HyperText Transfer Protocol (HTTP is a protocol using which hypertext is transferred over the Web. Due to its simplicity, http has been the most widely used protocol for data transfer over the Web but the data (i.e. hypertext) exchanged using http isn’t as secure as we would like it to be. In fact, hyper-text exchanged using http goes as plain text i.e. anyone between the browser and server can read it relatively easy if one intercepts this exchange of data. But why do we need this security over the Web? Think of ‘Online shopping’ at Amazon or Flipkart. You might have noticed that as soon as we click on the Check-out on these online shopping portals, the address bar gets changed to use https. This is done so that the subsequent data transfer (i.e. financial transaction etc.) is made secure. And that’s why https was introduced so that a secure session is setup first between Server and Browser. In fact, cryptographic protocols such as SSL and/or TLS turn http into https i.e. https = http + cryptographic protocols. Also, to achieve this security in https, Public Key Infrastructure (PKI) is used because public keys can be used by several Web Browsers while private key can be used by the Web Server of that particular website. The distribution of these public keys is done via Certificates which are maintained by the Browser. You can check these certificates in your Browser settings.

**Difference between HTTP and HTTPS**

* In HTTP, URL begins with “http://” whereas URL starts with “https://”
* HTTP uses port number 80 for communication and HTTPS uses 443
* HTTP is considered to be unsecure and HTTPS is secure
* HTTP Works at Application Layer and HTTPS works at Transport Layer
* In HTTP, Encryption is absent and Encryption is present in HTTPS as discussed above
* HTTP does not require any certificates and HTTPS needs SSL Certificates