CSCI-2201
Lab 6

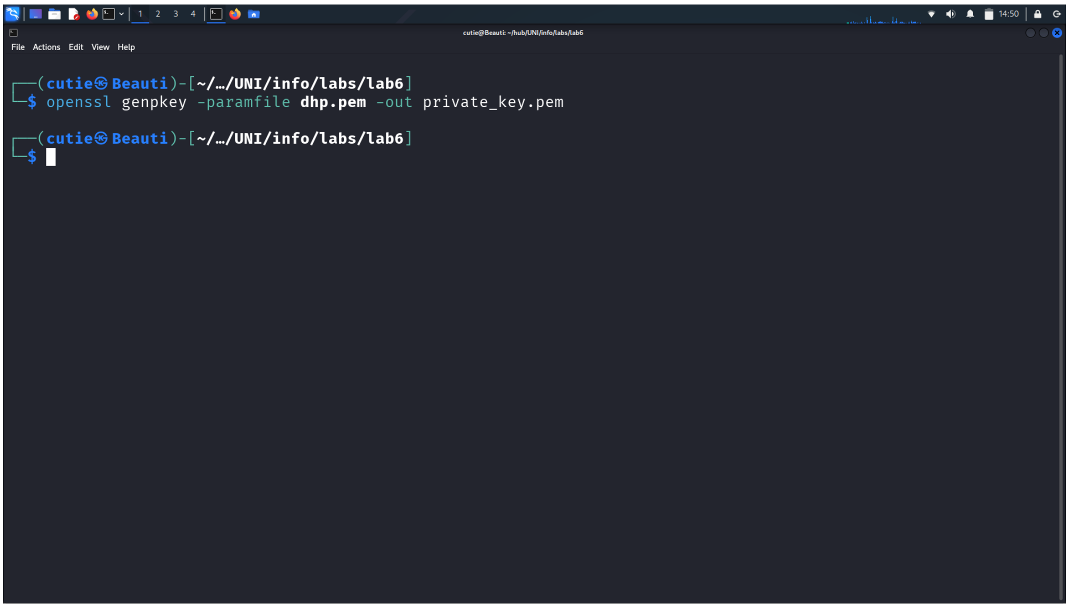
Anas Alhadi

B00895875

March 14, 2025

Contents

1 Exercise 1

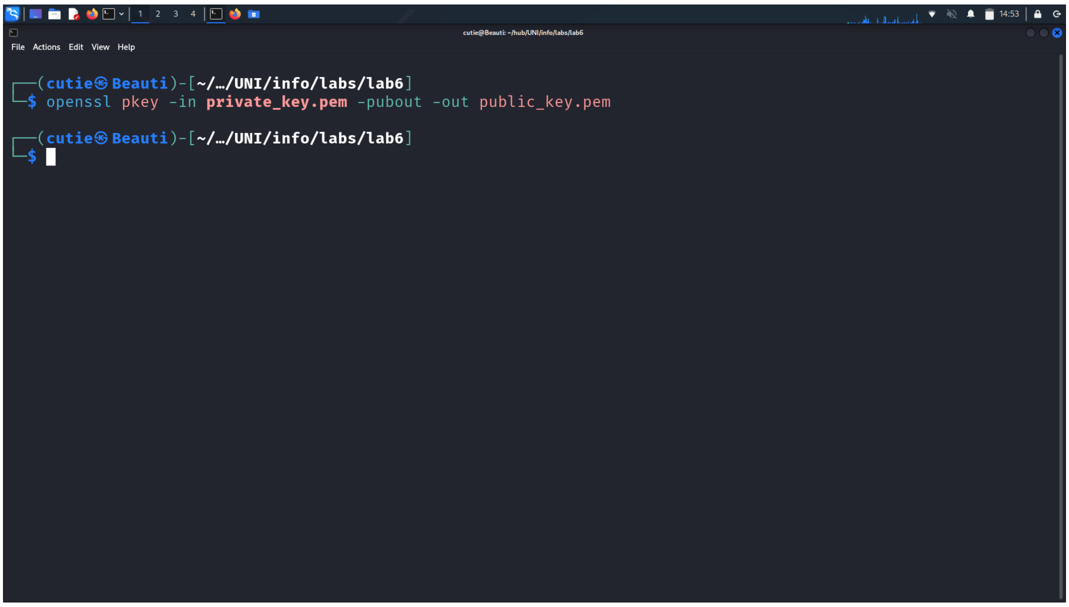


14:50
cutie@Beauti: ~/hub/UNI/info/labs/lab6
File Actions Edit View Help

```
┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ openssl genpkey -paramfile dhp.pem -out private_key.pem

┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ 
```

