Workshop 5 – Digital Signatures and Key Exchange

Task 1: Review Important Concepts

1. What are the principal elements of a digital signature system?

   Answer:

   The most basic elements of the digital signature system are:

   - For the message sender:
     - Signature, σ
     - Sender's private key, PR_b
     - Message, M

     Signing function: $\sigma = Sign(PR_b, M)$
     Data sent: (M, σ)

   - For the message receiver:
     - Signature, σ
     - Sender's Public key, PU_b
     - Message, M

     Verifying function: $Verify(PU_b, M, \sigma)$

   However, digitally signing large documents is not practical, the same way as using public key encryption on large files is not practical which lead to the adoption of hybrid encryption.

   Since hash functions produce a digest of fixed length that is unique, where any small change in the message will translate to noticeable changes in the hash function output.

   This means signing the hash value of the message is equivalent to signing the complete original message in term of producing a unique hash digest.

   Therefore the same principle mentioned above is still used except the message is used in a precursory step, that is hashing the message, and this hash is used in the signing process.

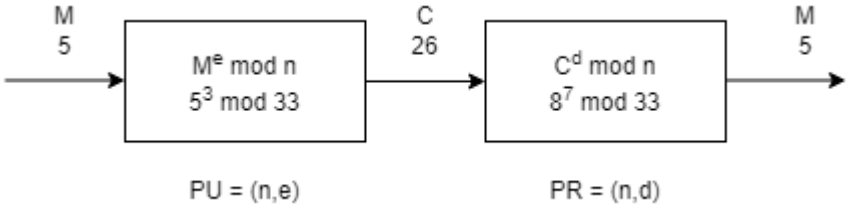
   Signing message:
   Calculate the hash digest:
   $h = H(M)$
   Calculate the signature, $\sigma = Sign(PR, h)$
   Data sent: (M, σ)

Verification by the receiver: Verify(PU,M, σ)

Compute the hash value using the received message: h = H(M)

Compare the value of h to σ^e mod n

Below is proof how this verification process works:



	Signing	Verification
Signing Plain message	$\sigma = M^d \bmod n$ $= 5^3 \bmod 33$ $= 14$	$\sigma^e \bmod n = 14^3 \bmod 33$ $= 5$
Signing encrypted Message	$\sigma = M^d \bmod n$ $= 26^7 \bmod 33$ $= 5$	$\sigma^e \bmod n = 5^3 \bmod 33$ $= 26$

2. What is an existential forgery for digital signature systems? Why do we want to prevent that?

Answer:

Existential forgery is the fraudulent creation of a digital signature by an unauthorized party that does not know the private key, d in PR = (n,d). If the signature of the sender is not immune e to existential forgery, then the signature is said to not be trustworthy.

Forging a counterfeit signature is usually done through a process called chosen-message attack, this is where an attacker produces a signature that can be verified using the senders public key.

The attacker might be working on forgery via passive attack techniques such as interacting with the senders signing machine, whereby the attacker tries to get as many signature samples as possible for the given messages.

This attack technique is similar to the concept of collision resistance, second preimage resistance and preimage resistance in cryptographic hash functions (covered in workshop 3).

It is necessary that a digital signature be unforgeable even if the user can enumerate a large sample of messages.

In order to prevent existential forgery, the signing process uses hashing of the original message before signing since hashing functions create a unique digest

for the slightest change in the message file (see Workshop 3 to see md5 and sha256 in terms of finding collisions to hashes).

Signing with hashing add an additional layer of difficulty for the attacker similar to the concept of diffusion and confusion in product ciphers, however this is not an exact parallel analogy as hashing for unique digest is not the same as using block ciphers for large data files.

3. Is Diffie-Hellman key exchange a public-key encryption system or a digital signature system?

Answer:

Diffie-Hellman key exchange is not a public key encryption system or a digital signature system. It is a method for two parties that want to be involved in secure communication to securely build a secret key together in the private space of their own systems, rather than exchange it through the public network. There is no key "exchange" over the network only public variables for both parties to develop a shared secret key using their private variables. This way both parties' creates the same key.

So, this method is used to share some public numbers, and use private variables to get a shared secret key no one else can know

This method would perhaps be used at the beginning of a conversation to derive a secret key for (symmetric) encryption between two parties.

It is used at the beginning, before conversations, before encrypted message exchange or digital signature is initiated.

4. What is a digital certificate used for? What information does a digital certificate contain?

Answer:

Digital certification is the use of a third party, that is the certificate authority, to sign public keys of parties on the network. Certificate authorities are used to:

a) Resister public key, and/or
b) Verify public keys

Certificate authorities allow users to verify and register public keys, they wish to share with others on the network, (a). Or to verify that the public key one wishes to use truly belong to the intended client or end user, i.e. authentication, (b).

The digital certificate of the certificate authority is trusted, based on this trust public keys are registered and verified. This way the public keys to be used are trusted.

Digital certification prevents man-in-the middle attacks by, for example an attacker, Eve. Eve may masquerade to two parties, for example Eve may masquerade to Bob as Alice and pretend to give Bob Alice's public key and the same to Alice. In this example, Bob and Alice cannot know that Eve is masquerading to Bob as Alice, and to Alice as Bob during public key exchange. Digital certificates prevent such attacks.

Task 2: Use RSA Tools from OpenSSL

In this task, we perform RSA operations using OpenSSL.

