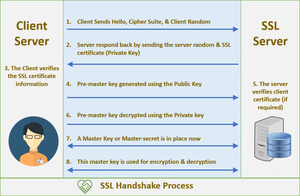
HTTPS:

The green lock means that the site has been issued a certificate and that a pair of cryptographic keyshas been generated for it. Such sites encrypt information transmitted between you and the site. In this case, the page URLs begin with HTTPS, with the last “S” standing for “Secure.”

Sure, encrypting transmitted data is a good thing. It means that information exchanged is safe and prevents MITM. However, its is important to point out that a secure connection and communication does not mean a safe site.

In order to send data to the server using HTTPS we need to add extra level of security.It is concerned with providing encrypted application layer packets. First TCP handshake takes place between client and server which helps to send http requests. However, http requests are plain texts and they are vulnerable to man in the middle attacks. So, we need to establish a secure session. This is achieved using SSL/TLS handshake.



1. The SSL or TLS client sends an initial hello message that contains cryptographic data, for example, the CipherSuites strengthened by the customer. The server has a pair of public and private keys.
2. The SSL or TLS server reacts with a server hello message that contains the CipherSuite picked by the server from the outline given by the customer, the session ID. The server additionally sends its SSL certificate.
3. The client verifies the SSL certificate of server using public CA or trusted cert store.
4. The client encrypts the message using the server's public key and then the server decrypts it using its own private key.
5. Then they come up with a shared secret and use that to have symmetric encryption further.
6. Symmetric is more efficient than asymmetric encryption.