step 1

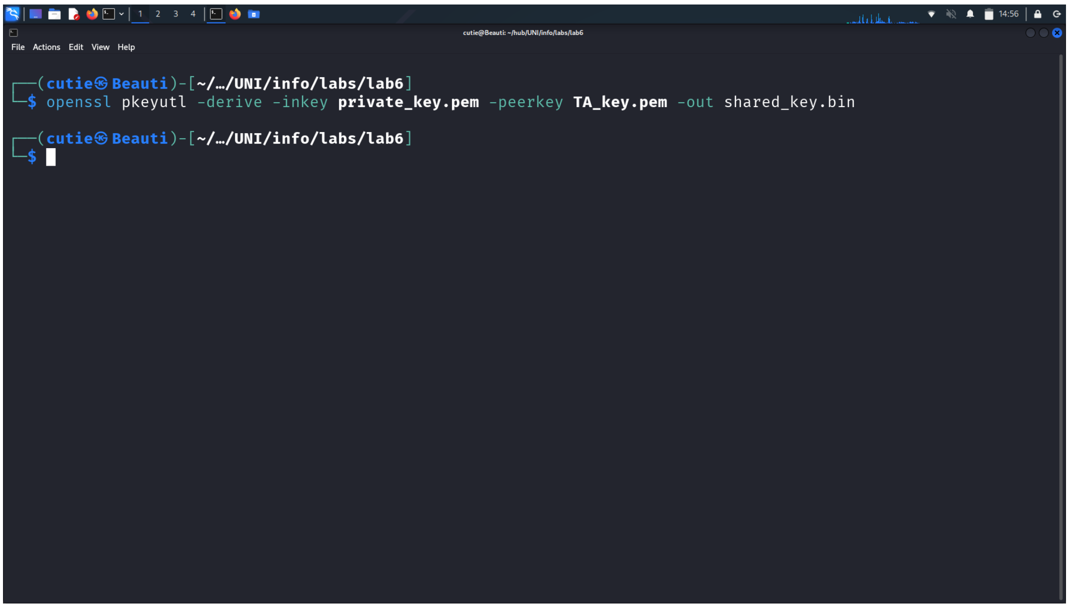


14:53
cutie@Beauti: ~/hub/UNI/info/labs/lab6
File Actions Edit View Help

```
┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ openssl pkey -in private_key.pem -pubout -out public_key.pem

┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ 
```

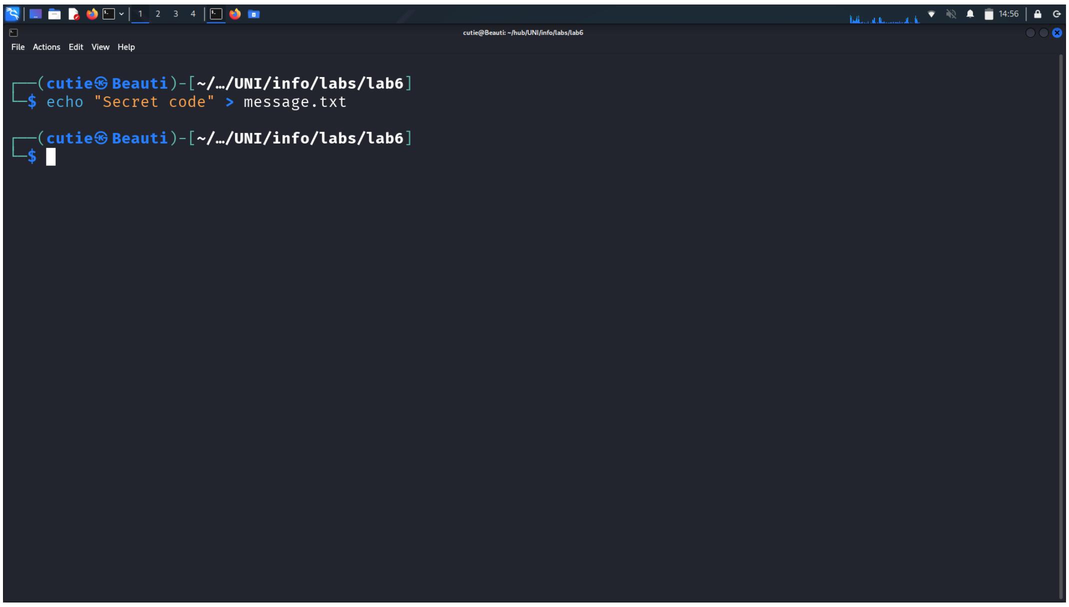
step 2



```
┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ openssl pkeyutl -derive -inkey private_key.pem -peerkey TA_key.pem -out shared_key.bin

┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ 
```