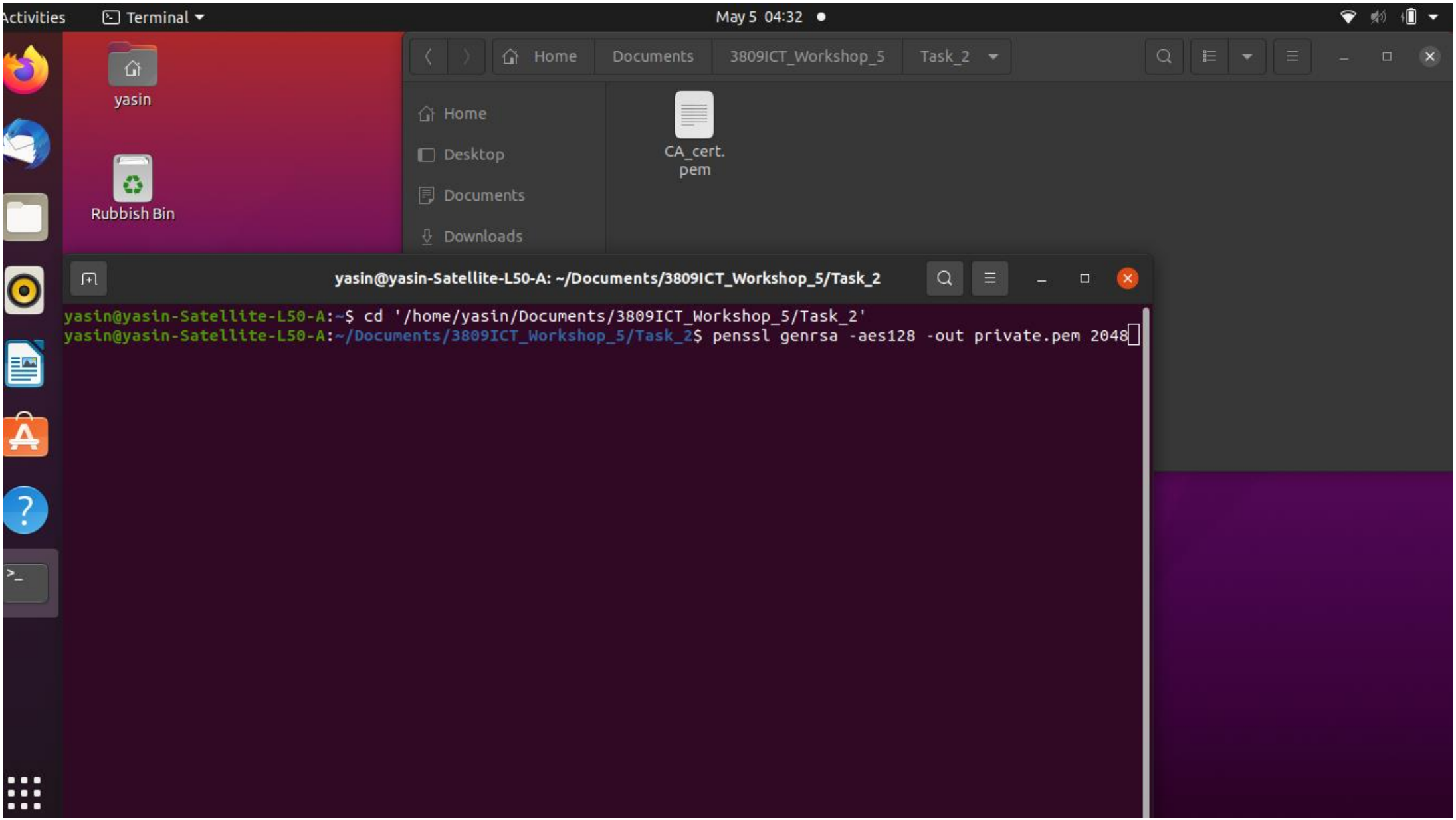
1. We first generate an RSA public/private key pair. We specify the modulo number n to be 2048 bits, which is recommended for Internet security communication.

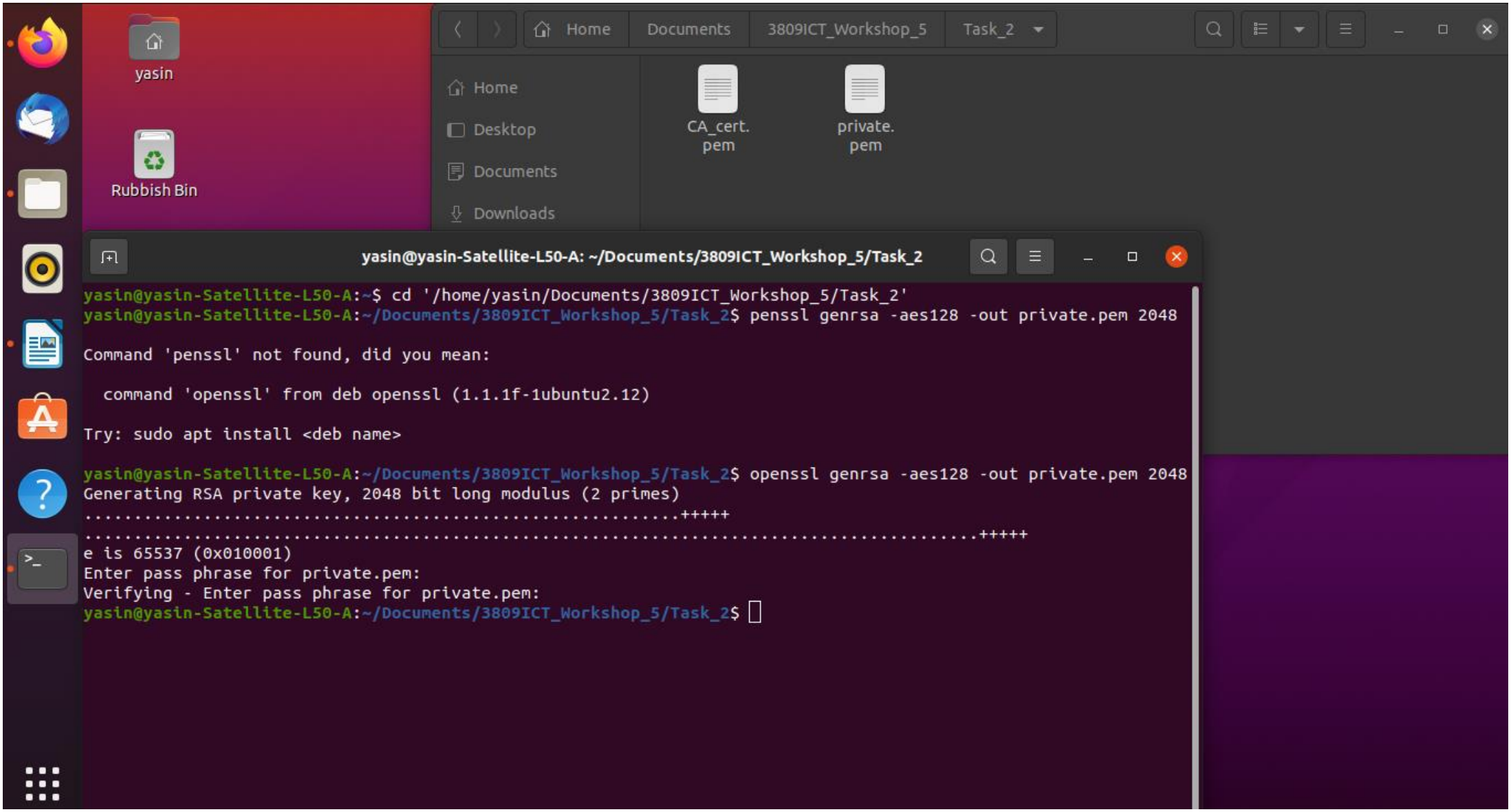
   ```
   $ openssl genrsa -aes128 -out private.pem 2048
   ```

