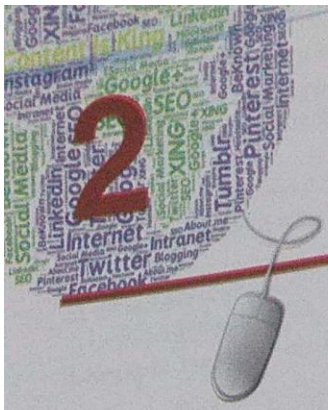


Internet Protocols

INTRODUCTION

The internet relies on millions of computers all over the world communicating with each other. These computers might run different software, hardware and operating systems. Protocols are set of rules that determine how information is sent.

INTERNET PROTOCOLS

A **protocol** is a set of rules governing how things work in a certain technology so that is some kind of standardization. In another words, it is a set of rules that checks the communication between two computers on a network. The most common protocol of **www.** is **HTTP** and HTTPS.

Definition

A **Protocol** is a set of rules that define how something is to be done.

- **HTTP (Hyper Text Transfer Protocol) :** A set of rules that supervises the flow of information on the Internet is called **Hyper Text Transfer Protocol**. When a web browser requests for an information, the request is served by an HTTP server or the web server. In another words, it is a protocol which is used to transfer and manage the links between one hypertext document and another on web. While surfing the net, we open a lot of web pages and other hypertext files containing text, images, animations, graphics, audio, videos etc. when the first part of a URL denotes http e.g. http://www.amazon.in.

Definition

HTTP (Hyper Text Transfer Protocol) is the set of rules for transferring hypertext (text, graphics, image, audio, video etc.) on www (World Wide Web).

- **HTTPS (Hyper Text Transfer Protocol Secure) :** It is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. The 's' at the end of HTTPS stands for secure. It means all communications between your browser and the website are encrypted.

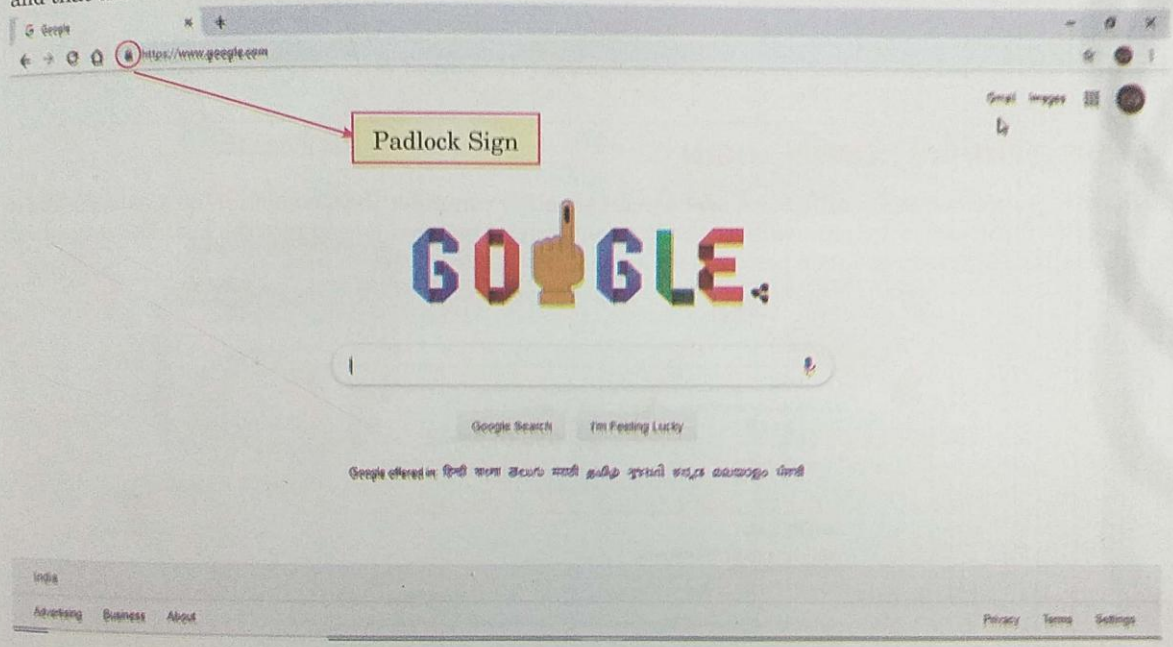
With regular HTTP protocol, the text/information being transferred flows from server to browser directly, without any encryption, which means it can be easily stolen. You can understand encryption as the

the actual text/information is converted into code words using a specific type of technology called SSL (Secure Sockets Layer).

