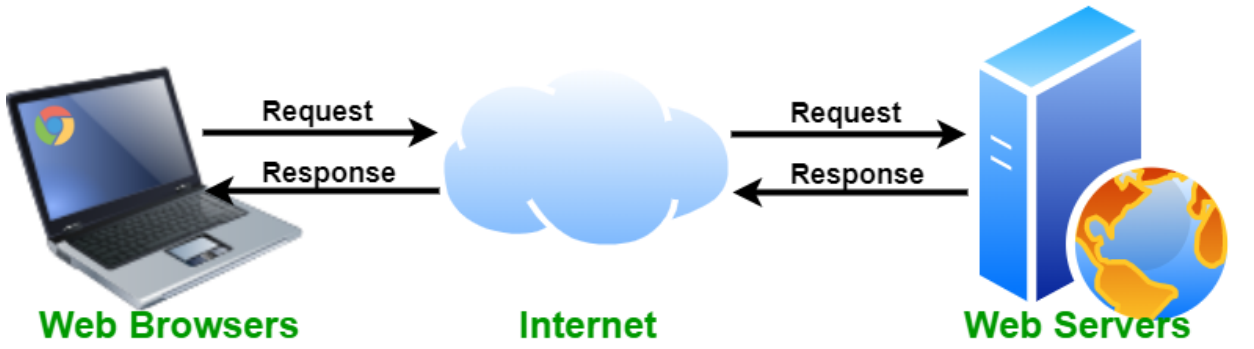
Web Server

A web server is a computer program that distributes web pages as they are requisitioned. The basic objective of the web server is to store, process and deliver web pages to the users. This intercommunication is done using Hypertext Transfer Protocol (HTTP). These web pages are mostly static content that includes HTML documents, images, style sheets, test etc. Apart from HTTP, a web server also supports SMTP (Simple Mail transfer Protocol) and FTP (File Transfer Protocol) protocol for emailing and for file transfer and storage.
he Web Server is requested to present the content website to the user's browser. All websites on the Internet have a unique identifier in terms of an IP address. This Internet Protocol address is used to communicate between different servers across the Internet.



Generally, web servers are used by web hosting companies and professional web app developers. But, actually anyone who satisfies one of the below category can use it-

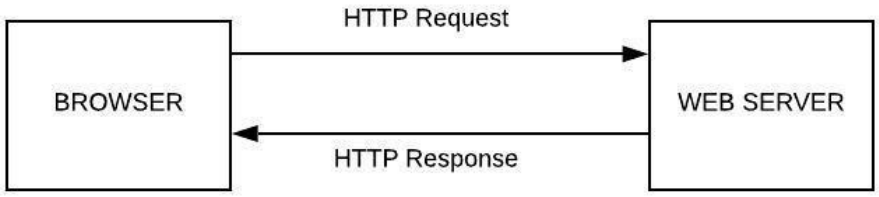
- One who owns a website (to make the local copy on their system resemble what is on internet).
- One who wants to use server-side technologies, such as, PHP or ColdFusion, can also use the web server.

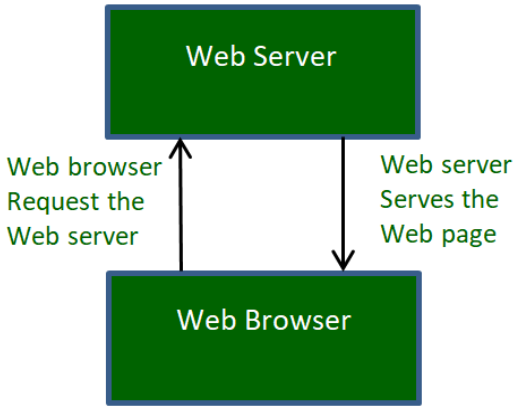
Examples: Apache Web Server, IIS Web Server, Nginx Web Server, LiteSpeed Web Server, Apache Tomcat, Node. js, Lighttpd.

How Web servers work?

A page on internet can be viewed, when the browser requests it from the web server and the web server responds with that page. A simple diagrammatic representation of this is as given below in the figure:

By: Pragya Singh Tomar
ICS, Vikram University, Ujjian





Simple process consists of 4 steps, they are:

1. **Obtaining the IP Address from domain name:** Our web browser first obtains the IP address the domain name (for e.g., for this page the domain name is www.geeksforgeeks.org) resolves to. It can obtain the IP address in 2 ways-
    - By searching in its cache.
    - By requesting one or more DNS (Domain Name System) Servers.

    Note: Any website is assigned an IP address when it is first created on web server.

2. **Browser requests the full URL** : After knowing the IP Address, the browser now demands a full URL from the web server.
3. **Web server responds to request:** The web server responds to the browser by sending the desired pages, and in case, the pages do not exist or some other error occurs, it will send the appropriate error message.

By: Pragya Singh Tomar
ICS, Vikram University, Ujjian

Essential Features : Authentication, Authorization, and Encryption

Authentication

- Authentication is used by a server when the server needs to know exactly who is accessing their information or site.
- Authentication is used by a client when the client needs to know that the server is system it claims to be.
- In authentication, the user or computer has to prove its identity to the server or client.
- Usually, authentication by a server entails the use of a user name and password. Other ways to authenticate can be through cards, retina scans, voice recognition, and fingerprints.
- Authentication by a client usually involves the server giving a certificate to the client in which a trusted third party states that the server belongs to the entity that the client expects it to.
- Authentication does not determine what tasks the individual can do or what files the individual can see. Authentication merely identifies and verifies who the person or system is.

