**APDS7311 ICE 3 TASK**

Karabo Dlamini ST10139672

**Creating a self-signed SSL certificate:** To create a self-signed SSL certificate, follow these steps:

**Step 1:** Open a terminal and run the command to generate a private key:

openssl genrsa -out privatekey.key 2048

This generates a 2048-bit RSA private key file named privatekey.key.

**Step 2:** Create a certificate signing request (CSR):

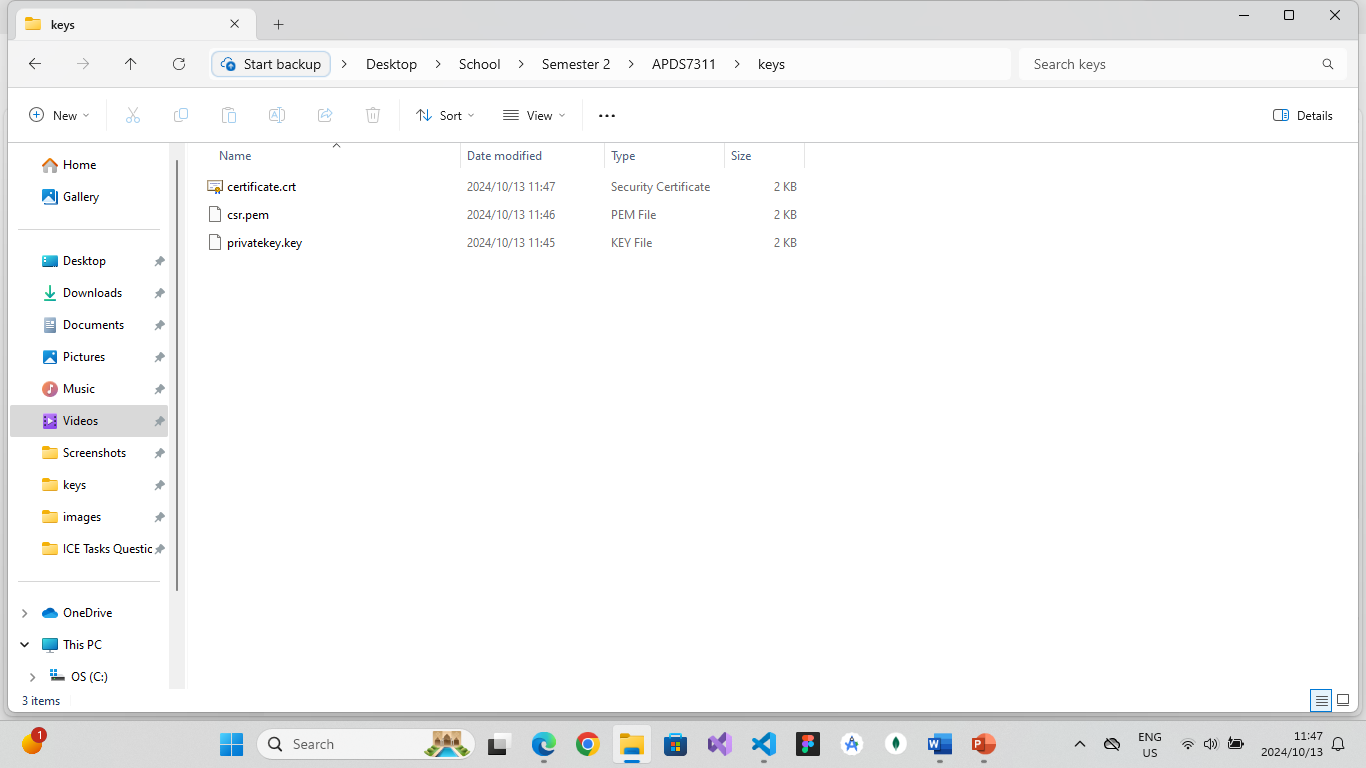
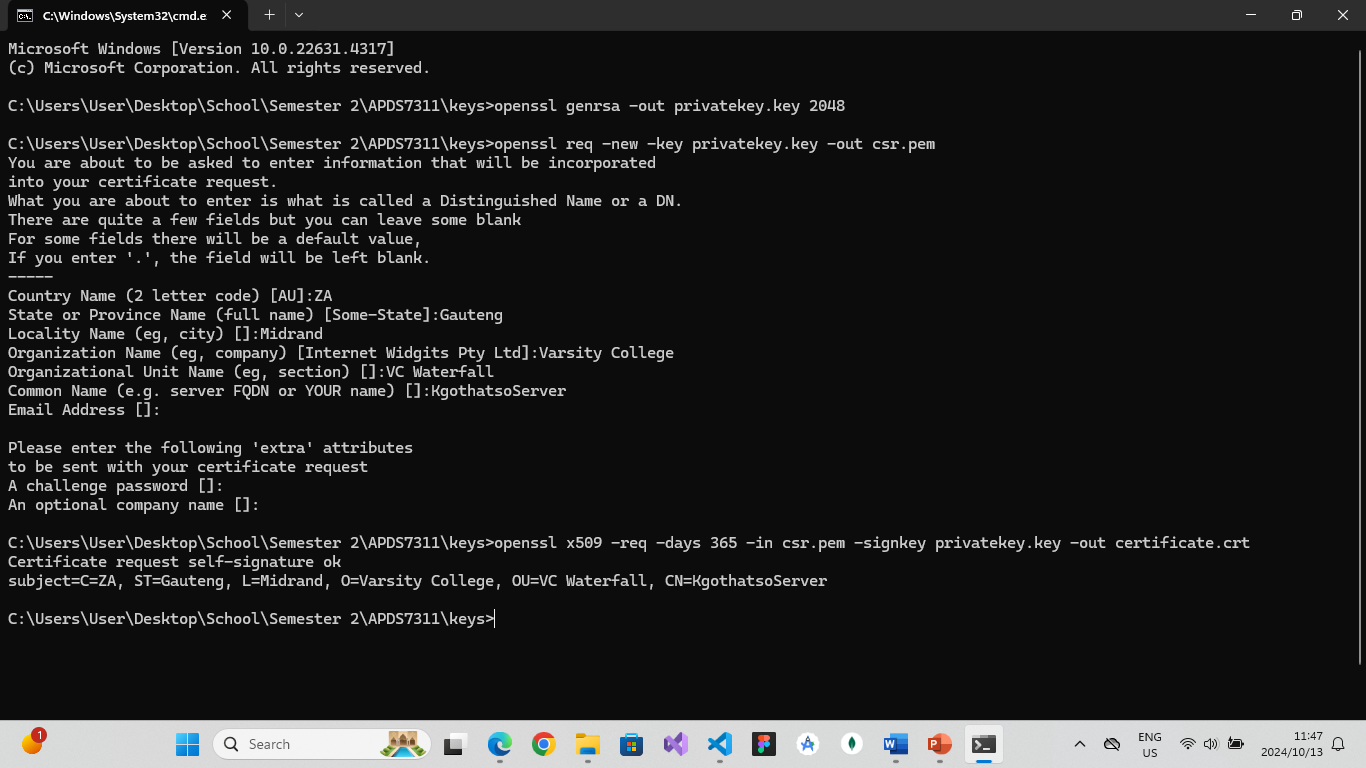
openssl req -new -key privatekey.key -out csr.pem

You'll be prompted to enter information like the domain name, organization, and location.

**Step 3:** Generate the self-signed certificate:

openssl x509 -req -days 365 -in csr.pem -signkey privatekey.key -out certificate.crt

This generates the certificate (certificate.crt) that is valid for 365 days.



2. Using the self-signed certificate in a web application: The self-signed certificate can be used to enable HTTPS for your local web server. You'll configure your server (Express.js) to use the generated .crt and .key files. Although browsers will warn users about the certificate being untrusted (since it's self-signed and not verified by a trusted Certificate Authority), it can still be useful for development and testing purposes.