The **SSL (Secure Sockets Layer)** helps to create a secure and encrypted connection between the server and the browser. This ensures that the information is safe/secure so that hackers cannot steal your sensitive information or data (such as Login Id and Password for online payments).

How to check if your connections is secure?

Before keying in any information or any website, make sure that the URL starts with the word "HTTPS" and that there is a Padlock Sign (🔒) on the navigation bar of your browser as shown below :



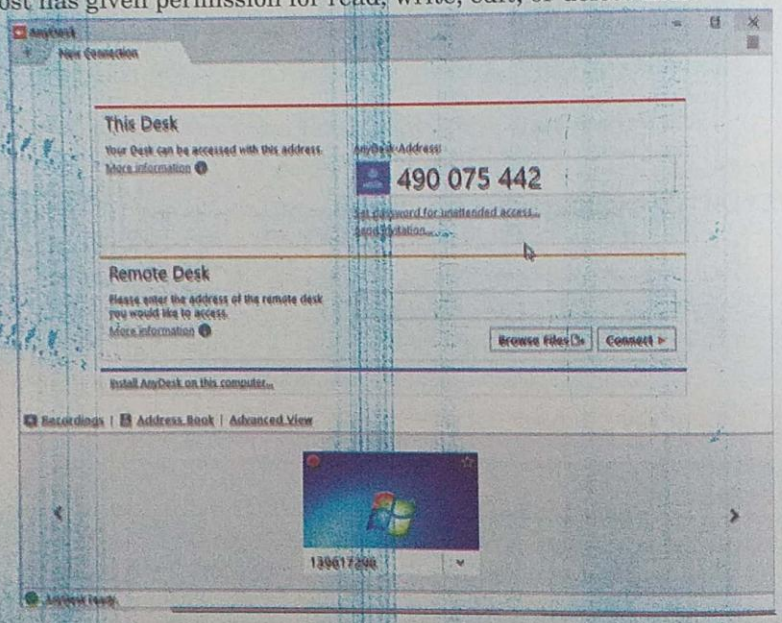
DIFFERENCE BETWEEN HTTP AND HTTPS PROTOCOLS

S.No.	HTTP	HTTPS
1.	It is a system for transferring information over the Internet without any security.	It is a system for transferring information with SSL (Secure Socket Layer) that encrypts and send information over a secure connection.
2.	HTTP URL begins with "http://".	HTTPS URL begins with "https://".
3.	HTTP is unsecured connection.	HTTPS is secured connection.
4.	It uses port 80 for communication by default.	It uses port 443 for communication by default.
5.	No Encryption is required.	Data Encryption is required before sending and Data Decryption is required after receiving the information.

6.	It is unreliable.	It is reliable.
7.	Stands for Hyper Text Transfer Protocol.	Stands for Hyper Text Transfer Protocol Secure.
8.	Helps to transfer text, audio, video, images through web pages.	Helps to transfer data securely via the network.
9.	It does not require any additional technology for data exchange or transfers.	It requires additional SSL certificate for secure exchange of data or information through secure connection.
10.	It is used for sending non-sensitive information.	It is used for transferring sensitive information.

UNDERSTANDING REMOTE LOGIN

Remote login access means authorized user can access other computer (host computer) on a network and to interact as if the user were physically at the host computer. Once you logged into the host, the user can do anything that the host has given permission for read, write, edit, or delete files.



HOW REMOTE LOGIN WORKS?

1. Remote Login will only work if the host computer is powered on, connected to the Internet and run into desktop sharing software.
2. Each time you open and run the desktop sharing software on the host computer, the software starts a new session. Each session has a particular login id and password that are required to remotely log into the host computer.
3. Once you are logged in, both computers will communicate with each other over a secure desktop sharing network. Access to this network can be force or subscription-based dependig on the service. While

connected you will have access to keyboard controls, mouse controls, all softwares, all files and all folders on the host machine.

4. For security purposes, all packets of information that are sent over the network will be typically encrypted on each end of **Secure Shell (SSH)**. For added security, no session Id's and passwords are stored on desktop sharing servers, they are automatically generated by the host machine.

