**Information Security COMP 421 Fall 2024 Section B**

**Assignment 2**

**NAME: AMMAR BIN AZHAR**

**ROLL NO: 251684528**

1. **Generate a private and public key:**

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

1. **Generate a Certificate Signing Request (CSR):**

* openssl req -new -key private\_key.pem -out my\_csr.csr
* ls -l my\_csr.csr

1. **Create a self-signed certificate:**

* openssl x509 -req -days 365 -in my\_csr.csr -signkey private\_key.pem -out self\_signed\_cert.pem
* openssl x509 -in self\_signed\_cert.pem -text -noout

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

* openssl genpkey -algorithm RSA -out ca\_private\_key.pem
* openssl req -new -x509 -days 365 -key ca\_private\_key.pem -out ca\_cert.pem
* openssl x509 -req -in my\_csr.csr -CA ca\_cert.pem -CAkey ca\_private\_key.pem -CAcreateserial -out issued\_cert.pem -days 365
* openssl x509 -in issued\_cert.pem -text -noout
* ls -l