**Information Security COMP 421**

**Fall 2024 Section B**

**Assignment 2**

**Aysha Shahzad**

**241605890**

1. Generate a private key (2048-bit RSA):

command: openssl genrsa -out private\_key.pem 2048

This command generates a 2048-bit RSA private key and saves it in the file `private\_key.pem`.

2. Extract the public key from the private key

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

This command extracts the public key from the private key and saves it in the file `public\_key.pem`.

3. Generate a Certificate Signing Request (CSR)

command: openssl req -new -key private\_key.pem -out certificate\_request.csr

This command generates a CSR using the private key, prompting the user to enter certificate details (e.g., country, state, common name).

**Screenshots of 1-3 commands:**



4. Create a self-signed certificate (valid for 365 days)

command: openssl x509 -req -days 365 -in certificate\_request.csr -signkey private\_key.pem -out self\_signed\_certificate.crt

This command creates a self-signed certificate using the CSR and the private key. The certificate is valid for 1 year (365 days).

5. Generate a private key for the Certification Authority (CA)

command: openssl genrsa -out ca\_private\_key.pem 2048

command: This command generates a 2048-bit RSA private key for the CA and saves it in the file `ca\_private\_key.pem`.

6. Create a self-signed certificate for the CA (valid for 365 days)

command: openssl req -new -x509 -days 365 -key ca\_private\_key.pem -out ca\_certificate.crt

This command creates a self-signed certificate for the CA using the CA's private key.

7. Sign the client CSR with the CA certificate to issue a client certificate (valid for 365 days)

command: openssl x509 -req -days 365 -in certificate\_request.csr -CA ca\_certificate.crt -CAkey ca\_private\_key.pem -CAcreateserial -out client\_certificate.crt

This command uses the CA's private key and certificate to sign the client CSR, issuing a client certificate valid for 1 year.

**Screenshot of next 4-6 commands:**