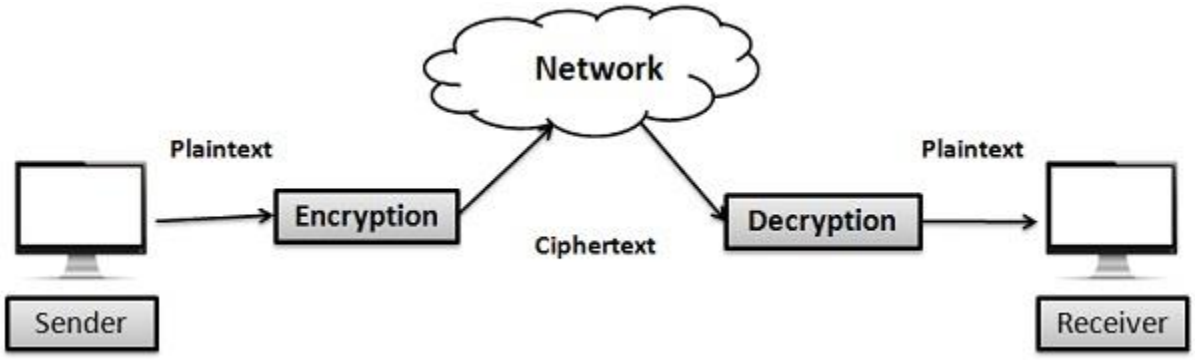
Authorization

- Authorization is a process by which a server determines if the client has permission to use a resource or access a file.
- Authorization is usually coupled with authentication so that the server has some concept of who the client is that is requesting access.
- The type of authentication required for authorization may vary; passwords may be required in some cases but not in others.
- In some cases, there is no authorization; any user may be use a resource or access a file simply by asking for it. Most of the web pages on the Internet require no authentication or authorization.

Encryption

- Network encryption is the process of encrypting or encoding data and messages transmitted or communicated over a computer network.
- It is a broad process that includes various tools, techniques and standards to ensure that the messages are unreadable when in transit between two or more network nodes.

By: Pragya Singh Tomar
ICS, Vikram University, Ujjian



- Encryption involves the process of transforming data so that it is unreadable by anyone who does not have a decryption key.
- By encrypting the data exchanged between the client and server information like social security numbers, credit card numbers, and home addresses can be sent over the Internet with less risk of being intercepted during transit.

The sender requires an encryption algorithm and a key to transform the **plaintext** (original message) into a **ciphertext** (encrypted message), it's also known as enciphering.

Plaintext is the data that need to be protected during transmission. The ciphertext is the scrambled text produced as an outcome of the encryption algorithm for which a specific key is used. The ciphertext is not shielded. It flows on the transmission channel. The encryption algorithm is a cryptographic algorithm that inputs plain text and an encryption key and produces a ciphertext.

In conventional encryption methods, the encryption and decryption keys are same and secret. Conventional methods are broadly divided into two classes: Character level encryption and Bit level Encryption.

- **Character-level Encryption:** In this method, encryption is performed at the character level. There are two common strategies for character-level encryption are substitutional and Transpositional.
- **Bit- level Encryption:** In this technique, firstly data (such as text, graphics, audio, video, etc.) is divided into blocks of bits, then modified by encoding/ decoding, permutation, substitution, exclusive OR, rotation, and so on.

Definition of Decryption

Decryption inverts the encryption process in order to convert the message back to its real form. The receiver uses a decryption algorithm and a key to transform the ciphertext back to original plaintext, it is also known as deciphering.

By: Pragya Singh Tomar
ICS, Vikram University, Ujjian

A mathematical process utilized for decryption that generates original plaintext as an outcome of any given ciphertext and decryption key is known as Decryption algorithm. This process is the reverse process of the encryption algorithm.

The keys used for encryption and decryption could be similar and dissimilar depending on the type of cryptosystems used (i.e., **Symmetric key** encryption and **Asymmetric key** encryption).

Key Differences Between Encryption and Decryption

1. The encryption algorithm uses message (plaintext) and the key at the time of encryption process. On the other hand, in the process of decryption, the decryption algorithm converts the scrambled form of the message (i.e., ciphertext)with the help of a key.
2. Encryption takes place at the sender's end whereas decryption takes place at the receiver's end.
3. The major function of Encryption is to convert plaintext in the ciphertext. As against, decryption transforms ciphertext into plaintext.

Examples Using Authentication, Authorization, and Encryption

Authentication, authorization, and encryption are used in every day life. One example in which authorization, authentication, and encryption are all used is booking and taking an airplane flight.

- Encryption is used when a person buys their ticket online at one of the many sites that advertises cheap ticket. Upon finding the perfect flight at an ideal price, a person goes to buy the ticket. Encryption is used to protect a person's credit card and personal information when it is sent over the Internet to the airline. The company encrypts the customer's data so that it will be safer from interception in transit.
- Authentication is used when a traveler shows his or her ticket and driver's license at the airport so he or she can check his or her bags and receive a boarding pass. Airports need to authenticate that the person is who he or she says she is and has purchased a ticket, before giving him or her a boarding pass.
- Authorization is used when a person shows his or her boarding pass to the flight attendant so he or she can board the specific plane he or she is supposed to be flying on. A flight attendant must authorize a person so that person can then see the inside of the plane and use the resources the plane has to fly from one place to the next.
- Authentication and Authorization are often used together. For example, students at University are required to authenticate before accessing the Student Link. The authentication they provide determines what data they are authorized to see. The authorization step prevents students from seeing data of other students.

By: Pragya Singh Tomar
ICS, Vikram University, Ujjian