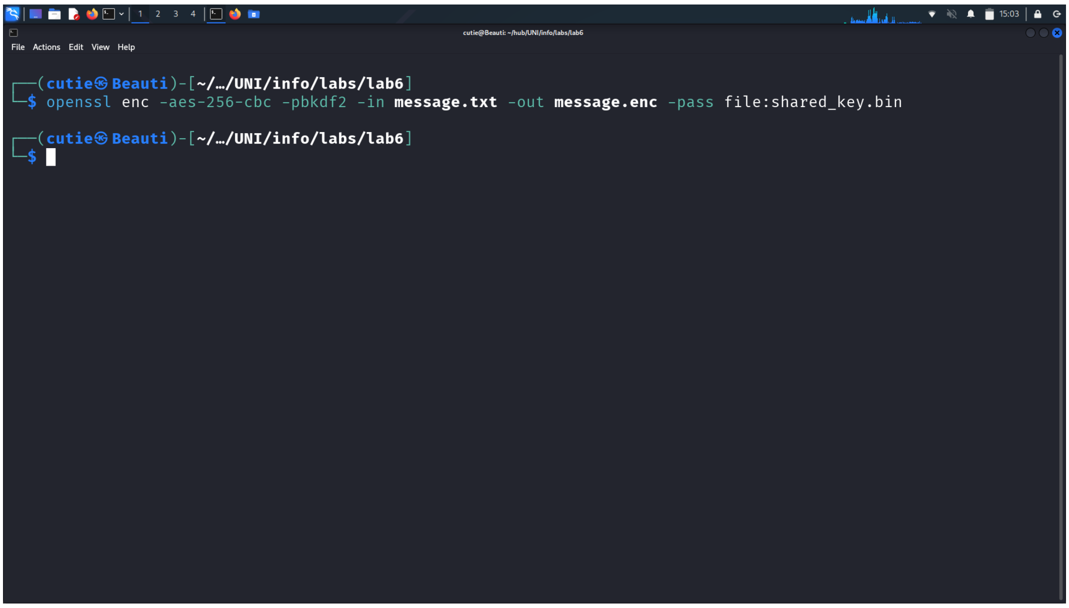
step 3



```
┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ echo "Secret code" > message.txt

┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ 
```

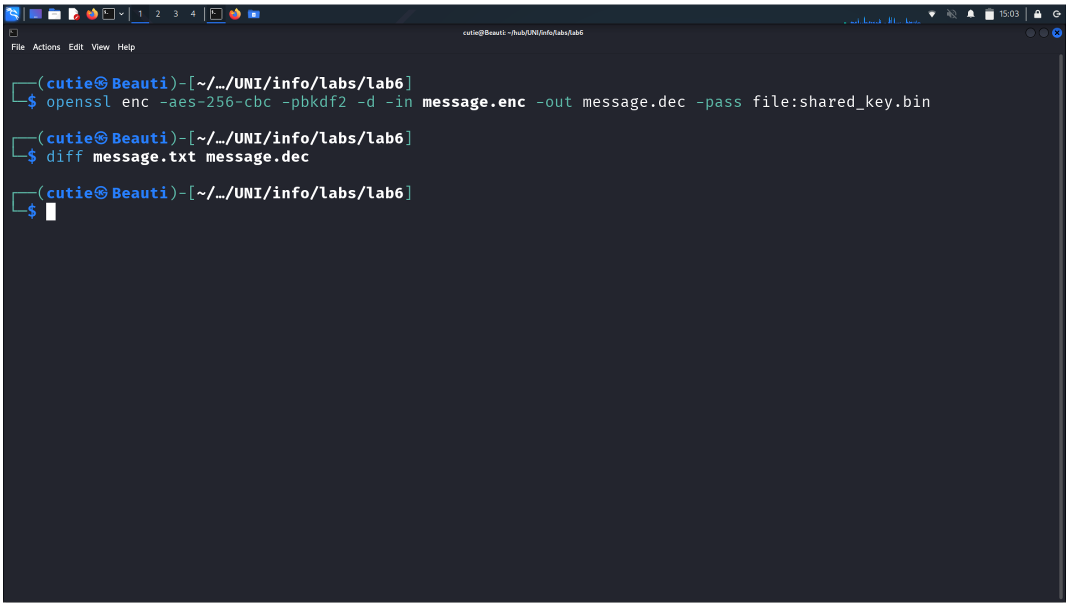
step 4



```
┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ openssl enc -aes-256-cbc -pbkdf2 -in message.txt -out message.enc -pass file:shared_key.bin

┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ 
```

step 5



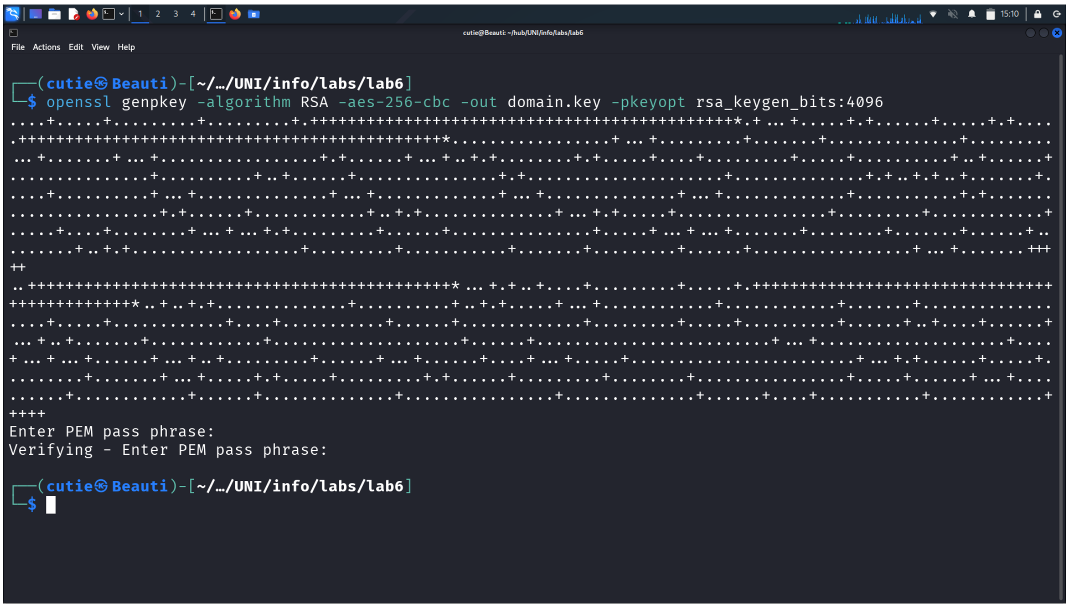
```
┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ openssl enc -aes-256-cbc -pbkdf2 -d -in message.enc -out message.dec -pass file:shared_key.bin

┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ diff message.txt message.dec

┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ 
```