Some popular Remote access software :

Team Viewer

Desktop Now

Chrome Remote Desktop

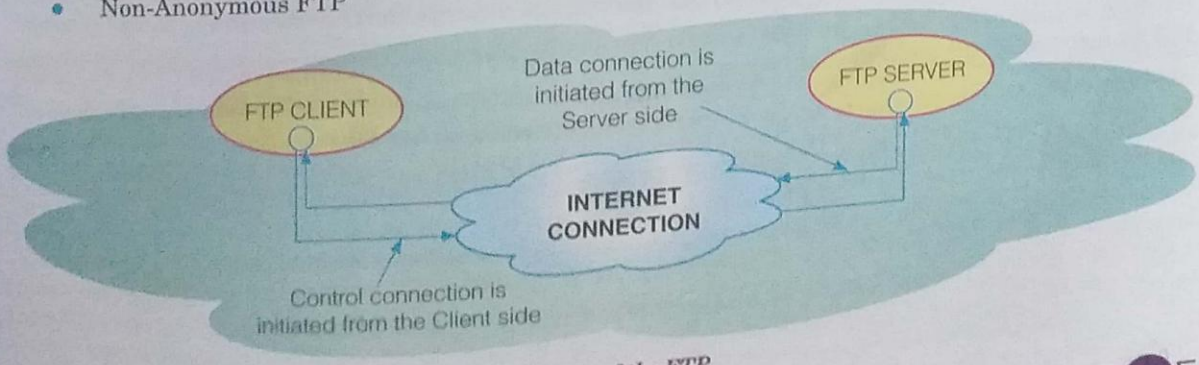
Any Desk

FTP PROTOCOL

The most popular use of the Internet is getting files transferred from one computer to another. The files can be graphics, sound files, or text files. Most of these files are downloaded using a protocol which is File Transfer Protocol, popularly known as **FTP**. It is a standard network protocol used to upload files from one computer to another. **FTP** address resembles like **HTTP** except that instead of **http://, it uses ftp://**.

There are two types of FTP connections available on the Internet :

- Anonymous FTP
- Non-Anonymous FTP



Working of the FTP

FTP or File Transfer Protocol is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol. TCP/IP is a main protocol used for communications over Internet and Intranet.

Definition

Intranet is a local communication network or a private network created using WWW (World Wide Web) software.

There are two computers involved in a FTP transfer :

1. FTP Server
2. FTP Client

1. **FTP Server :** The **FTP Server** is a computer that is running FTP Server Software. An FTP server listens on the network for connection requests from other computers.
2. **FTP Client :** The **FTP client** is a computer that is running FTP client software. An FTP client computer initiates a connection to the server. Once connected, the customer can do a number of file manipulation operations such as uploading files to the server, downloading files from the server, renaming or deleting files on the server.

There are many existing FTP client and server programs.

Some examples include :

Windows	WinSCP, FileZilla, Smart FTP
Mac OS	One Button FTP, Captain FTP
Linux	gFTP, FileZilla

TCP/IP (TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL)

TCP : (Transmission Control Protocol)

TCP/IP is the underlying communication language of the Internet that allows one computer to talk to another computer via Internet through packets of data and sending them to right location. These two protocols were developed in the early days of the Internet by the U.S. Military. The purpose was to allow computers to communicate over long distance networks. TCP/IP Software is in-built into all major Operating Systems such as Windows, MacOS, Unix, Linux etc.

In another words, it is the most important protocol. **TCP** establishes a connection between computers to facilitate communication. It breaks message into smaller packets that are transmitted over the Internet and also reassembles these smaller packets into the original message that are received from the Internet.

TCP is responsible for breaking data down into small packets before they can be sent over a network and for assembling the packets again when they arrive.

IP (Internet Protocol)

IP takes care of the communication between computers. It is responsible for addressing, sending and receiving the data packets over the Internet.

Definition

IP Address is a unique address that computing device use to identify itself and communicate with other devices in the Internet Protocol network. Any device connected to the IP network must have a unique IP address within its network.

In another words it handles the address part of each packet, so that the data is sent to the correct address. Each gateway on the network check this address to see where to forward the message.

