**FORMAN CHRISTIAN COLLEGE**

**(A CHARTERED UNIVERSITY)**



**COMP421: Information Security**

**Section B**

**Assignment-2**

**Shaiq Zeeshan**

**251684243**

**List of Commands used:**

Private key:  
openssl genrsa -out private\_key.pem 2048

Public key:

openssl rsa -in private\_key.pem -pubout -out public\_key.pem

Csr:  
openssl req -new -key private\_key.pem -out request.csr

Self-signed certificate:

openssl req -x509 -sha256 -days 365 -key private\_key.pem -in request.csr -out self\_signed\_certificate.crt

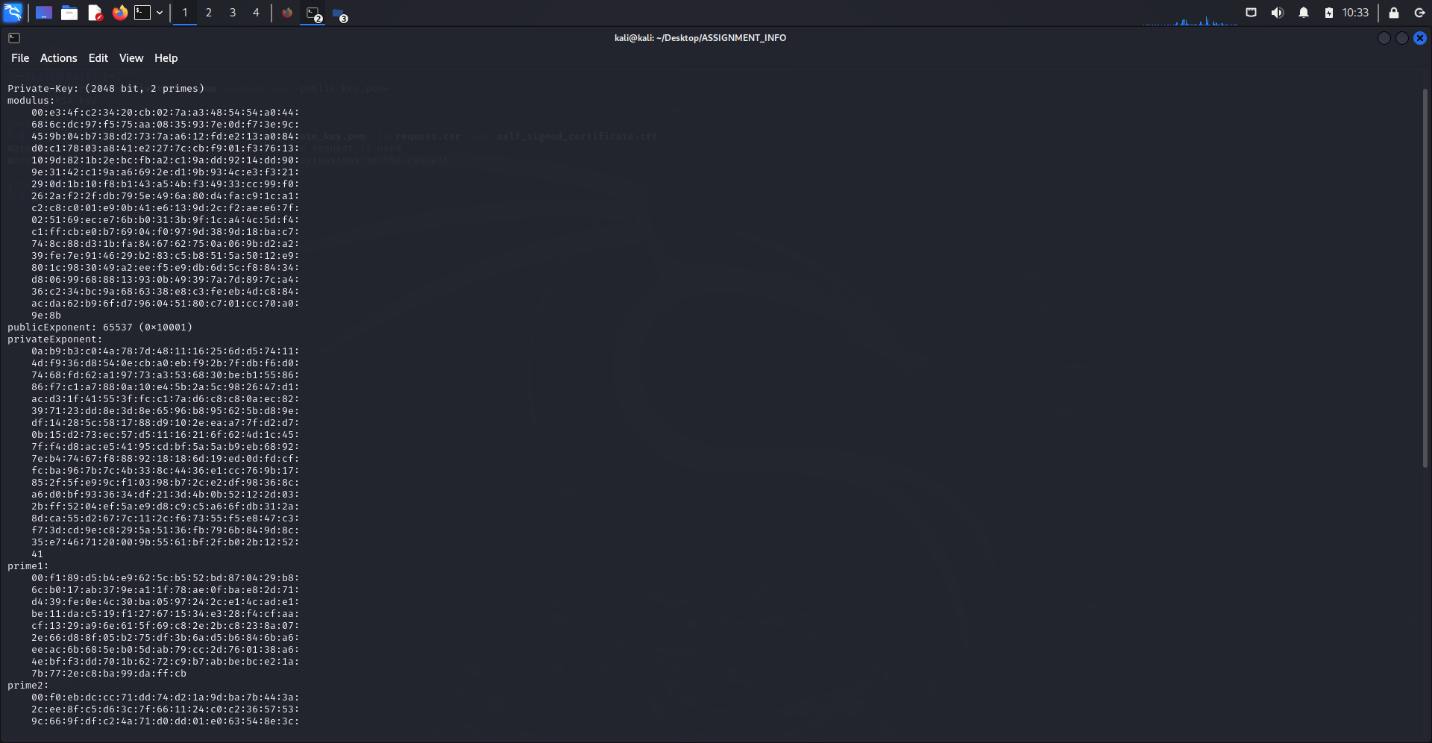
Private key for CA;  
openssl genrsa -out ca\_private\_key.pem 2048