step 6

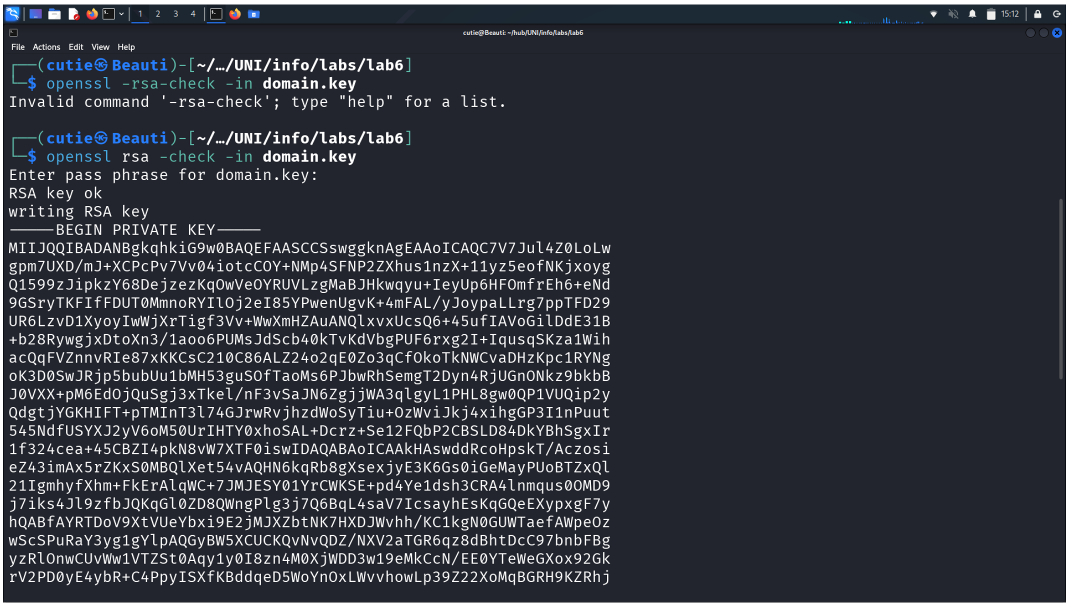
2 Exercise 2



```
┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ openssl genpkey -algorithm RSA -aes-256-cbc -out domain.key -pkeyopt rsa_keygen_bits:4096
....+.....+.........+.........+.++++++++++++++++++++++++++++++++++++++++++++++++*.+...+.....+.+......+.....+.+....
.+++++++++++++++++++++++++++++++++++++++++++++++++*................+...+.........+.......+..............+.........
...+.......+...+.................+.+......+...+..+.+........+.+.....+....+.........+.....+...........+..+......+
..............+..........+..+......+...............+.+.....................+..............+.+..+.+..+........+.
....+..........+...+..............+...+.............+...+..............+...+............+............+.+.......
...............+.+......+............+..+.+..............+...+.+.....+.................+.........+...........+
.....+....+........+...+...+.+.........+......+...............+.....+...+...+.......+........+........+......+..
.......+..+.+.................+.........+............+.......+.........+......+..................+...+........+++
++
..+++++++++++++++++++++++++++++++++++++++++++++++*...+.+..+....+.........+.....+.++++++++++++++++++++++++++++++++
+++++++++++++*..+..+.+..............+..........+..+.+.....+...+.............+.............+.........+.........
....+.....+..........+....+..........+......+.............+.........+.....+.........+......+..+....+......+
...+..+.......+...........+...................+......+.........................+...+......................+....
+...+...+......+...+..+.........+......+...+......+....+...+.....+.........................+...+.+.......+.....+.
........+.......+...+.....+.+.....+.........+.+......+.........+........+..................+.....+.......+...+....
......+............+......+..............+................+.............+......+....+...........+............+
++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ █
```

