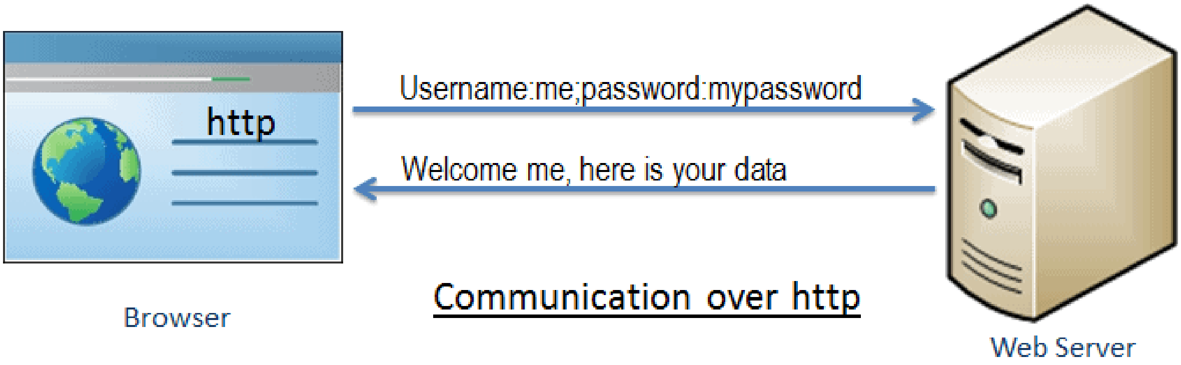
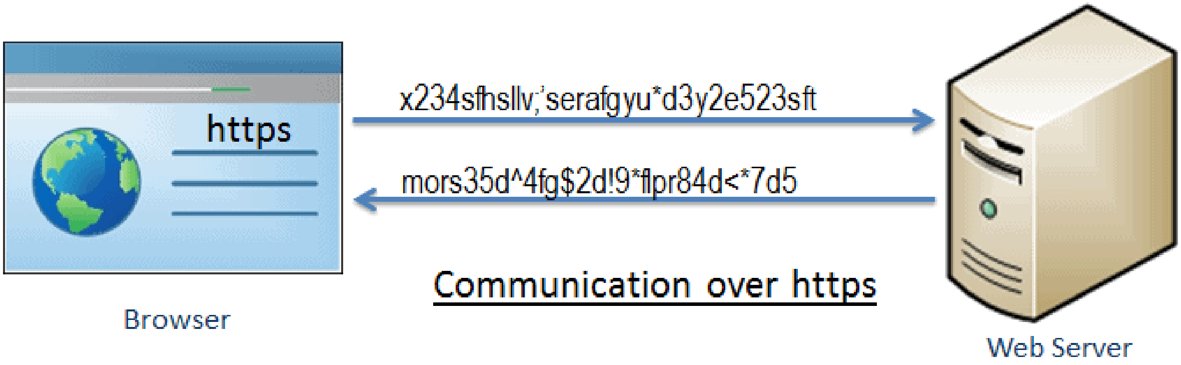
HTTPS stands for Hyper Text Transfer Protocol Secure. It is a protocol for securing the communication between two systems e.g. the browser and the web server.


http
Username:me;password:mypassword
Welcome me, here is your data
Browser
Communication over http
Web Server


https
x234sfhsllv;'serafgyu*d3y2e523sft
mors35d^4fg$2d!9*flpr84d<*7d5
Browser
Communication over https
Web Server

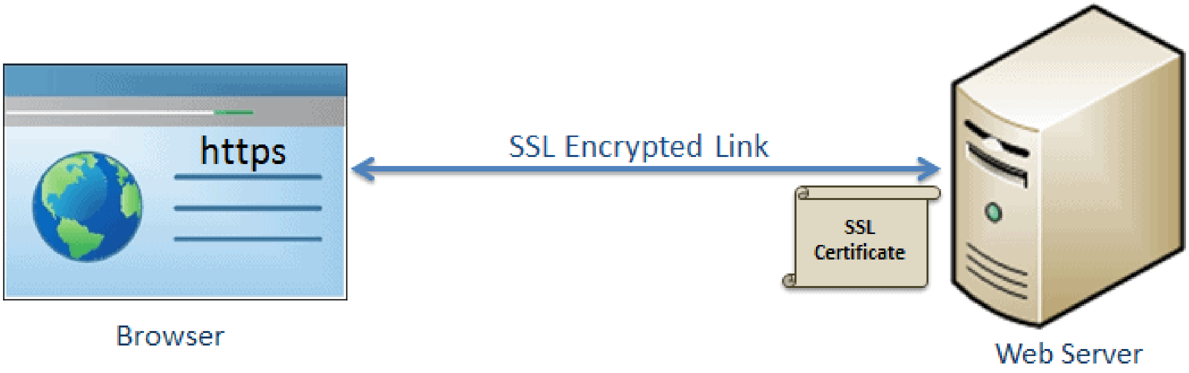
As you can see in the above figure transfers data between the browser and the web server in the hypertext format, whereas https transfers data in the encrypted format.