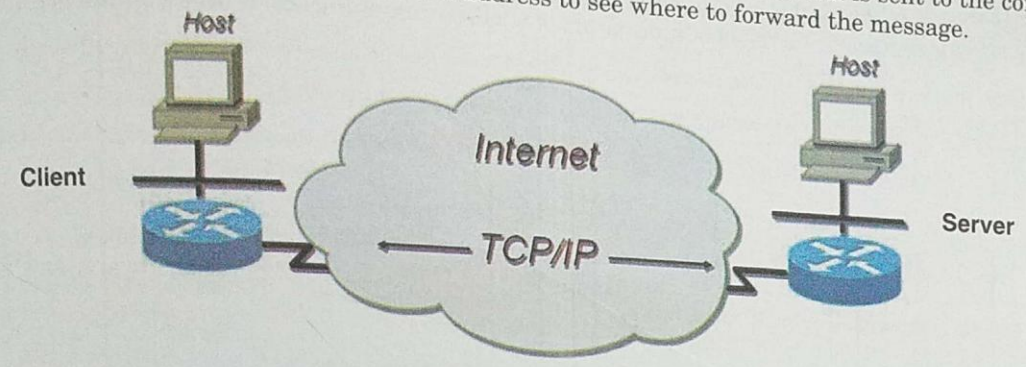


Diagram of TCP/IP

SSH (SECURE SHELL PROTOCOL)

SSH is remote logging protocol that logs into remote machine via a shell where all data between the client and server is encrypted. The SSH protocol is a protocol which facilitates secure communications between two systems using a client and server architecture and allowing users to log into server host system remotely.

SCP (SECURE COPY PROTOCOL)

SCP is a network protocol that allow to copy files between two servers or two connected machines over Internet. The **SCP protocol** allows you to transmit files from one machine to another over Internet with the encryption benefits of SSH. It offers own set of command options for secure copying of files across two connected machines over Internet.

SFTP (SECURE FILE TRANSFER PROTOCOL)

SFTP is a file transfer protocol but is secure contrary to unsecure FTP.

File Transfer Protocol is unsecure protocol and data/files travelling over FTP are not protected during a session. **SFTP (Secure File Transfer Protocol)** is a secure protocol for file transfer and it ensures security of data based on the secure shell protocol.

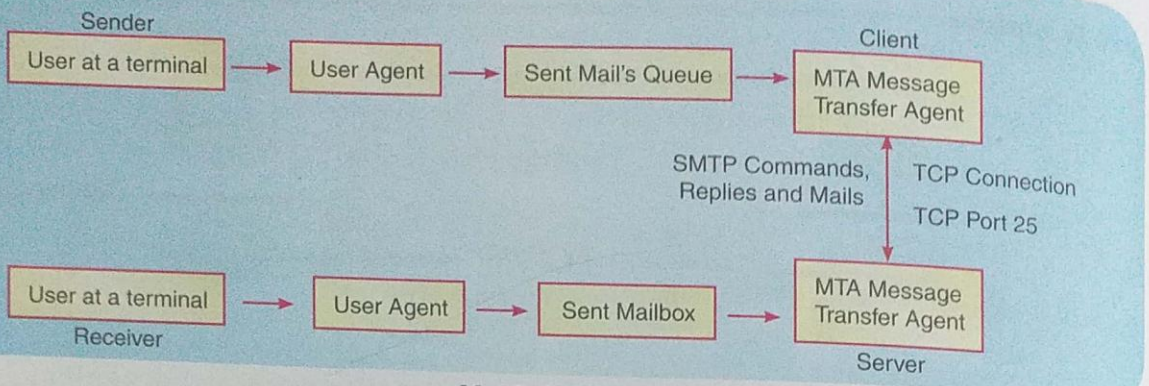
SFTP ensures data safety measures :

1. SFTP requires that the client must be authenticated by the server and the data transfer must take place over a secure channel (SSH).
2. All data is encrypted before being sent across the network.

SMTP (SIMPLE MAIL TRANSFER PROTOCOL)

The **SMTP** is a communication protocol for electronic mail transmission. As an Internet standard, SMTP was first defined in 1982 and updated in 2008. Mail servers and other message transfer agents use SMTP to send and receive mail messages. Proprietary Systems such as Microsoft Exchange and IBM Notes and Web Mail Systems such as outlook.com and gmail may use non-standard protocols internally, but all use SMTP when sending to or receiving email from outside their own systems. SMTP servers commonly use the transmission control protocol on port number 25. In another words, email is emerging as the one of the most valuable service in internet today. Most of the 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 mails at the