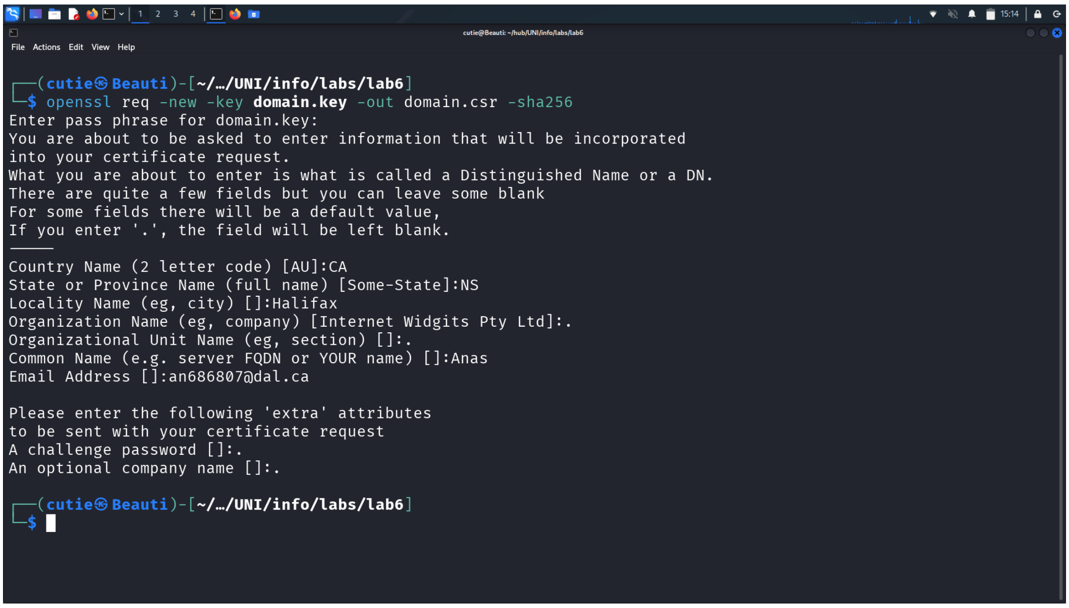
step 1



```
┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ openssl -rsa-check -in domain.key
Invalid command '-rsa-check'; type "help" for a list.

┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ openssl rsa -check -in domain.key
Enter pass phrase for domain.key:
RSA key ok
writing RSA key
-----BEGIN PRIVATE KEY-----
MIIJQQIBADANBgkqhkiG9w0BAQEFAASCCSswggknAgEAAoICAQC7V7Jul4Z0LoLw
gpm7UXD/mJ+XCPcPv7Vv04iotcCOY+NMp4SFNP2ZXhus1nzX+11yz5eofNKjxoyg
Q1599zJipkzY68DejzezKqOwVeOYRUVLzgMaBJHkwqyu+IeyUp6HFOmfrEh6+eNd
9GSryTKFIfFDUT0MmnoRYIlOj2eI85YPwenUgvK+4mFAL/yJoypaLLrg7ppTFD29
UR6LzvD1XyoyIwWjXrTigf3Vv+WwXmHZAuANQlxvxUcsQ6+45ufIAVoGilDdE31B
+b28RywgjxDtoXn3/1aoo6PUMsJdScb40kTvKdVbgPUF6rxg2I+IqusqSKza1Wih
acQqFVZnnvRIe87xKKCsC210C86ALZ24o2qE0Zo3qCfOkoTkNWCvaDHzKpc1RYNg
oK3D0SwJRjp5bubUu1bMH53guSOfTaoMs6PJbwRhSemgT2Dyn4RjUGnONkz9bkbB
J0VXX+pM6EdOjQuSgj3xTkel/nF3vSaJN6ZgjjWA3qlgyL1PHL8gw0QP1VUQip2y
QdgtjYGKHIFT+pTMInT3l74GJrwRvjhzdWoSyTiu+OzWviJkj4xihgGP3I1nPuut
545NdfUSYXJ2yV6oM50UrIHTY0xhoSAL+Dcrz+Se12FQbP2CBSLD84DkYBhSgxIr
1f324cea+45CBZI4pkN8vW7XTF0iswIDAQABAoICAAkHAswddRcoHpskT/Aczosi
eZ43imAx5rZKxS0MBQlXet54vAQHN6kqRb8gXsexjyE3K6Gs0iGeMayPUoBTZxQl
21IgmhyfXhm+FkErAlqWC+7JMJESY01YrCWKSE+pd4Ye1dsh3CRA4lnmqus0OMD9
j7iks4Jl9zfbJQKqGl0ZD8QWngPlg3j7Q6BqL4saV7IcsayhEsKqGQeEXypxgF7y
hQABfAYRTDoV9XtVUeYbxi9E2jMJXZbtNK7HXDJWvhh/KC1kgN0GUWTaefAWpeOz
wScSPuRaY3yg1gYlpAQGyBW5XCUCKQvNvQDZ/NXV2aTGR6qz8dBhtDcC97bnbFBg
yzRlOnwCUvWw1VTZSt0Aqy1y0I8zn4M0XjWDD3w19eMkCcN/EE0YTeWeGXox92Gk
rV2PD0yE4ybR+C4PpyISXfKBddqeD5WoYnOxLWvvhowLp39Z22XoMqBGRH9KZRhj
```