HTTPS established an encrypted link between the browser and the web server using the Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocols. TLS is the new version of SSL.

Secure Socket Layer (SSL)

SSL is the standard security technology for establishing an encrypted link between the two systems. These can be browser to server, server to server or client to server. Basically, SSL ensures that the data transfer between the two systems remains encrypted and private.

The https is essentially http over SSL. SSL establishes an encrypted link using an SSL certificate which is also known as a digital certificate.



How SSL works?

SSL fundamentally works with the following concepts:

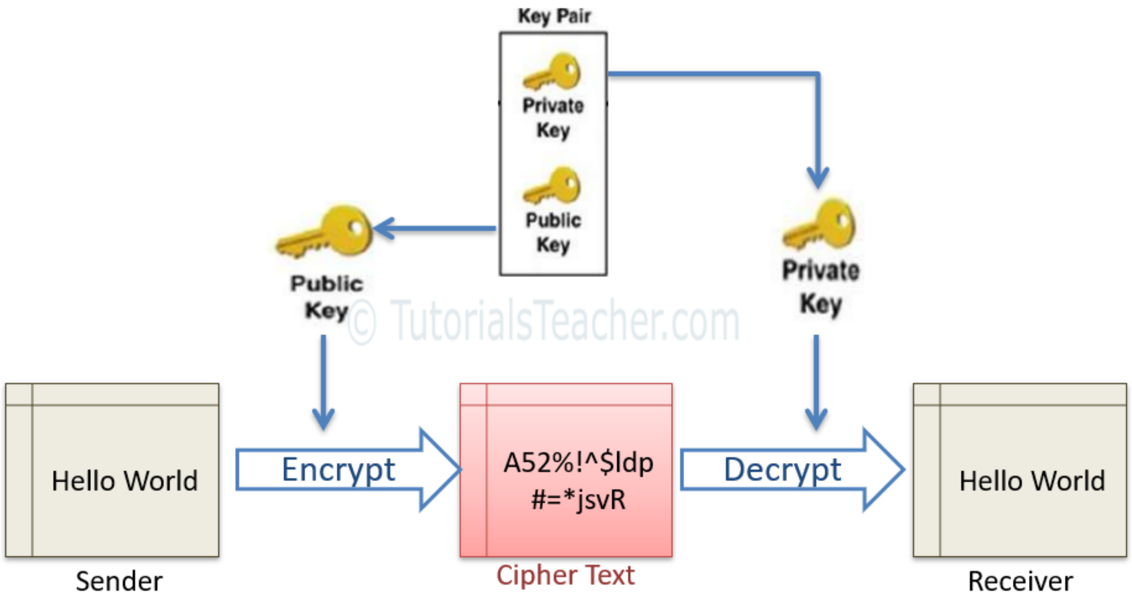
1. Asymmetric Cryptography
2. Symmetric Cryptography

Asymmetric Cryptography

Asymmetric cryptography (also known as Asymmetric Encryption or Public Key Cryptography) uses a mathematically-related key pair to encrypt and decrypt data. In a key pair, one key is shared with anyone who is interested in a communication. This is called Public Key. The other key in the key pair is kept secret and is called Private Key.

Public and private keys are mathematical related and were created using cryptographic algorithms which are based on mathematical problems termed These keys are used to encrypts or decrypts the data.