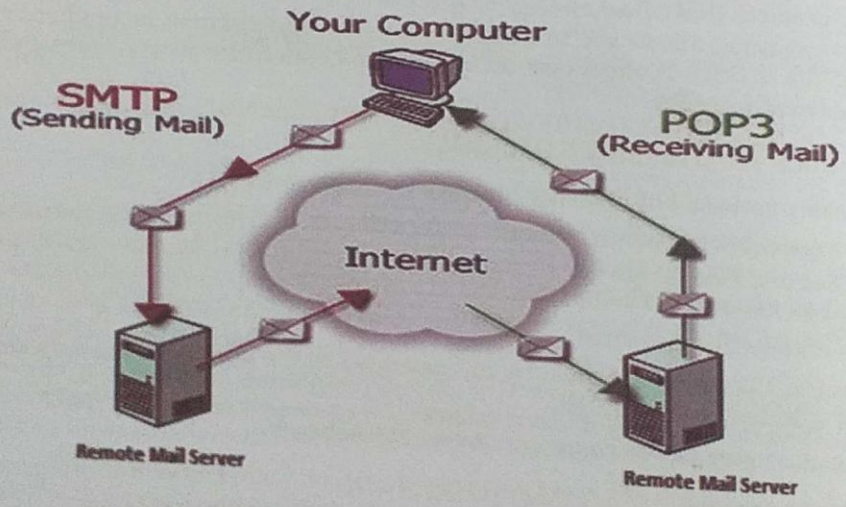
receiver's side.



Model of SMTP

POP3 (POST OFFICE PROTOCOL 3)

POP3 is the most recent version of a standard protocol for receiving e-mail. POP3 is a client or server protocol in which e-mail is received and held for you by your internet server. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail. This standard protocol is built into most popular e-mail products, such as Outlook Express. It is also built into the Netscape and Microsoft Internet Explorer browsers.



TELNET

Telnet is an older Internet utility that lets you log onto remote computer systems. Basically, a telnet program gives you a character-based terminal window on another system. You get a login prompt on that system. If you are permitted access, you can work on that system, just as would if you were sitting next to it.

Definition

TELNET is an Internet utility that lets you log onto remote computer systems.

Let's Summarize

- **Internet Protocol** is a communications protocol for computers connected to a network.
- **File Transfer Protocol (FTP)** means transferring a file from one computer to another over the Internet.
- **HTTP (HyperText Transfer Protocol)** is a protocol where web browsers and web servers communicate with each other over the Internet.
- The technique used by the Internet/Networking Protocols to send and receive the messages is called **Packet Switching techniques** in which data is sent/received in the forms of packets.
- **TCP (Transmission Control Protocol)** is responsible for breaking data down into small packets before they can be sent over a network and for assembling the packets again when they arrive.
- **IP Address (Internet Protocol Address)** is responsible for addressing, sending and receiving the data packets over the Internet.
- IP Address is a unique address that computing devices use to identify itself and communicate with other devices in the Internet network.
- **Usenet** is a collection of newsgroups where the users can post messages on different topics and these posted messages are distributed via usenet servers.
- **Secure Shell (SSH)** is a protocol which facilitates secure communications between two systems using a client/server architecture and allows user to log into server host system remotely.
- **Secure Copy Protocol (SCP)** is a file transfer protocol, which works on the Secure Shell (SSH) protocol technique that helps in transferring files securely from a local host to a remote host.
- Remote Login/Access means allowing authorized user to login/access other computers (host) on a network and internet as if the user is physically hosting his computer.
- E-mail or Electronic Mail is the transmission of messages over electronic networks like the internet.
- **Blog** is a piece of software or website which allows you to write an online diary on a website. Your last entry called a **post** is displayed on the front page i.e., home page of the site.
- **Newsgroup** is a place on the Internet where people can talk about a particular subject by reading and leaving messages.

QUESTIONS WITH THEIR SOLUTIONS

Fill in the Blanks

1. A term used when an authorized user has access to other computer is ..... .
2. Give an example of any popular newsgroup is ..... .
3. The another name of FTP software is ..... .
4. A protocol that facilitates secure communications between two systems is ..... .
5. A network protocol used on the Internet or local area network (LAN) connections to provide a bidirectional interactive communication facility is ..... .
6. The protocol responsible for downloading and uploading files from the web server is ..... .
7. The protocol used by web server to allow web pages to be shown in a web browser is ..... .