checking step1

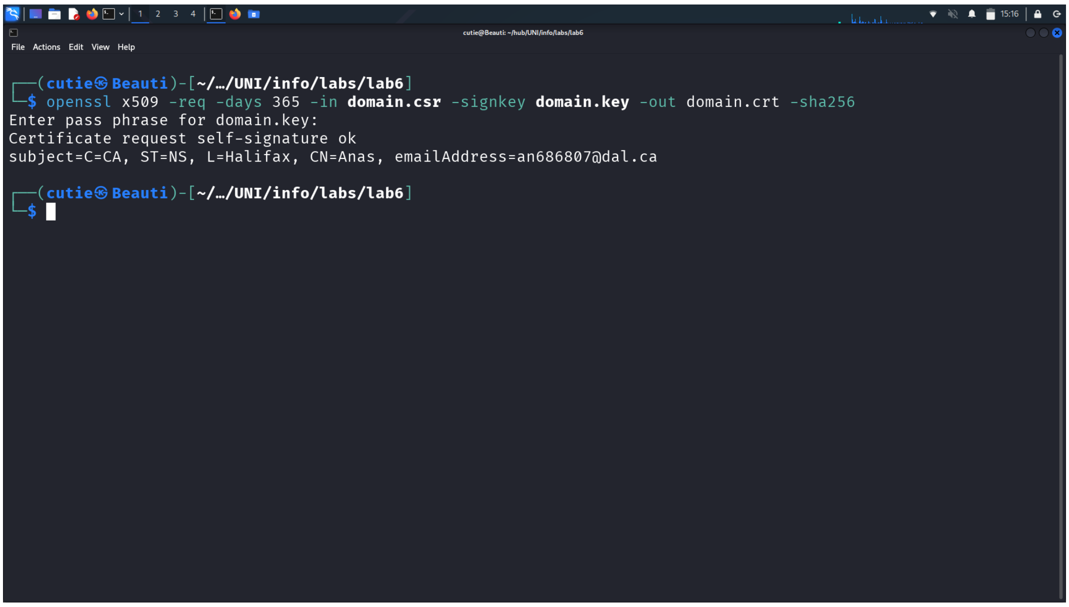


```
┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ openssl req -new -key domain.key -out domain.csr -sha256
Enter pass phrase for domain.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished 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]:CA
State or Province Name (full name) [Some-State]:NS
Locality Name (eg, city) []:Halifax
Organization Name (eg, company) [Internet Widgits Pty Ltd]:.
Organizational Unit Name (eg, section) []:.
Common Name (e.g. server FQDN or YOUR name) []:Anas
Email Address []:an686807@dal.ca

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

┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ 
```

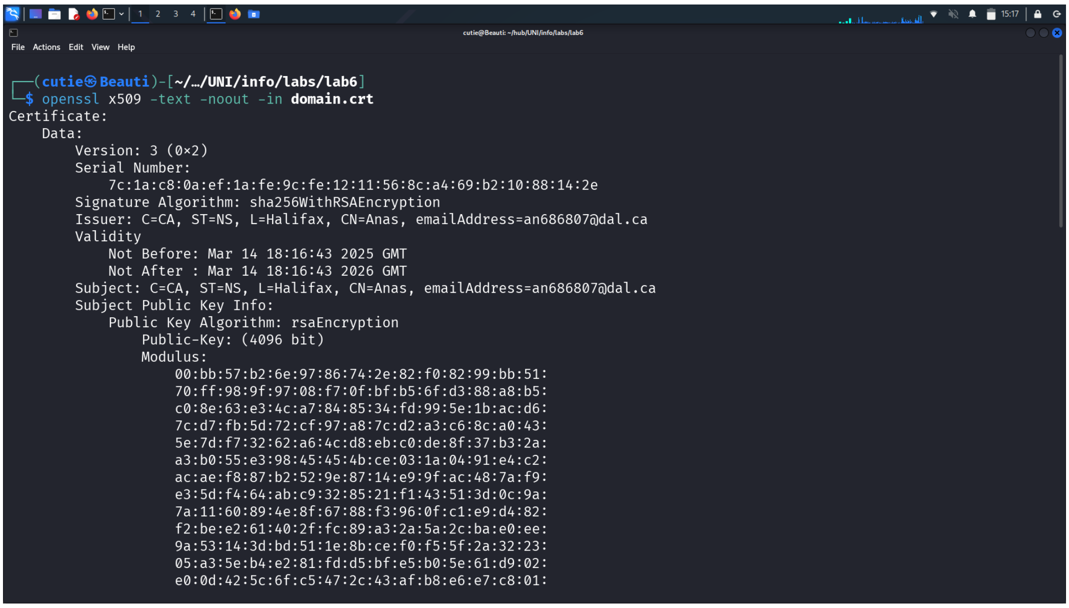
step 2



```
┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ openssl x509 -req -days 365 -in domain.csr -signkey domain.key -out domain.crt -sha256
Enter pass phrase for domain.key:
Certificate request self-signature ok
subject=C=CA, ST=NS, L=Halifax, CN=Anas, emailAddress=an686807@dal.ca

┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ 
```

