1. How does HTTPS work behind the scene?

Https is a secure version of Http which is the primary protocol used to send data between web browsers and a website.Https is encrypted in order to increase the security of data transfer.

Https uses an encryption protocol to encrypt communication. Protocol is called TLS(Transport layer security),and secures the communication by using an asymmetric public key infrastructure.

There is two key Public and the private key:-

Private key: Lives on a web browser and decrypts the information encrypted by the public key.

Public Key: It is public to anyone who wants to interact with the server and encrypt the information and convert it into the cipher text with the help of a session layer and transferred over the browser.

When we use the same key for transmission on both ends it’s called symmetric encryption.

But it becomes more complicated to website on the public internet because we don't control the other end's connection.

And in asymmetric connection you used different keys.

Steps:

1) our browser reaches out to the website server and requests a connection.

2) The server sends the public key and keeps it a private key secret.

3) The browser generates a third key called session key.

4) The session key is encrypted by our computer using the public key we got from the server.

5) Encrypted session key then shared with the server .

6) Server decrypts the session key using its private key.

7) The public key encryption is terminated and replaced with symmetric encryption. And now we are in the session with the server and that's how it remains until we leave the website.

2. What are the different https methods available and what are they exactly?

3. Understand and explain the use of various http response codes?

4. What are the different web communications protocols and their use cases?

1) Transmission control protocol: TCP is a communication protocol which is used for communicating over the internet.TCP establishes a connection between a source and its destination, which it ensures remains live until communication begins and then it divides any message into a series of packages and sent from one source to the designation.

2) User Datagram protocol: UDP is a suitable communication protocol to the transmission Control Protocol implemented primarily for creating loss-tolerating and low-latency linking between different applications.

3) Post office protocol(POP): It is designed to receive the mails.it is a message access agent protocol work for SMTP. When the message is sent, then SMTP is used to deliver the message from the client to the server and then to the recipient server. But the message is sent from the recipient server to the actual server with the help of the Message Access Agent.

4) Simple mail transfer protocol(SMTP): It is also a communication protocol for web browsers.it is a protocol used to send the mail over the internet.

5) File transfer protocol(FTP): FTP is the file transmission protocol over a network that uses TCP. FTP allows our data to be transferred between two computers.TCP, or Transmission Control Protocol, is what makes FTP reliable; checking and ensuring that your data actually arrives at its destination.

6) Hyper text transfer protocol(HTTP): The Hypertext Transfer Protocol is [an application protocol](https://tools.ietf.org/html/rfc2616) for distributed, collaborative, hypermedia information systems that allows users to communicate data on the World Wide Web.

7) Hyper Text Transfer Protocol Secure (HTTPS): Hyper Text Transfer Protocol Secure is a standard protocol to secure the communication among two computers one using the browser and other fetching data from a web server. HTTPS is used for transferring data between the client browser and the web server in the hypertext format.it uses the encryption method with the help of public and private keys.

5) Pros and cons of single page and multipage application:

**Multi Page application**: Multi-page applications are the traditional web applications that reload the entire page and display the new one when a user interacts with the web app and try to exchange data each time a new page is created.

**Pros of MPA**:

Multi-page applications are more SEO-friendly in comparison with single-page solutions. Their content is being constantly updated.

There are almost no restrictions on the number of pages to add to the existing application. Single-page applications don’t have such privileges as they are limited to the amount of content.

There are almost no restrictions on the number of pages to add to the existing application. Single-page applications don’t have such privileges as they are limited to the amount of content.

**Cons of MPA**:

Since multi-page applications have a higher number of features compared to single-page solutions, their creation requires more effort and resources.

The development time increases in proportion to the number of pages to be built and the functionality to be implemented.

The content in multi-page applications is constantly reloaded which increases the load on your servers. This can affect web page speed and overall system performance in a negative way.

Maintaining security may be problematic because developers need to secure each separate page. Single-page apps allow developers to just secure data endpoints.

**Single Page applications:**

A single-page application works in the browser and requires no page reloads and no extra time for waiting. The page doesn’t need to be updated since content is downloaded automatically.

**Pros of SPA:**

Since single-page applications don’t update the entire page but only require content, they significantly improve a website’s speed.

A single-page can cache any local data effectively. An SPA sends only one request to a server and then stores all the data it receives.

SPAs provide users with a simple linear experience.

The development is simplified and streamlined. There is no need to write code to render pages on the server.

**Cons of SPA:**

It is very tricky and not an easy task to make SEO optimization of a Single-Page Application.

An SPA doesn’t save visitors from jumping between states. This means that when users click the back button, they won’t go back. A browser only takes users to the previous page.

Automated security scans can have difficulty discovering links when your entire page is built dynamically by a SPA framework.

SPAs require a lot of resources from the browser since the browser is doing most of the tasks for the SPAs.

6. What is TCP ,Why do we use TCP, How does it work?

**TCP(Transmission control protocol):**

TCP is a communications standard protocol that enables application programs and computing devices to exchange messages over a network. It is designed to send packets across the internet and ensure the successful delivery of data and messages over networks.

TCP organizes data so that it can be transmitted between a server and a client. It guarantees the integrity of the data being communicated over a network. Before it transmits data, TCP establishes a connection between a source and its destination, which it ensures remains alive until communication begins.

**WHY:**

TCP helps you to determine how a specific computer should be connected to the internet and how data should be transmitted between them. It helps you to create a virtual network when multiple computer networks are connected together**.**

**How does it work:**

TCP provides communication between an application program and the Internet Protocol.TCP allows for transmission of information in both directions. This means that computer systems that communicate over TCP can send and receive data at the same time.

The TCP protocol uses segments (packets) as the basic units of data transmission.It divides the whole message into the segment and sends over the internet to the receiving end.

TCP divides a stream of data into chunks, and then adds a TCP header to each chunk to create a TCP segment. A TCP segment consists of a header and a data section. The TCP header contains 10 mandatory fields, and an optional extension field. The payload data follows the header and contains the data for the application.and send these chunks over the internet after the connection being made between the two ends.

7. Peer-2-Peer real life example?

**P2p:** A peer-to-peer network allows computer hardware and software to communicate without the need for a server. Unlike client-server architecture, there is no central server for processing requests in a P2P architecture. The peers directly interact with one another without the requirement of a central server. Both the systems in p2p work as client and server.Both can send and receive data from each other and are directly connected to each other without any intermediate server.

**Example:**