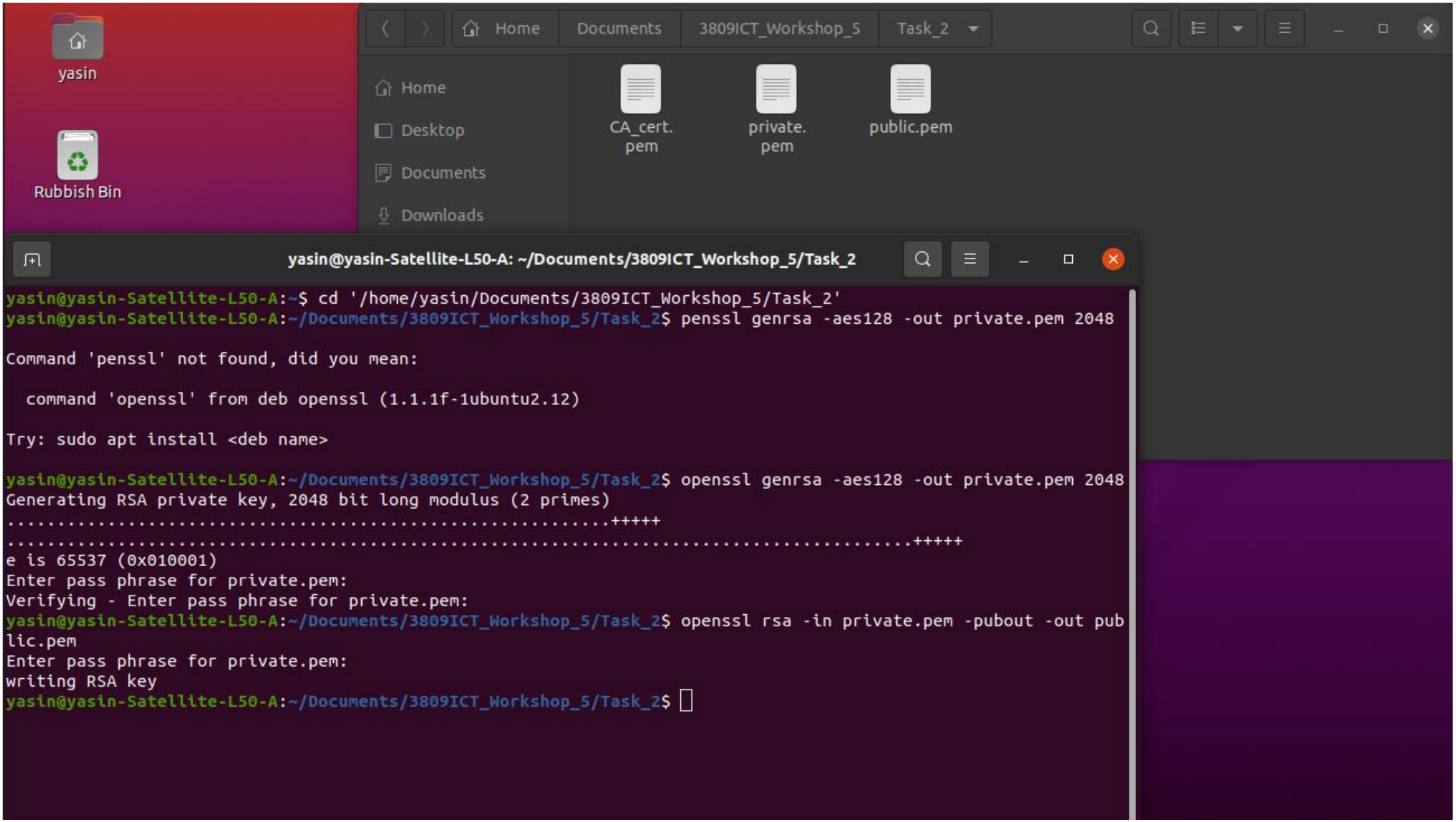
   You will be asked to entre a passphrase (password). The passphrase is used to generate an AES key to encrypt the private key file private.pem.

   ```
   $ openssl rsa -in private.pem -pubout -out public.pem
   ```

   Answer:


Activities
Terminal
May 5 04:32
yasin
Rubbish Bin
Home
Documents
3809ICT_Workshop_5
Task_2
Home
Desktop
Documents
Downloads
CA_cert.
pem
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_2
yasin@yasin-Satellite-L50-A:~$ cd '/home/yasin/Documents/3809ICT_Workshop_5/Task_2'
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ penssl genrsa -aes128 -out private.pem 2048


yasin
Rubbish Bin
Home
Documents
3809ICT_Workshop_5
Task_2
Home
Desktop
Documents
Downloads
CA_cert.
pem
private.
pem
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_2
yasin@yasin-Satellite-L50-A:~$ cd '/home/yasin/Documents/3809ICT_Workshop_5/Task_2'
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ penssl genrsa -aes128 -out private.pem 2048
Command 'penssl' not found, did you mean:
command 'openssl' from deb openssl (1.1.1f-1ubuntu2.12)
Try: sudo apt install <deb name>
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ openssl genrsa -aes128 -out private.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for private.pem:
Verifying - Enter pass phrase for private.pem:
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$


yasin
Rubbish Bin
Home
Documents
3809ICT_Workshop_5
Task_2
Home
Desktop
Documents
Downloads
CA_cert.pem
private.pem
public.pem
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_2
yasin@yasin-Satellite-L50-A:~$ cd '/home/yasin/Documents/3809ICT_Workshop_5/Task_2'
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ penssl genrsa -aes128 -out private.pem 2048
Command 'penssl' not found, did you mean:
command 'openssl' from deb openssl (1.1.1f-1ubuntu2.12)
Try: sudo apt install <deb name>
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ openssl genrsa -aes128 -out private.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for private.pem:
Verifying - Enter pass phrase for private.pem:
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ openssl rsa -in private.pem -pubout -out public.pem
Enter pass phrase for private.pem:
writing RSA key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$

2. Sign your name using the provide key and the hash function SHA-256.

```
$ echo “Your Name” > msg.txt
$ openssl dgst -sha256 -sign private.pem -out signature_name
msg.txt
```

Q: Check the size of the signature file. What is it? Does the signature file contain the message? Why?