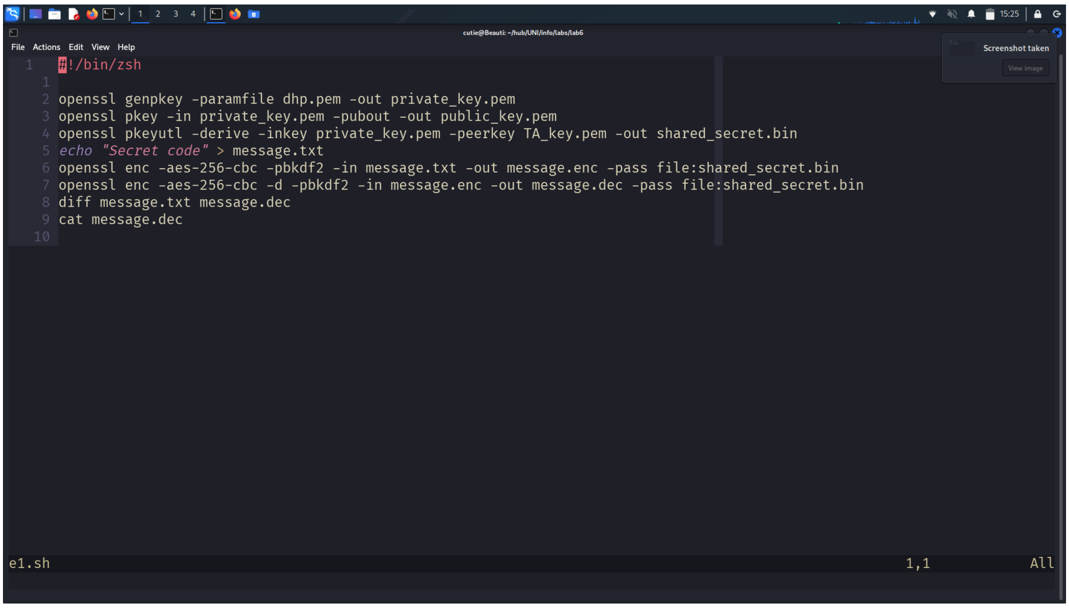
step 3



```
┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ openssl x509 -text -noout -in domain.crt
Certificate:
    Data:
        Version: 3 (0×2)
        Serial Number:
            7c:1a:c8:0a:ef:1a:fe:9c:fe:12:11:56:8c:a4:69:b2:10:88:14:2e
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CA, ST=NS, L=Halifax, CN=Anas, emailAddress=an686807@dal.ca
        Validity
            Not Before: Mar 14 18:16:43 2025 GMT
            Not After : Mar 14 18:16:43 2026 GMT
        Subject: C=CA, ST=NS, L=Halifax, CN=Anas, emailAddress=an686807@dal.ca
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:bb:57:b2:6e:97:86:74:2e:82:f0:82:99:bb:51:
                    70:ff:98:9f:97:08:f7:0f:bf:b5:6f:d3:88:a8:b5:
                    c0:8e:63:e3:4c:a7:84:85:34:fd:99:5e:1b:ac:d6:
                    7c:d7:fb:5d:72:cf:97:a8:7c:d2:a3:c6:8c:a0:43:
                    5e:7d:f7:32:62:a6:4c:d8:eb:c0:de:8f:37:b3:2a:
                    a3:b0:55:e3:98:45:45:4b:ce:03:1a:04:91:e4:c2:
                    ac:ae:f8:87:b2:52:9e:87:14:e9:9f:ac:48:7a:f9:
                    e3:5d:f4:64:ab:c9:32:85:21:f1:43:51:3d:0c:9a:
                    7a:11:60:89:4e:8f:67:88:f3:96:0f:c1:e9:d4:82:
                    f2:be:e2:61:40:2f:fc:89:a3:2a:5a:2c:ba:e0:ee:
                    9a:53:14:3d:bd:51:1e:8b:ce:f0:f5:5f:2a:32:23:
                    05:a3:5e:b4:e2:81:fd:d5:bf:e5:b0:5e:61:d9:02:
                    e0:0d:42:5c:6f:c5:47:2c:43:af:b8:e6:e7:c8:01:
```

