Date:21.11.2022

**Final Year B. Tech., Sem VII 2022-23**

**Cryptography And Network Security Lab**

**Assignment submission**

**PRN : 2019BTECS00071**

**Name : Abhishek Charpale**

**Batch: B3**

**Assignment: 14**

**Title of assignment: Implementation of SSL using openssl**

**Title:**

Implementation of SSL using openssl

**Aim:**

To create SSL certificate using openssl

**Theory:**

* **SSL (Secure Sockets Layer)** and its successor , is protocol for establishing authenticated and encrypted links between networked computers.

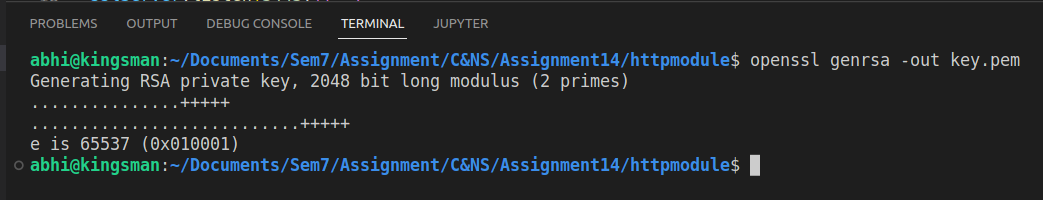
What is an SSL certificate?

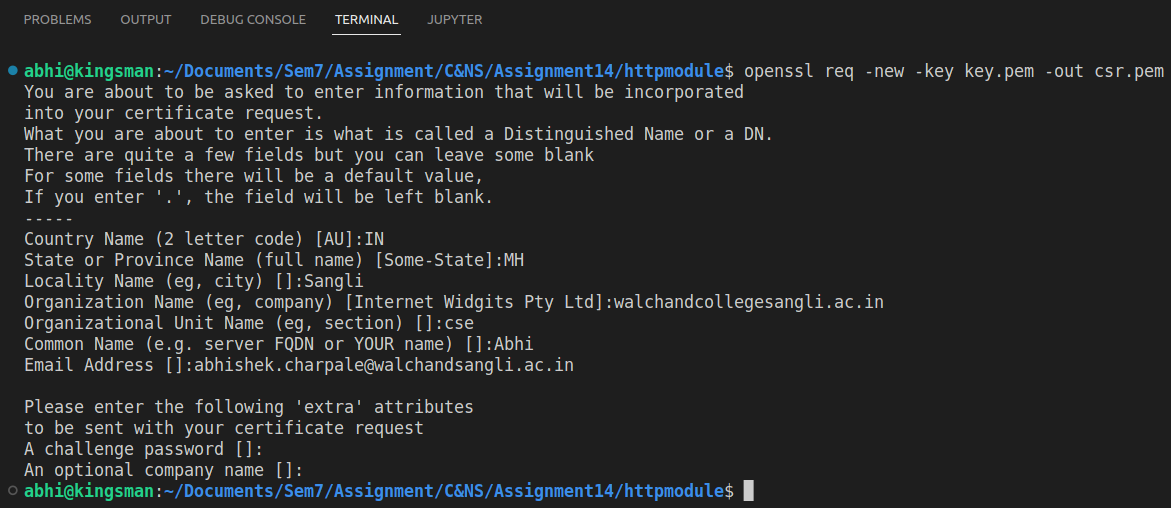
* An SSL certificate (also known as a TLS or SSL/TLS certificate) is a digital document that binds the identity of a website to a cryptographic key pair consisting of a public key and a private key. The public key, included in the certificate, allows a web browser to initiate an encrypted communication session with a web server via the TLS and HTTPS protocols. The private key is kept secure on the server, and is used to digitally sign web pages and other documents (such as images and JavaScript files).
* An SSL certificate also includes identifying information about a website, including its domain name and, optionally, identifying information about the site’s owner. If the web server’s SSL certificate is signed by a publicly trusted certificate authority (CA), like SSL.com, digitally signed content from the server will be trusted by end users’ web browsers and operating systems as authentic.
* An SSL certificate is a type of X.509 certificate.