Answer:

Here the hash value of the message file is signed rather than the message itself.

The sha256 hash algorithm outputs a 256 bit digest, the hash value is signed using the private key generated, private.pem, to output a binary signature file, i.e. signature_name using the message file, msg.txt file.

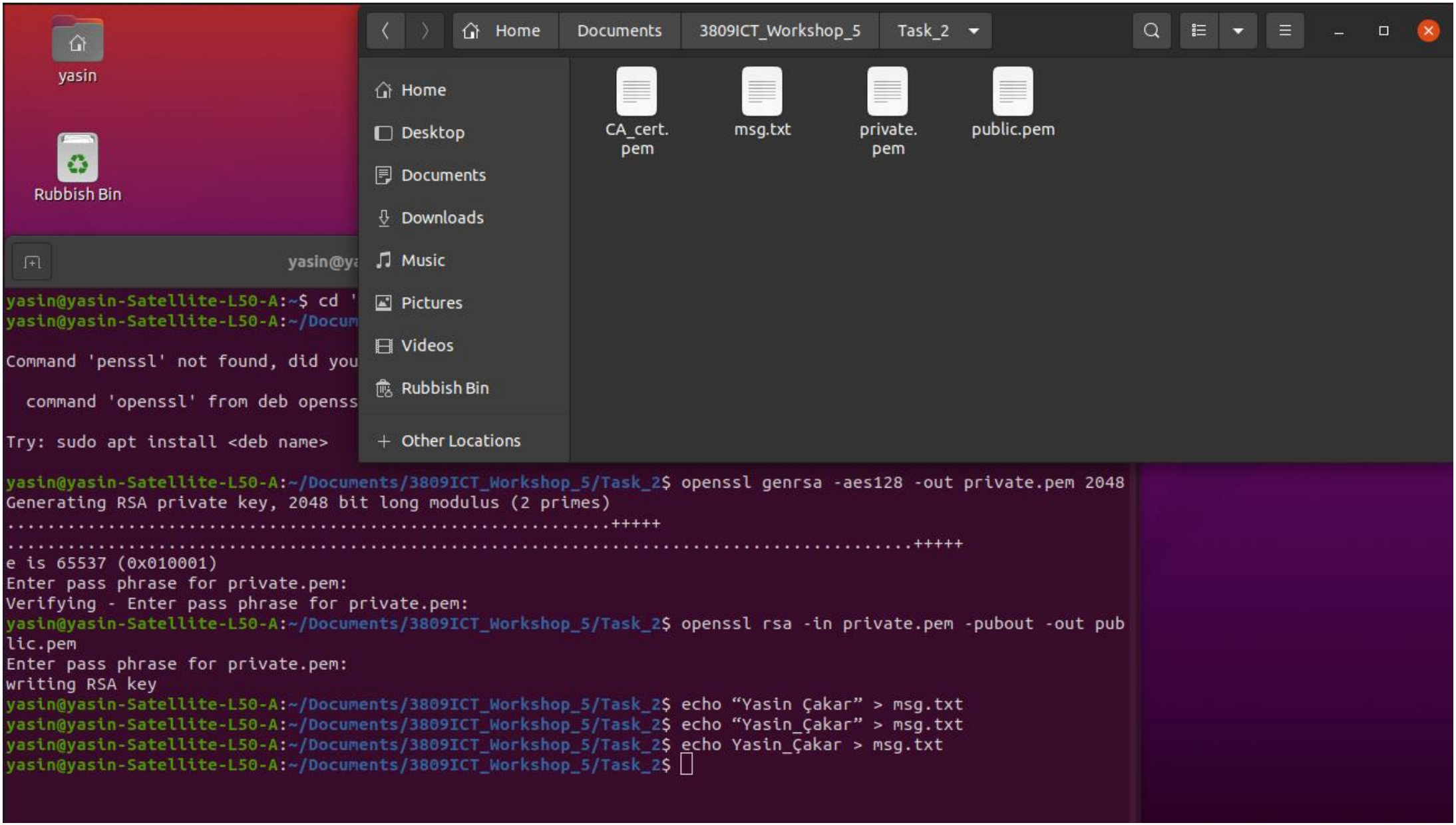
The signature size is 256 bytes because the modulus encodes using 2048 bits, that is the n in $\sigma = \text{Sign}(PR_b, M) = M^d \bmod n$.

