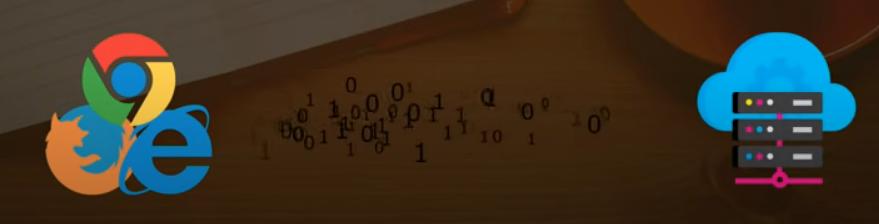
What is SSL?

SSL stands for **Secure Sockets Layer**

SSL is a technology that keeps internet connections secure. It encrypts and protects sensitive information and data as it’s sent between two systems (like your browser and another website or two servers). SSL stops bad people and bots from reading or changing the information being sent between the systems, like credit card information during an e-commerce transaction. In simple SSL is industry standard for secure client – server communication.



In most cases client will be web browser (Chrome, IE, Fire Fox) and server may be application server like web logic

SSL Capabilities:

1. **Encryption**: It encrypts the data that is been transferred between client and server. There are many encryption algorithms supported by SSL like RSA, DES, AES and so on. RSA is a most commonly used algorithm.
2. **Integrity**: Its responsible to maintain data integrity by making sure that its data is not getting tampered by its communication process. This data integrity is maintained by generating a digest using Hash function in this process client hashes the message and send the result which is called as digest to the server. On the server-side server also generates the digest using the same hash function and compares the resulting digest.

If the message is untampered then both the digest will be same. SHA1 is a commonly used hashed function in SSL and its practically impossible to generate identical digest for different messages.

1. **Authentication**: Finally, it is responsible to mutually authenticate client and server which prevents unintended data transfer. When the client initiates the SSL session server sends digital certificate signed by third party **Certificate Authority (CA)** to the client and the client verifies the trust or root certificate in the certificate chain. The third-party CA guarantees that certificate is valid. If the trust certificate is not in the browsers trust store or the certificate is expired then SSL communication will not happen and browser complains that the certificate is not valid and these are the three capabilities of SSL.

**Advantages to using SSL**

* Faster web page loading
  + HTTPS loads pages faster than HTTP. Who waits around for a webpage to load nowadays when there’s always a competitor around the digital corner whose site might be faster?
* [**SEO**](https://www.domain.com/blog/2019/06/21/a-guide-to-seo-basics-for-beginners/) Improvement: Your site is likely to rank higher in search results if you’re using HTTPS as opposed to HTTP.
* Stop hackers and bad actors in their tracks
  + SSL encrypts the data transferred back and forth between two systems. Even if these bad people and bots could somehow see the data being transferred, they won’t know what it says.
* Maintain PCI Compliance
  + PCI Compliance stands for Payment Card Industry Compliance. This is required by all credit card companies when making transactions online to further secure and protect against data and identity theft.
  + Part of the PCI Compliance guidelines are that your site must use HTTPS, which means your SSL certificate needs to be configured on your site before you can accept payments via credit card for purchases.
* No scary alerts
  + If you’re using HTTP then chances are your site visitors are receiving notices telling them your website isn’t secure when they land on it. Frankly, this looks bad. It causes them to lose confidence in your site and odds are good they won’t be back.