**Q1.Diffrence Between HTTP and HTTPS ?**

The most important difference between HTTP and HTTPS is the presence of an additional layer of security provided by HTTPS. Here's a breakdown of the key differences:

1. Security: HTTP (Hypertext Transfer Protocol) is not secure, meaning the data exchanged between a web server and a browser is sent in plain text. This makes it vulnerable to interception and manipulation by attackers. On the other hand, HTTPS (Hypertext Transfer Protocol Secure) uses encryption to secure the communication channel, ensuring that the data transmitted between the server and the browser is encrypted and cannot be easily accessed or modified by unauthorized parties.

2. Encryption: HTTP does not provide any encryption, whereas HTTPS uses SSL (Secure Sockets Layer) or TLS (Transport Layer Security) protocols to encrypt the data. This encryption helps protect sensitive information, such as login credentials, credit card numbers, and other personal data, from being intercepted and read by hackers.

3. Authentication: HTTPS includes an authentication component that verifies the identity of the website or server you are connecting to. This is done through SSL/TLS certificates issued by trusted Certificate Authorities (CAs). These certificates validate the authenticity of the website, ensuring that you are connecting to the intended server and not an impostor. In contrast, HTTP does not offer such authentication, leaving it susceptible to spoofing and man-in-the-middle attacks.

4. Port: HTTP typically uses port 80 for communication, while HTTPS typically uses port 443. This port difference helps servers distinguish between regular HTTP and secure HTTPS connections.

Overall, the switch from HTTP to HTTPS provides a more secure and trustworthy browsing experience, safeguarding the confidentiality, integrity, and authenticity of data transmitted between the server and the client. It has become increasingly important for websites, particularly those handling sensitive user information, to adopt HTTPS as the standard protocol.

**Q2. What are the difference between Cookies and cache ?**

Cookies are small text files that are stored on a user's device (such as a computer or smartphone) by websites they visit. These files contain data that can be accessed by the website or other websites that recognize the cookie. Cookies serve various purposes and are commonly used to enhance the browsing experience and provide personalized content.

Here are some key points about cookies:

1. Purpose: Cookies serve different functions. They can remember user preferences, such as language settings or font size, to provide a customized experience. Cookies can also store login information, allowing users to stay logged in across multiple sessions. Additionally, they enable websites to track user behavior and gather information for analytics and marketing purposes.

2. Types of Cookies: There are different types of cookies with varying lifespans and functionalities. Some common types include:

- Session Cookies: These cookies are temporary and are deleted once the user closes the browser or session. They enable websites to remember user actions within a browsing session.

- Persistent Cookies: These cookies remain on the user's device even after closing the browser or session. They have an expiration date and are used to remember user preferences or login information for future visits.

- First-party Cookies: These cookies are set by the website domain that the user is visiting. They are commonly used for functional purposes, such as remembering user preferences.

- Third-party Cookies: These cookies are set by domains other than the website being visited. They are often used for tracking and advertising purposes.

3. Privacy Considerations: While cookies are generally harmless and essential for many website functionalities, they can raise privacy concerns. Some third-party cookies, especially those used for tracking and targeted advertising, have raised debates about user privacy. As a result, many browsers offer options to control cookie settings and allow users to block or delete specific cookies.

It's important to note that my knowledge is based on information available up until September 2021, and there may have been advancements or changes in cookie technology since then.

Cache refers to a high-speed data storage mechanism used to store frequently accessed data or information in a location that can be accessed more quickly than fetching it from its original source. In computing, cache is used to improve the performance and efficiency of data retrieval.

Here are some key points about cache:

1. Purpose: The main purpose of a cache is to reduce the time and resources required to access data. By storing frequently accessed data closer to the processor or user, cache minimizes the need to retrieve the data from its original, slower source, such as a hard drive or the internet.

2. Functionality: When a system or application needs to access data, it first checks the cache to see if the data is already stored there. If the data is found in the cache (cache hit), it can be retrieved much faster than if it had to be fetched from the original source. This speeds up the overall performance of the system.

3. Cache Hierarchy: Caches are often organized in a hierarchy with multiple levels, each serving as a faster but smaller storage. The closer a cache level is to the processor or user, the faster it can deliver data. The hierarchy typically consists of multiple levels, such as L1 (level 1), L2, and sometimes L3 caches in computer processors.

4. Cache Coherency: In systems with multiple processors or cores, cache coherency ensures that all caches have a consistent view of shared data. It ensures that when one processor modifies data stored in its cache, other processors accessing the same data get the updated version. This maintains data integrity across multiple caches.

5. Web Browser Cache: Web browsers use a cache to store web page elements, such as HTML, images, CSS files, and scripts, locally on a user's device. This allows subsequent visits to the same website to load faster since the browser can retrieve some elements from the cache instead of downloading them again from the web server.

6. Clearing Cache: Clearing the cache is the process of deleting the stored data from the cache. It can be done to free up storage space, resolve caching issues, or ensure that the most up-to-date version of a website or application is loaded.

Caching plays a vital role in improving system performance by reducing data retrieval time and optimizing resource utilization. It is widely used in various computing systems, including CPUs, web browsers, databases, and content delivery networks (CDNs).