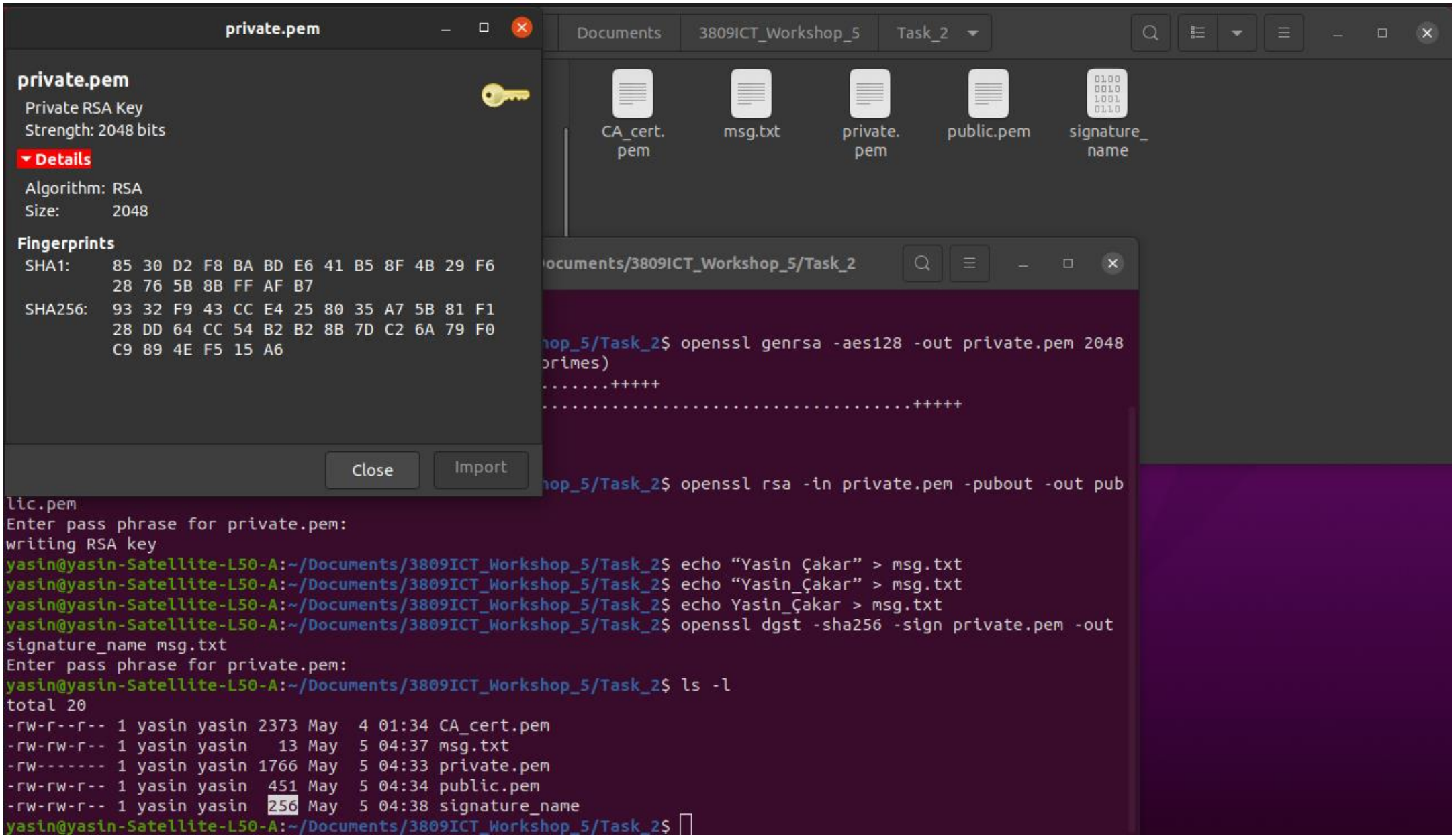
The message file, M, in this example msg.txt is required in it original form (data integrity) to verify.

The hash digest of the message file is being signed not the original message itself.

h = H(M)

The receiver verifies using the sender’s public key, message and the known hashing algorithm sha256, as shown in part 3.


yasin
Rubbish Bin
Home
Documents
3809ICT_Workshop_5
Task_2
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
CA_cert.pem
msg.txt
private.pem
public.pem
yasin@yasin-Satellite-L50-A:~$ cd '
yasin@yasin-Satellite-L50-A:~/Docum
Command 'penssl' not found, did you
command 'openssl' from deb openss
Try: sudo apt install <deb name>
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ openssl genrsa -aes128 -out private.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for private.pem:
Verifying - Enter pass phrase for private.pem:
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ openssl rsa -in private.pem -pubout -out pub
lic.pem
Enter pass phrase for private.pem:
writing RSA key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ echo “Yasin Çakar” > msg.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ echo “Yasin_Çakar” > msg.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ echo Yasin_Çakar > msg.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$

