An SSL (Secure Sockets Layer) connection establishes an encrypted link between a server and a client. SSL is configured using three keys: the public, private, and session keys. With the public key, anything encrypted can only be decrypted with the private key and vice versa.

Due to the difficulty of encrypting and decrypting with private and public keys, they are only used during the SSL Handshake in order to create a symmetric session key. Using the session key, all transmitted data is encrypted after the secure connection has been established.

**Check the OS version** 🡪 lsb release -a

**Install the apache server** 🡪 sudo apt install apache2 -y

**Create a sample index.html file for that create a directory** 🡪 mkdir /var/www/test

**Create a index.html file** 🡪 vim /var/www/test/index.html

<!DOCTYPE html>

<html>

<head>

<title>testing</title>

</head>

<body>

<h1>Welcome to Linux help</h1>

</body>

</html>

!wq save and exit

**Change the ownership and permission for this directory** 🡪 chmod -R 755 /var/www/test

**Change the ownership** 🡪 chown -R www-data(username of apache server). /var/www/test

**Set up virtual hosts for Apache2** 🡪 vim /etc/apache2/sites-available/test.conf

<virtualhost \*:80>

servername www [www.linuxhelp1.com](http://www.linuxhelp1.com)

documentroot /var/www/test

</virtualhost>

!wq

**Enable this virtual host 🡪** a2ensite test.conf

**Restart this web server 🡪** systemctl restart apache2

Add a host entry for this server name 🡪 vim /etc/hosts

Add IP adress with the server name (Sample 🡪 192.168.6.115 – [www.linuxhelp1.com](http://www.linuxhelp1.com))

!wq

Go to the browser and bring the server name ([www.linuxhelp1.com](http://www.linuxhelp1.com))

Connection is not secured. To make secure it, we use SSL certificate.

Before we generating, we need to enable the SSL model 🡪 a2enmod ssl

Restart apache server 🡪 systemctl restart apache2

To generate ssl certificate use 🡪 openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/linuxhelp1.key \*out /etc/ssl/certs/linuxhelp1.crt

Country name : IN

Locality Name: Default (press enter)

Create a virtual host for SSL 🡪 vim /etc/apache2/sites-available/test-ssl.conf

<virtualhost \*:443>

servername [www.linuxhelp1.com](http://www.linuxhelp1.com)

documentroot /var/www/test

SSLEngine on

SSLCertificateFile /etc/ssl/certs/linuxhelp1.crt

SSLCertificateKeyFile /etc/ssl/private/linuxhelp1.key

</virtualhost>

!wq

Redirect port 80 to 443 port 🡪 vim /etc/apache2/sites-available/test.conf

<virtualhost \*:80>

servername [www.linuxhelp1.com](http://www.linuxhelp1.com)

documentroot /var/www/test

redirect / <https://www.linuxhelp1.com>

Press ESC and type !wq

Enable the virtual SSL file 🡪 a2ensite test-ssl.conf

Restart the server 🡪 systemctl restart apache2

Go to the browser 🡪 Click Advanced (https working)