Kennan Seno
D14123582
Lab 9

NOTE: For this lab, "**cryptographer**" package was used to achieve the given tasks. Please refer to the package's github link for installation process.

Question 1

To run the python script for this task, type 'python lab9-part1.py' in the terminal.

The script will generate a key and save it in a file in the folder called 'part1-key.pem'. The key will also be used to create a self signed certificate which will be used as a root certificate. A file called 'selfsigned-cert.pem' for the cerficate will also be created in the folder.

Question 2

To run the python script for this task, type 'python lab9-part2.py' in the terminal.

The script will read the key used to create the root certificate in question one and use it to create another certificate.

Question 3

To check the keys and chaining certificates, enter the command below in the terminal.

```
# check self-signed cert
openssl x509 -in selfsigned-cert.pem -text -noout

# check Question 1 key
 openssl rsa -in part1-key.pem -check

# check CSR cert in part 2
openssl req -in csr.pem -text -noout
```

You can also use the shell script "verifyChainCerts.sh" located in the lab folder