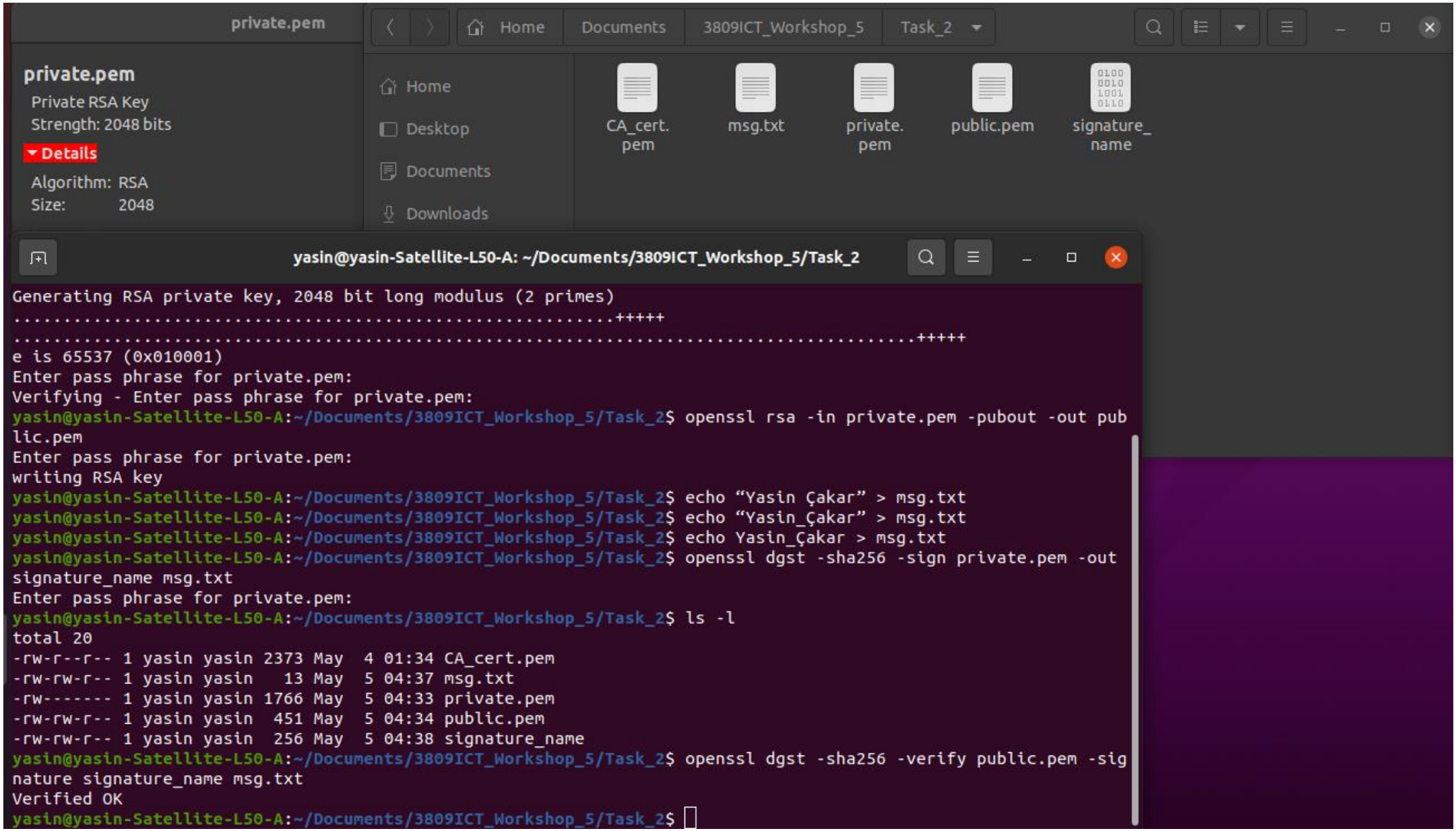

private.pem
private.pem
Private RSA Key
Strength: 2048 bits
Details
Algorithm: RSA
Size: 2048
Fingerprints
SHA1: 85 30 D2 F8 BA BD E6 41 B5 8F 4B 29 F6 28 76 5B 8B FF AF B7
SHA256: 93 32 F9 43 CC E4 25 80 35 A7 5B 81 F1 28 DD 64 CC 54 B2 B2 8B 7D C2 6A 79 F0 C9 89 4E F5 15 A6
Close
Import
Documents
3809ICT_Workshop_5
Task_2
CA_cert.pem
msg.txt
private.pem
public.pem
signature_name
ocuments/3809ICT_Workshop_5/Task_2
hop_5/Task_2$ openssl genrsa -aes128 -out private.pem 2048
primes)
.....+++++
.....+++++
hop_5/Task_2$ openssl rsa -in private.pem -pubout -out pub
lic.pem
Enter pass phrase for private.pem:
writing RSA key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ echo “Yasin Çakar” > msg.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ echo “Yasin_Çakar” > msg.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ echo Yasin_Çakar > msg.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ openssl dgst -sha256 -sign private.pem -out
signature_name msg.txt
Enter pass phrase for private.pem:
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ ls -l
total 20
-rw-r--r-- 1 yasin yasin 2373 May 4 01:34 CA_cert.pem
-rw-rw-r-- 1 yasin yasin 13 May 5 04:37 msg.txt
-rw------- 1 yasin yasin 1766 May 5 04:33 private.pem
-rw-rw-r-- 1 yasin yasin 451 May 5 04:34 public.pem
-rw-rw-r-- 1 yasin yasin 256 May 5 04:38 signature_name
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$

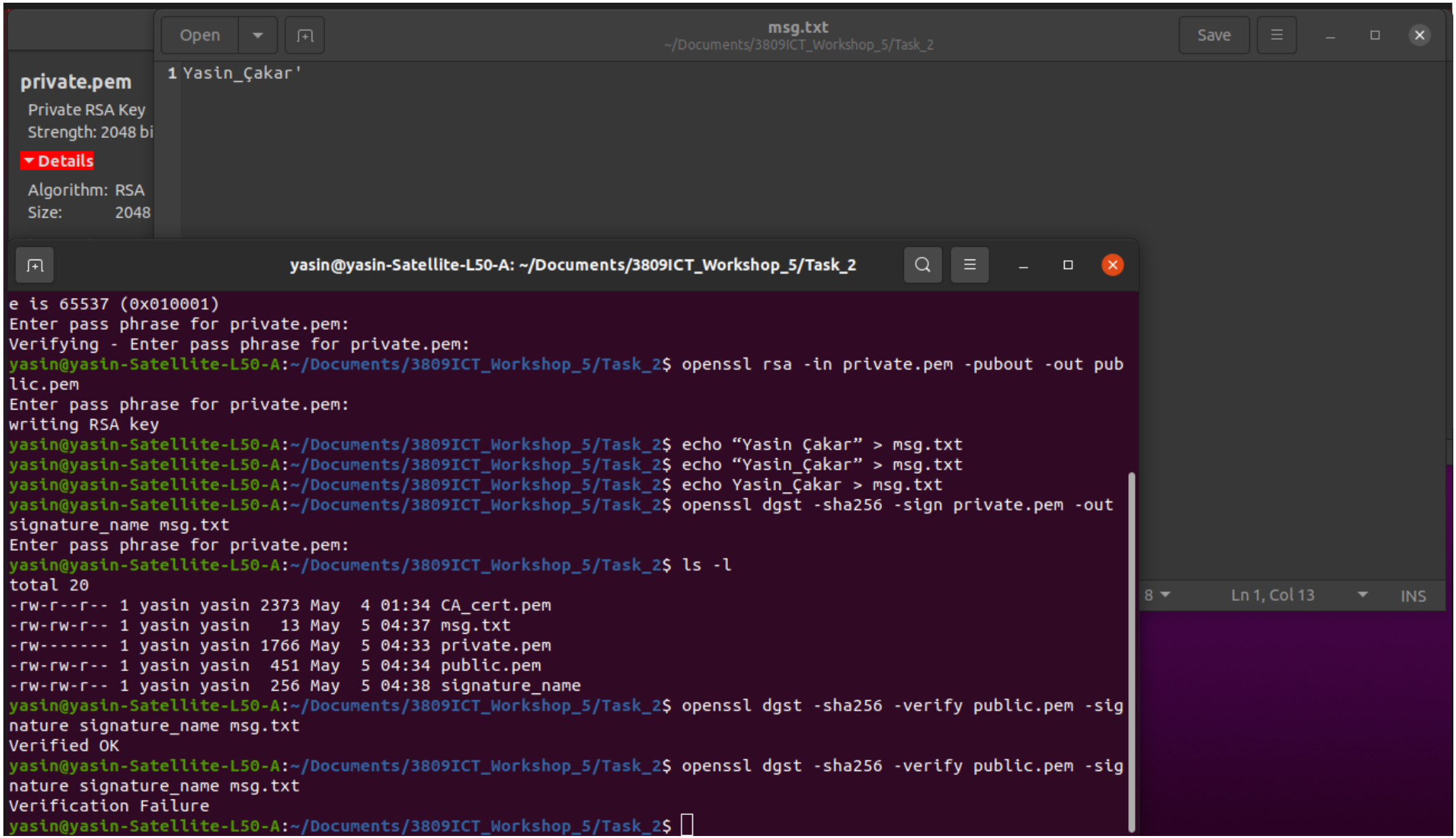
3. Now we verify the signature to see if it is valid or not.

```
$ openssl dgst -sha256 -verify public.pem -signature
signature_name msg.txt
```