step 4

3 Exercise 3

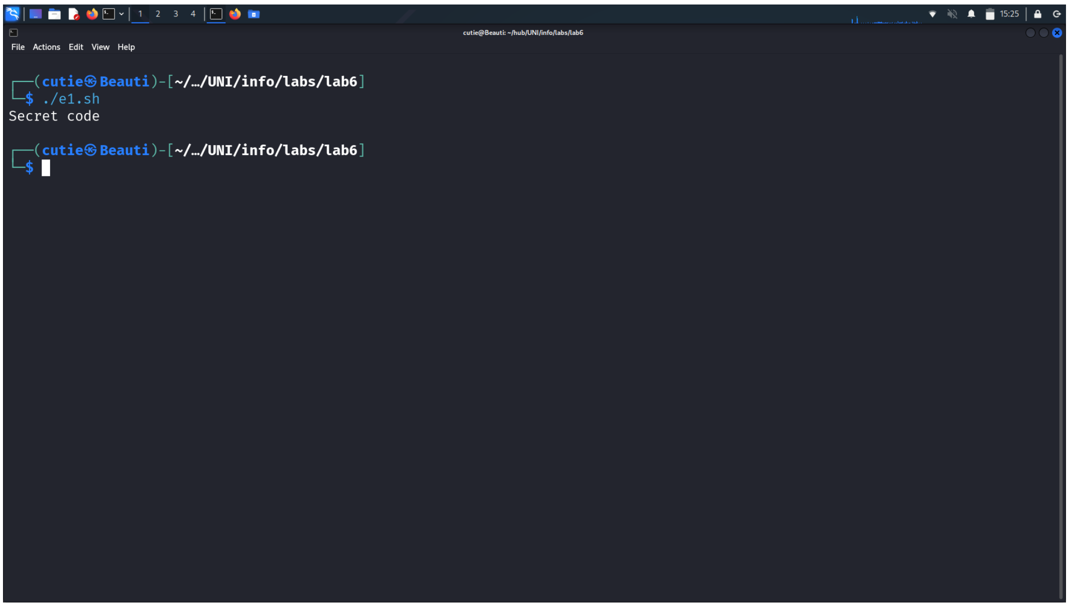

cutie@Beauti: ~/hub/UNI/info/labs/lab6
File Actions Edit View Help
Screenshot taken
View image

```
#!/bin/zsh

openssl genpkey -paramfile dhp.pem -out private_key.pem
openssl pkey -in private_key.pem -pubout -out public_key.pem
openssl pkeyutl -derive -inkey private_key.pem -peerkey TA_key.pem -out shared_secret.bin
echo "Secret code" > message.txt
openssl enc -aes-256-cbc -pbkdf2 -in message.txt -out message.enc -pass file:shared_secret.bin
openssl enc -aes-256-cbc -d -pbkdf2 -in message.enc -out message.dec -pass file:shared_secret.bin
diff message.txt message.dec
cat message.dec

e1.sh                                                                    1,1          All
```

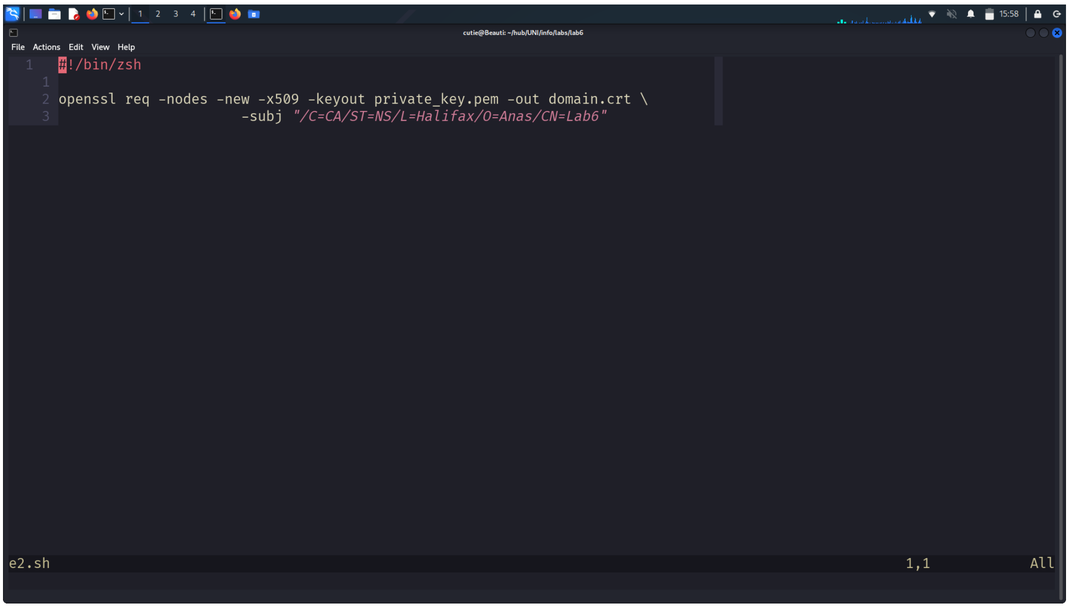
Exercise 1 script


cutie@Beauti: ~/hub/UNI/info/labs/lab6
File Actions Edit View Help

```
┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ ./e1.sh
Secret code

┌──(cutie㉿Beauti)-[~/…/UNI/info/labs/lab6]
└─$ 
```

script check



cutie@Beauti: ~/hub/UNI/info/labs/lab6
File Actions Edit View Help
15:58

```
#!/bin/zsh

openssl req -nodes -new -x509 -keyout private_key.pem -out domain.crt \
                        -subj "/C=CA/ST=NS/L=Halifax/O=Anas/CN=Lab6"
```

```
e2.sh                                                                   1,1           All
```

Exercise 2 script

3.1 Algorithms:

We can use the command “openssl ciphers -v” to list all of the available algorithms, some that I have access to are:

1. AES(256)
2. AESCCM8(256)
3. Camellia(256)
4. SEED(128)
5. CHACHA20/POLY1305(256)