**FORMAN CHRISTIAN COLLEGE (A CHARTERED UNIVERSITY)**

****

**Comp 421(B)**

**Fall 2024**

**Assignment 2**

**Information Security**

**List of Commands**

**Momina Binte Asad 251694202**

1. Generate a private and public key

* Private Key:

*openssl genrsa -out private\_key.pem 2048*

* Public Key:

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

1. Generate a Certificate Signing Request (CSR)

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

1. Create a self-signed certificate

*openssl req -x509 -key private\_key.pem -out self\_signed.crt -days 365*

1. Act as a Certification Authority (CA) to issue certificates.

* **Step 1: Create a CA key and certificate**

*openssl genrsa -out ca\_key.pem 2048*

*openssl req -x509 -new -key ca\_key.pem -out ca\_cert.crt -days 365*

* **Step 2: Use the CA to sign a certificate request**

*openssl x509 -req -in request.csr -CA ca\_cert.crt -CAkey ca\_key.pem*

*-CAcreateserial -out issued\_cert.crt -days 365*