Answer:

The example below shows the result when there is an integrity violation as a small change in the message. This change is reflected in the message digest. In the second example the verification fails for this reason.


private.pem
Home
Documents
3809ICT_Workshop_5
Task_2
private.pem
Private RSA Key
Strength: 2048 bits
Details
Algorithm: RSA
Size: 2048
Home
Desktop
Documents
Downloads
CA_cert.pem
msg.txt
private.pem
public.pem
signature_name
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_2
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for private.pem:
Verifying - Enter pass phrase for private.pem:
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ openssl rsa -in private.pem -pubout -out public.pem
Enter pass phrase for private.pem:
writing RSA key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ echo “Yasin Çakar” > msg.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ echo “Yasin_Çakar” > msg.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ echo Yasin_Çakar > msg.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ openssl dgst -sha256 -sign private.pem -out signature_name msg.txt
Enter pass phrase for private.pem:
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ ls -l
total 20
-rw-r--r-- 1 yasin yasin 2373 May 4 01:34 CA_cert.pem
-rw-rw-r-- 1 yasin yasin 13 May 5 04:37 msg.txt
-rw------- 1 yasin yasin 1766 May 5 04:33 private.pem
-rw-rw-r-- 1 yasin yasin 451 May 5 04:34 public.pem
-rw-rw-r-- 1 yasin yasin 256 May 5 04:38 signature_name
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ openssl dgst -sha256 -verify public.pem -signature signature_name msg.txt
Verified OK
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$


Open
msg.txt
~/Documents/3809ICT_Workshop_5/Task_2
Save
1 Yasin_Çakar'
private.pem
Private RSA Key
Strength: 2048 bi
Details
Algorithm: RSA
Size: 2048
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_2
e is 65537 (0x010001)
Enter pass phrase for private.pem:
Verifying - Enter pass phrase for private.pem:
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ openssl rsa -in private.pem -pubout -out pub
lic.pem
Enter pass phrase for private.pem:
writing RSA key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ echo “Yasin Çakar” > msg.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ echo “Yasin_Çakar” > msg.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ echo Yasin_Çakar > msg.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ openssl dgst -sha256 -sign private.pem -out
signature_name msg.txt
Enter pass phrase for private.pem:
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ ls -l
total 20
-rw-r--r-- 1 yasin yasin 2373 May 4 01:34 CA_cert.pem
-rw-rw-r-- 1 yasin yasin 13 May 5 04:37 msg.txt
-rw------- 1 yasin yasin 1766 May 5 04:33 private.pem
-rw-rw-r-- 1 yasin yasin 451 May 5 04:34 public.pem
-rw-rw-r-- 1 yasin yasin 256 May 5 04:38 signature_name
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ openssl dgst -sha256 -verify public.pem -sig
nature signature_name msg.txt
Verified OK
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ openssl dgst -sha256 -verify public.pem -sig
nature signature_name msg.txt
Verification Failure
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$
8
Ln 1, Col 13
INS

Task 3: Verifying X.509 Digital Certificate

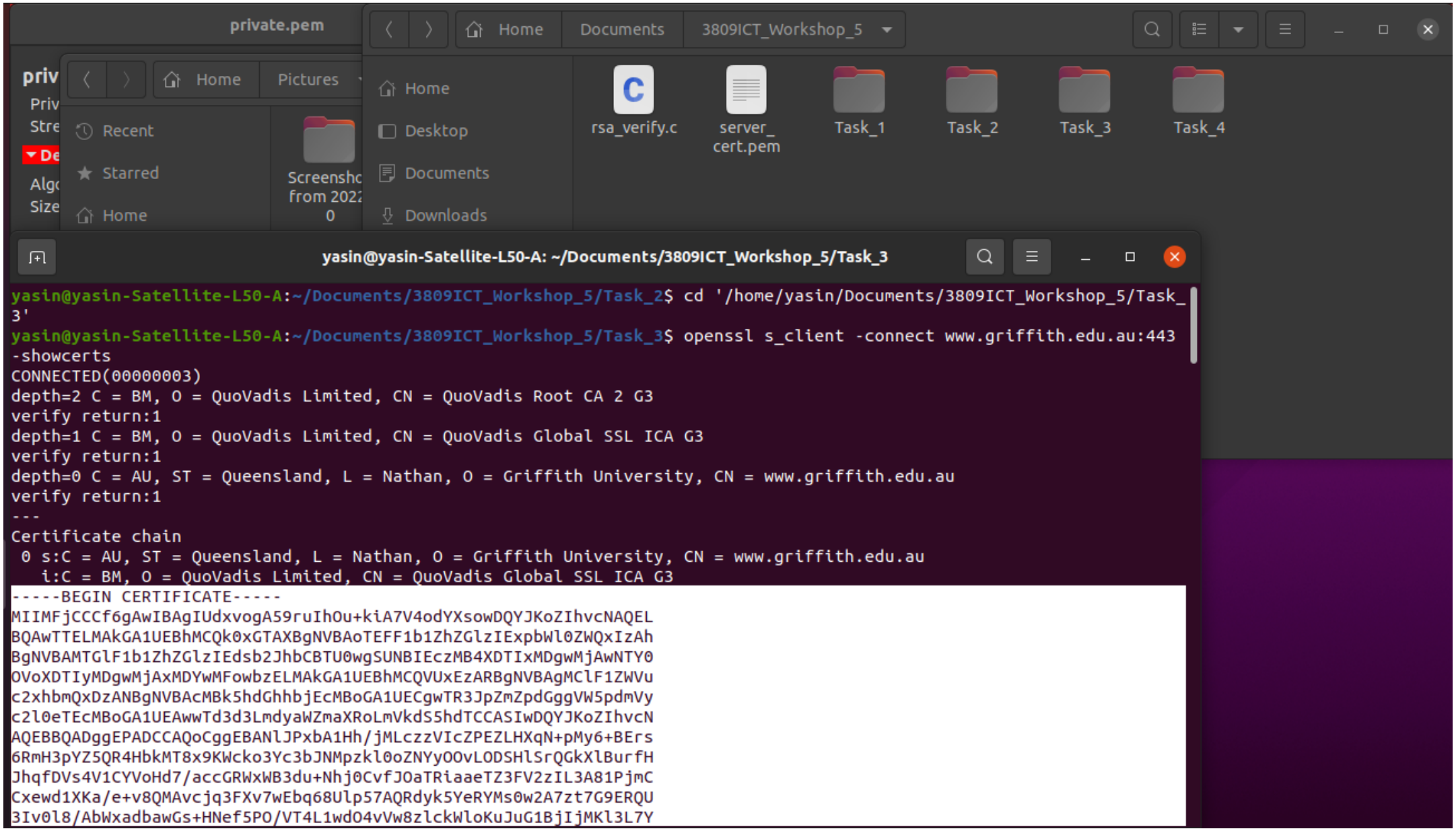
This task is to manually verify a digital certificate. It is to help you understand the internal verification process of verifying X.509 digital certificates. Failure in signature verification of certificate is often the reason that why your web browser warns you that it is insecure to connect to the URL you specified.

