Information Security COMP 421

Fall 2024 Section B

Assignment 2

Muhammad Rehan Wali

241546596

1) Generating private and public keys:

Private key: openssl genrsa -out myprivatekey.pem 2048

Public key from the private key: openssl rsa -in myprivatekey.pem -pubout -out mypublickey.pem

```
C:\Users\HP>mkdir assign2

C:\Users\HP>cd assign2

C:\Users\HP\assign2>openssl genrsa -out myprivatekey.pem 2048

C:\Users\HP\assign2>openssl rsa -in myprivatekey.pem -pubout -out mypublickey,pem writing rsa key
rsa: Extra option: "writing"
rsa: Use -help for summary.

C:\Users\HP\assign2>openssl rsa -in myprivatekey.pem -pubout -out mypublickey.pem writing RSA key
rsa: Extra option: "writing"
rsa: Use -help for summary.

C:\Users\HP\assign2>openssl rsa -in myprivatekey.pem -pubout -out mypublickey,pem
writing RSA key
```

2). Generate a Certificate Signing Request (CSR):

openssl req -new -key myprivatekey.pem -out myrequest.csr

```
C:\Users\HP\assign2>openssl req -new -key myprivatekey.pem -out myrequest.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PK
State or Province Name (full name) [Some-State]:Punjab
Locality Name (eg, city) []:Lahore
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PitchP
Organizational Unit Name (eg, section) []:Rehan
Common Name (e.g. server FQDN or YOUR name) []:RH
Email Address []:rehanwali386@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:12345
An optional company name []:Pitch

C:\Users\HP\assign2>openssl x509 -req -days 365 -in myrequest.csr -signkey myprivatekey.pem -out
x509: Option -out needs a value
x509: Use -help for summary.

C:\Users\HP\assign2>openssl x509 -req -days 365 -in myrequest.csr -signkey myprivatekey.pem -out myCertificate.crt
Certificate request self-signature ok
subject=C=PK, ST=Punjab, L=Lahore, O=PitchP, OU=Rehan, CN=RH, emailAddress=rehanwali386@gmail.com
```

3). Create a self-signed certificate:

openssl x509 -req -days 365 -in myrequest.csr -signkey myprivatekey.pem -out mycertificate.crt

```
C:\Users\HP\assign2>openssl x509 -req -days 365 -in myrequest.csr -signkey myprivatekey.pem -out myCertificate.crt
Certificate request self-signature ok
subject=C=PK, ST=Punjab, L=Lahore, O=PitchP, OU=Rehan, CN=RH, emailAddress=rehanwali386@gmail.com
```

4) Act as a Certification Authority (CA) to issue certificates:

• Create a CA private key: openssl genrsa -out ca_privatekey.pem 2048

• Create a CA certificate: openssl req -x509 -new -nodes -key ca_privatekey.pem - sha256 -days 3650 -out ca_certificate.crt

• Use the CA to sign a CSR and issue a certificate: openssl x509 -req -in myrequest.csr - CA ca_certificate.crt -CAkey ca_privatekey.pem -CAcreateserial -out issued_certificate.crt -days 365 -sha256