8. A number that uniquely identifies each computer or device connected to the internet is ..... .
9. A type of blog created for business purpose is ..... .
10. A type of blog which is developed by a user for his/her personal use is ..... .

Answer— 1. Remote Login 2. Easy news 3. Client
4. SSH (Secure Shell) 5. TELNET 6. FTP (File Transfer Protocol)
7. HTTP (Hyper Text Transfer Protocol)
8. IP Address (Internet Protocol) 9. Corporate Blog 10. Personal Blog

State True (T) or False (F)

1. It is compulsory to mention a http:// is the beginning of the domain address. ( )
2. Remote login will also work if the power of the host computer is off. ( )
3. E-mail is a fast, economic and reliable mode of communication. ( )
4. TCP/IP protocols are the built-in protocols of only MS-Windows Operating System. ( )
5. Chrome Remote Desktop Software needs Google Chrome web browser at the both ends. ( )

Answer— 1. (F) 2. (F) 3. (T) 4. (F) 5. (T)

Multiple Choice Questions

1. These two protocols were developed in the early days of the Internet by the U.S. Military.
   (a) TCP/IP (b) FTP
   (c) Telnet (d) SMTP
2. This internet service connects you to a news server on the Internet.
   (a) E-mail (b) Blog
   (c) Newsgroup (d) E-Group
3. A set of rules governing how things work in internet so that there is some kind of standardization.
   (a) Internet Laws
   (b) Internet Protocols
   (c) Internet Rules
   (d) Web Protocols
4. The prefix used in the beginning of the web address.
   (a) http://
   (b) www://
   (c) ftp://
5. Which of these symbols separate the two parts of an E-mail address :
   (a) $ (b) *
   (c) @ (d) &

Answer— 1. (a) 2. (c) 3. (b) 4. (a) 5. (c)

Write the full form of following abbreviations :

(a) TCP .....

(b) IP .....

(c) HTTP .....

(d) SCP .....

(e) SSH .....

(f) FTP .....

(g) TELNET .....

(h) HTTPS .....

(i) E-mail .....

(j) LAN .....

Answer— **(a)** Transmission Control Protocol **(b)** Internet Protocol
(c) Hyper Text Transfer Protocol **(d)** Secure Copy Protocol
(e) Secure Shell Protocol **(f)** File Transfer Protocol
(g) Telecommunication Network **(h)** Hyper Text Transfer Protocol Secure.
(i) Electronic Mail **(j)** Local Area Network.

Theoretical Questions

Q.1. Why SFTP preferred over FTP while exchanging sensitive data?

Ans. The major reason for implementing SFTP versus FTP is security. FTP is not even remotely secure. During an FTP session, your username and password are transmitted in clear text. If someone is eavesdropping, it is not difficult for them to log your FTP username and password.

In FTP all data is passed back and between the client and server without the use of encryption. This makes it possible for an eavesdropper to listen in and retrieve your confidential information including login details. With SFTP all the data is encrypted before it is sent across the network.

SFTP is not the same as FTP. The later implement of original FTP protocol through a separately created secure tunnel using SSH (Secure Shell).

Q.2. What do you understand by the term 'Internet Protocols'?

Ans. A protocol is a set of rules governing how things work in a certain technology so that is some kind of standardization.

Q.3. Difference between HTTP and HTTPS protocols.

Ans.

S.No.	HTTP	HTTPS
1.	It is a system for transferring information over the Internet without any security.	It is a system for transferring information with SSL (Secure Socket Layer) that encrypts and send information over a secure connection.

S.No.	HTTP	HTTPS
2.	HTTP stands for Hyper Text Transfer Protocol.	HTTPS stands for Hyper Text Transfer Protocol Secure.
3.	It is unreliable.	It is reliable.
4.	HTTP is unsecure connection.	HTTPS is secure connection.
5.	It is useful for sending non-sensitive information.	It is useful for sending sensitive information.

Q.4. Define Remote Login.

Ans. Remote Login Access means authorized user can access other computer (host computer) on a network and to interact as if the user were physically at the host computer. Once you logged into the host, the user can do anything that the host has given permission for Read, Write, Edit or Delete files.

Q.5. What is SCP (Secure Copy Protocol)?

Ans. SCP are protocol that allow to copy files between two servers or two connected machines over Internet. The SCP Protocol allows you to transmit files from one machine to another over Internet with the encryption benefits of SSH. It offers own set of command options for secure copying of files across two connected machines over Internet.