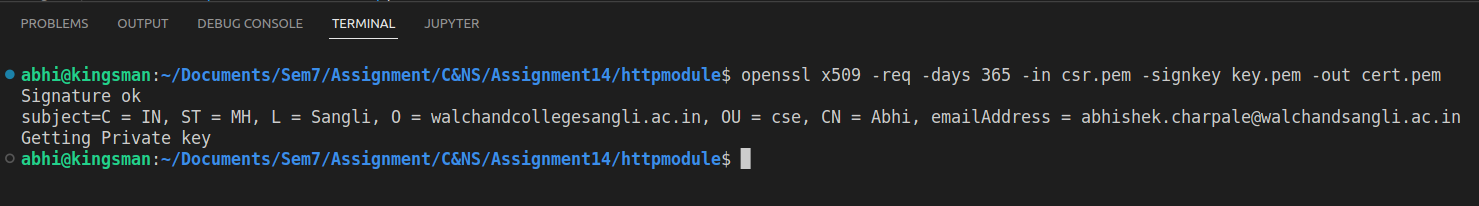
**Code:**

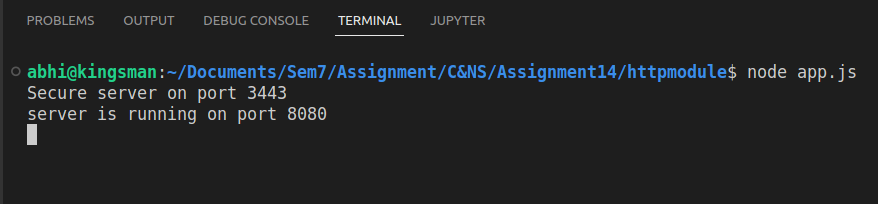
App.js

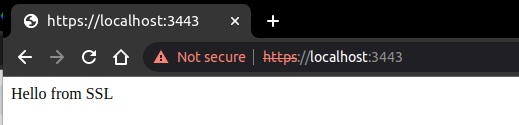
****

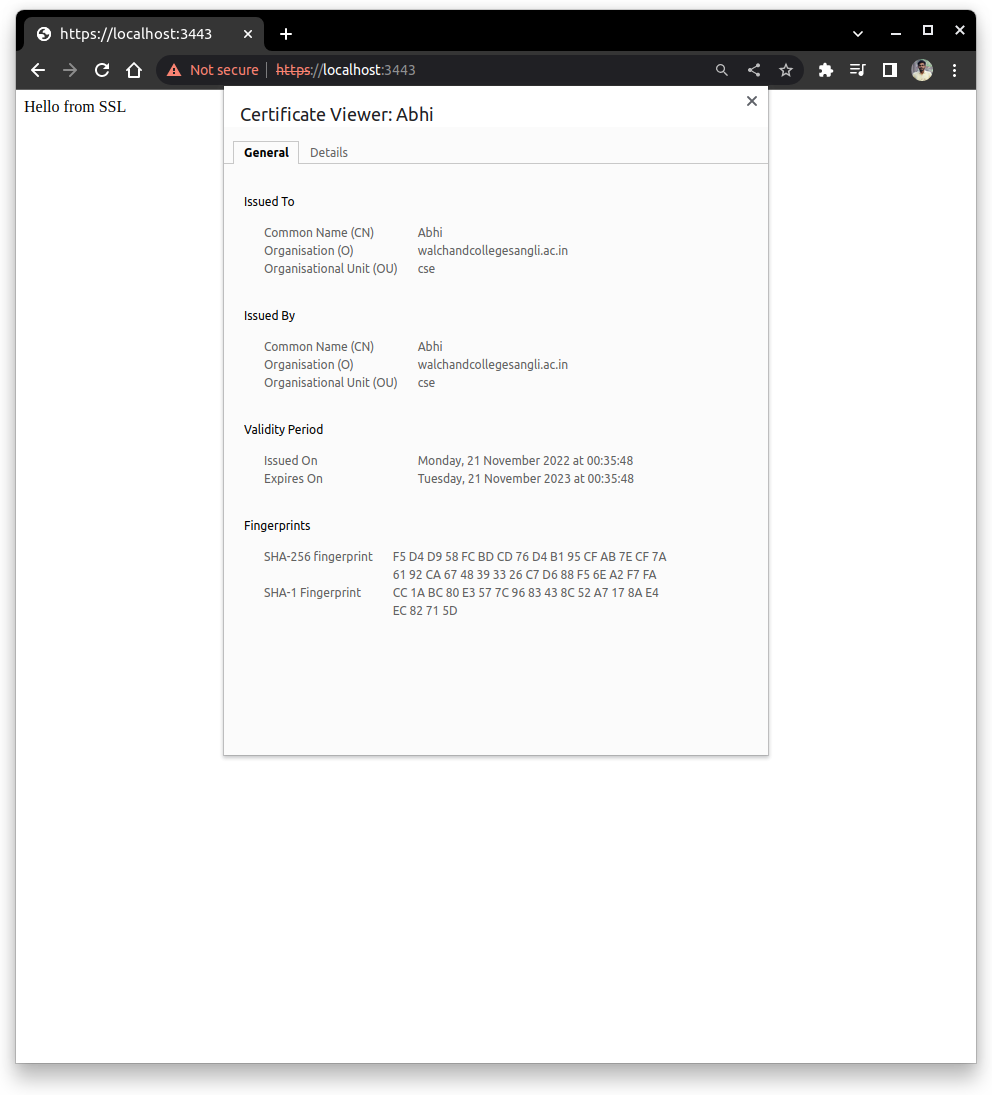












**Conclusion:**

Performed the experiment successfully.

The SSL certificate has been created.