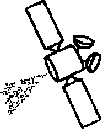
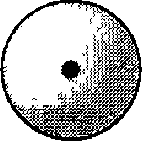
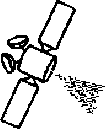
It takes a minimum of three satellites equidistant from each other in geostationary Earth orbit (OEO) to provide full global transmission

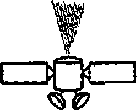
# MEO Satellites

Medium-Earth-orbit (MEO) satellites are positioned between the two Van Allen belts. A satellite at this orbit takes approximately 6-8 hours to circle the Earth.

*Global Positioning System*

One example of a MEO satellite system is the Global Positioning System (GPS), con• stracted and operated by the US Department of Defense, orbiting at an altitude about

Figure 16.16 *Satellites in geostationary orbit*



18,000 km (11,000 mi) above the Earth. The system consists of 24 satellites and is used for land, sea, and air navigation to provide time and locations for vehicles and ships. GPS uses 24 satellites in six orbits, as shown in Figure 16.17. The orbits and the locations of the satellites in each orbit are designed in such a way that, at any time, four satellites are visible from any point on Earth.

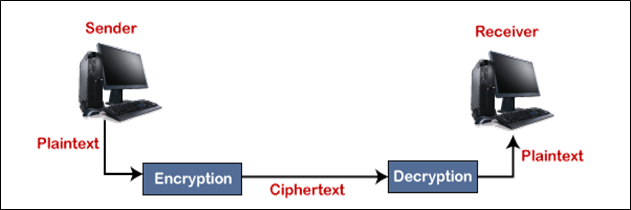
## LEO Satellites

Low-Earth-orbit (LEO) satellites have polar orbits. The altitude is between 500 and 2000 km, with a rotation period of 90 to 120 min. The satellite has a speed of 20,000 to 25,000 km/h. An LEO system usually has a cellular type of access, similar to the cellu• lar telephone system. The footprint normally has a diameter of 8000 km. Because LEO satellites are close to Earth, the round-trip time propagation delay is normally less than 20 ms, which is acceptable for audio communication.

# [Cryptography in Computer Network](https://www.tutorialandexample.com/cryptography-in-computer-network)

**Cryptography**: Cryptography is derived from the Greek word, which means "Hidden Secrets." In other words, it is an art in which we can protect our data and information. Through cryptography, we convert our data into Unreadable Secret Codes, called Cipher Text and can read this data only, which will have the secret key to decrypt it. Decrypt data is called plain text. It maintains the security and integrity of the data.

In cryptography, encryption and decryption are two processes. It is used to protect the Messages, Credit/Debit Card details, and other relevant information. In encryption, plain text is converted to ciphertext, and in decryption, the ciphertext is converted to plain text.



Cryptography has many advantages because encryption makes your data completely secure and safe. After encrypting the data, even if it is hacked or stolen, no one can access or read your data.

**Working**

When you send a message using an encrypted messaging service, this service converts the message into code. After this, only the right user can read this message. Digital encryption is highly complex, so it is difficult to crack.

### Encryption

In cryptography, encryption is a process in which the information is converted into a secret code called ciphertext. Ciphertext cannot be easily understood, only experts can understand it. The main purpose of encryption is to secure digital data or information, which transmit via the internet.

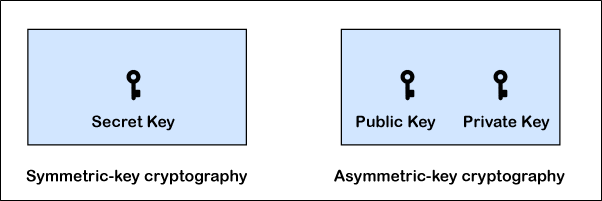
## 

### Decryption

Decryption is a process in which encrypted data is converted back to original data. The encrypted data is called ciphertext, and the original data is called plain text, and the conversion of ciphertext to plain text is called decryption.

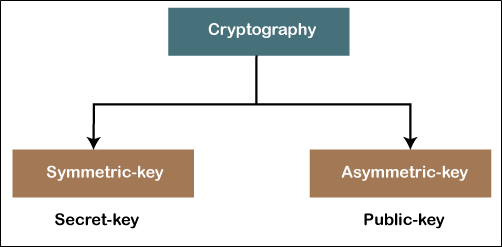
### Types of Keys

There are used three different types of the key in cryptography: a secret key, public key, and private key. The secret key is used in the symmetric-key cryptography, and the other two keys is used in the asymmetric key cryptography, as shown in the figure.



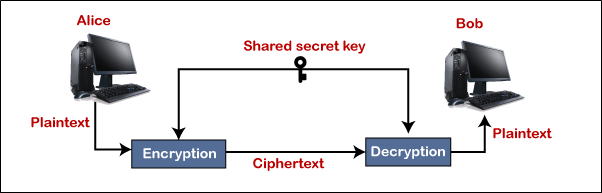
There are two types of cryptography

1. Symmetric key cryptography
2. Asymmetric key cryptography



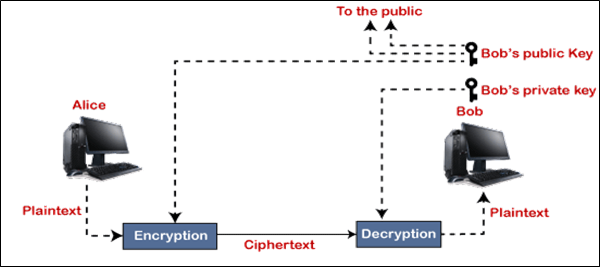
### Symmetric key cryptography

Symmetric key cryptography is that cryptography in which the same key (only one key) is used for encryption of plain text and decryption of ciphertext. Symmetric key cryptography is also known as secret-key cryptography.



### Asymmetric key cryptography

Asymmetric key cryptography is that cryptography in which both encryption and decryption have different keys. In this, the public key is used to do encryption, and the private key is used to do the decryption. It is also called public-key cryptography.



**For example**, if Paul sends a message to bob, they will use the bob's public key to encrypt the message, and then bob will decrypt that message with their private key.