Self signed certificate for ca:  
openssl req -x509 -new -nodes -key ca\_private\_key.pem -days 365 -out ca\_certificate.crt

Issuing certificate using ca:  
openssl x509 -req -in request.csr -CA ca\_certificate.crt -CAkey ca\_private\_key.pem -CAcreateserial -out signed\_certificate.crt -days 365 -sha256

**Snapshots**:

Private Key:

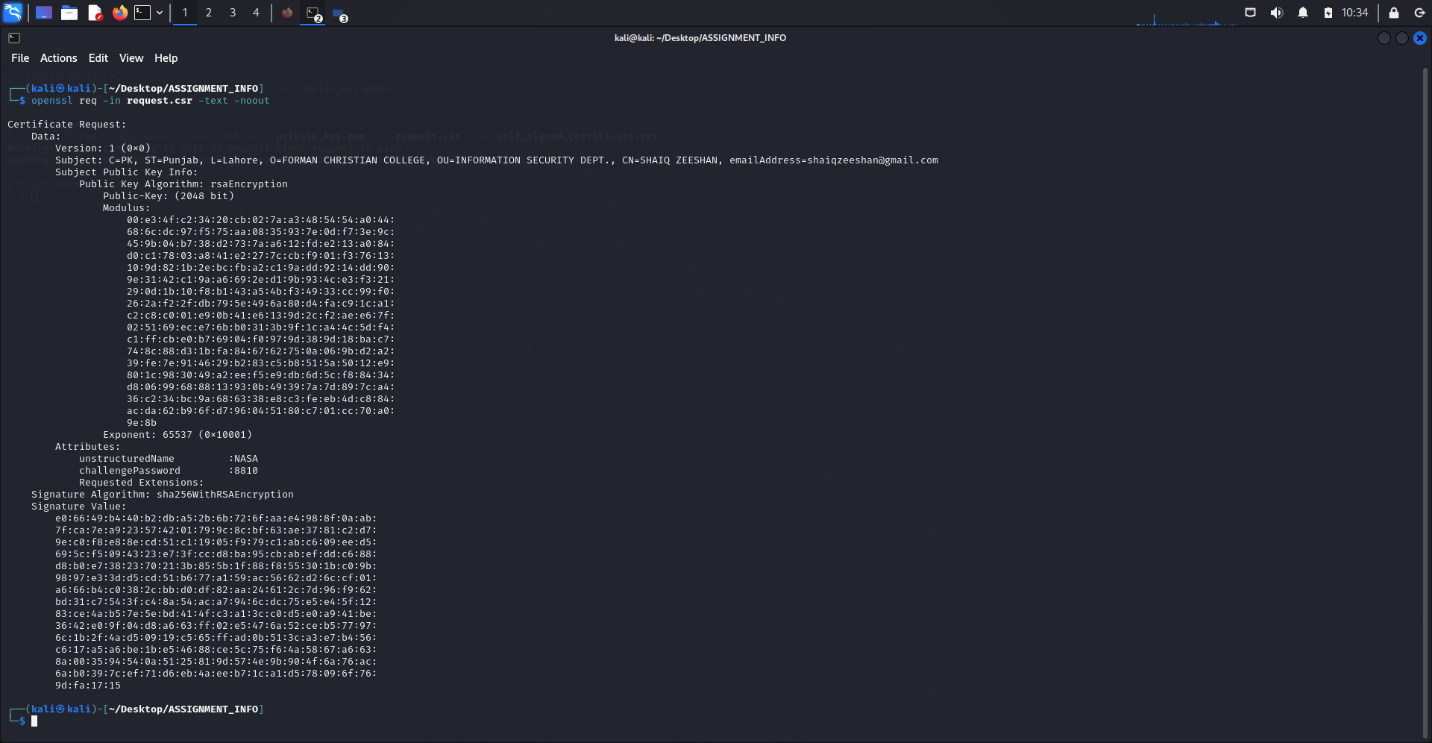


Public Key:

A computer screen shot of a computer

Description automatically generated

CSR:



Self Signed Certificate:

A screenshot of a computer

Description automatically generated

CA Certificate & CA sign certificate:

A screenshot of a computer

Description automatically generated