# SECURE SOCKET LAYER(SSL)

- SSL provides a secure communication between the Web Browser and Server.

- SSL is widely used in Websites, Mobile apps, Messaging etc.

- For example, when you are searching a particular site on the internet you can see some sites with 'http' or 'https' visible in the URL.

- The difference between them is ' s ', s stands for security, any website with https web address uses SSL.

- It transfers your information by encrypting the data so it provides you privacy for the data.

- When you access the internet for communication, the information is transferred on both sides in this case SSL is used.
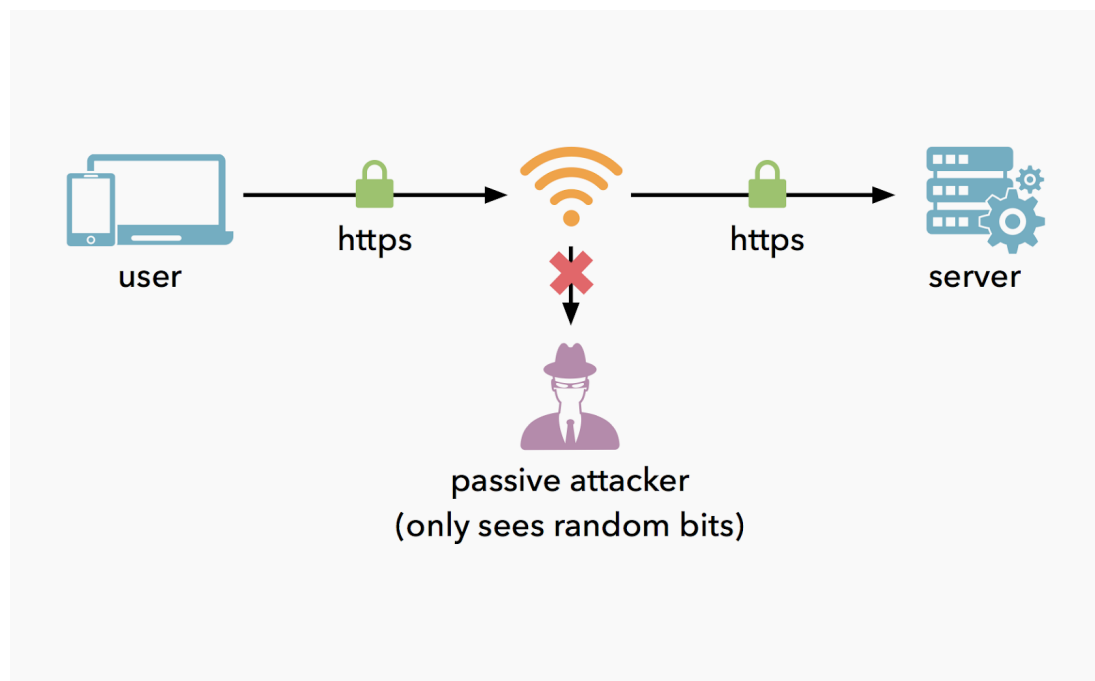
SSL CERTIFICATE

- SSL certificates are what enable websites to move from HTTP to HTTPS,which is more secure.

How SSL certificate works

- Browser connects to a web server (website) secured with SSL (https). Browser requests that the server identify itself.

- Server sends a copy of its SSL Certificate including the server's public key

- If the browser verifies the certificate, it creates, encrypts, and sends back a symmetric session key using the server's public key. Server decrypts the symmetric session key using its private key and sends back an acknowledgement encrypted with the session key to start the encrypted session.

- **Server** and **Browser** now encrypt all transmitted data with the session key.