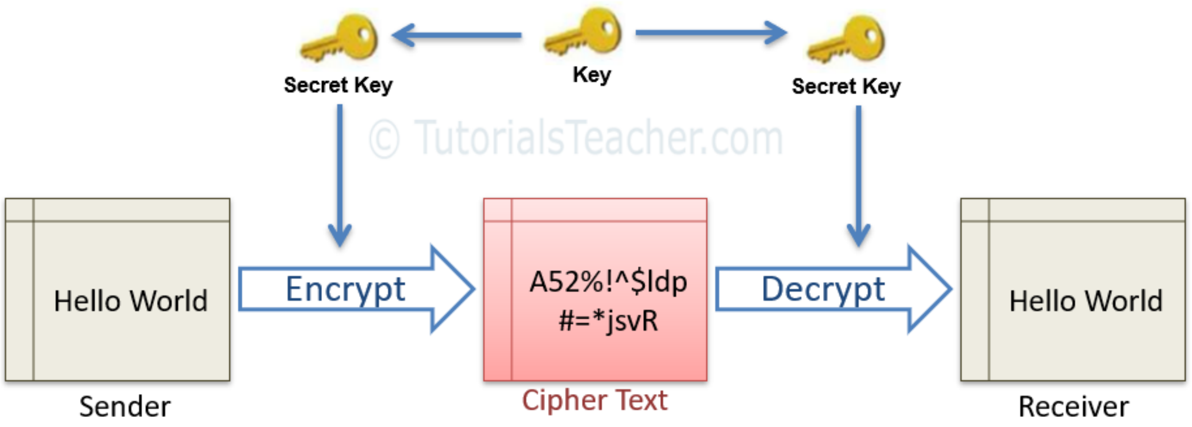
In the asymmetric cryptography, the sender encrypt data with the receiver's public key and send it to the receiver. The receiver decrypts it using the related private key.



SSL uses asymmetric cryptography to initiate the communication which is known as SSL handshake. Most commonly used asymmetric key encryption algorithms include EIGamal, RSA, DSA, Elliptic curve techniques and PKCS.

Symmetric Cryptography

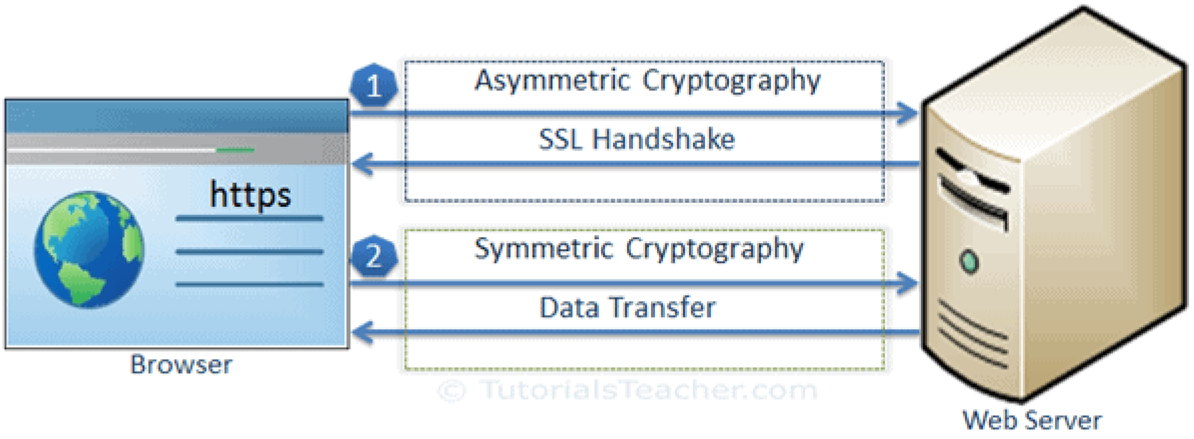
In the symmetric cryptography, there is only one key which encrypts and decrypts the data. Both sender and receiver should have this key, which is only known to them.



SSL uses symmetric cryptography using the session key after the initial handshake is done. The most widely used symmetric algorithms are AES-128, AES-192 and AES-256.

Data Transfer over SSL

SSL protocol uses asymmetric and symmetric cryptography to transfer data securely. The following figure illustrates the steps of SSL communication:



As you can see in the above figure, SSL communication between the browser and the web server (or any other two systems) is mainly divided into two steps: the SSL handshake and the actual data transfer.

What is SSL Certificate?

The SSL certificate (also known as digital certificate) plays an important role in securing the communication between two systems.

The SSL certificate is a data file issued by the authorised Certificate Authority (CA). As you learned in the previous chapter, SSL uses asymmetric cryptography to establish an encrypted link between the two systems using a key pair (public key and private key). The SSL certificate contains the owner's public key and other details. The web server sends a public key to the browser through an SSL certificate and the browser verifies it and authenticates the web server using the SSL certificate.