1. Download the two digital certificate files CA_cert.pem and server_cert.pem from the Week 6 folder on http://networksecurity.griffith.internal/ via the VM's web browser. These two certificate files are obtained from www.griffith.edu.au. The are the certificate of the university issued (and signed) by a trusted authority. The following command can be used to retrieve the certificates (you don't run this command as you do not have Internet connection in VM).

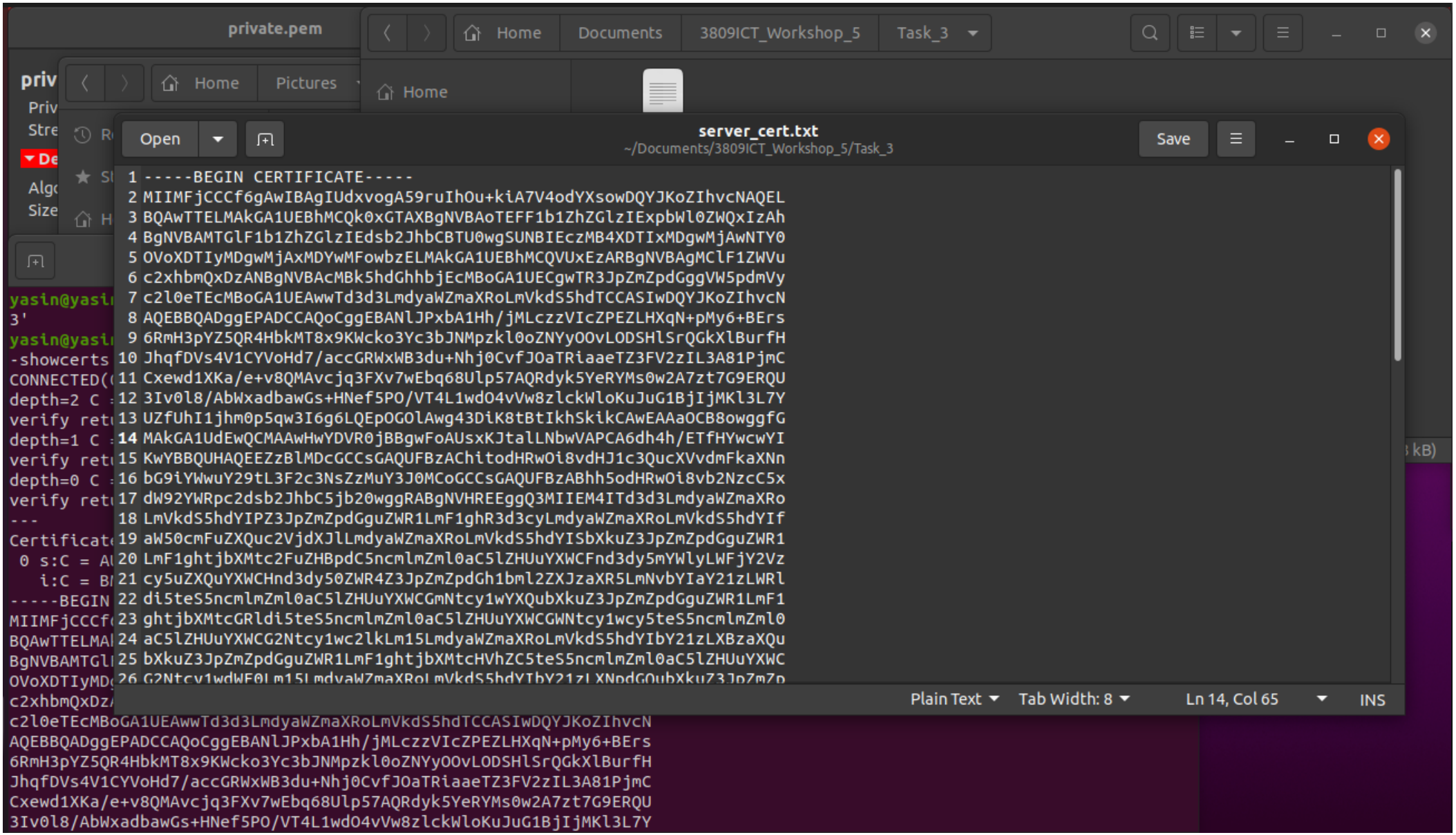
   ```
   $ openssl s_client -connect www.griffith.edu.au:443 -showcerts
   ```

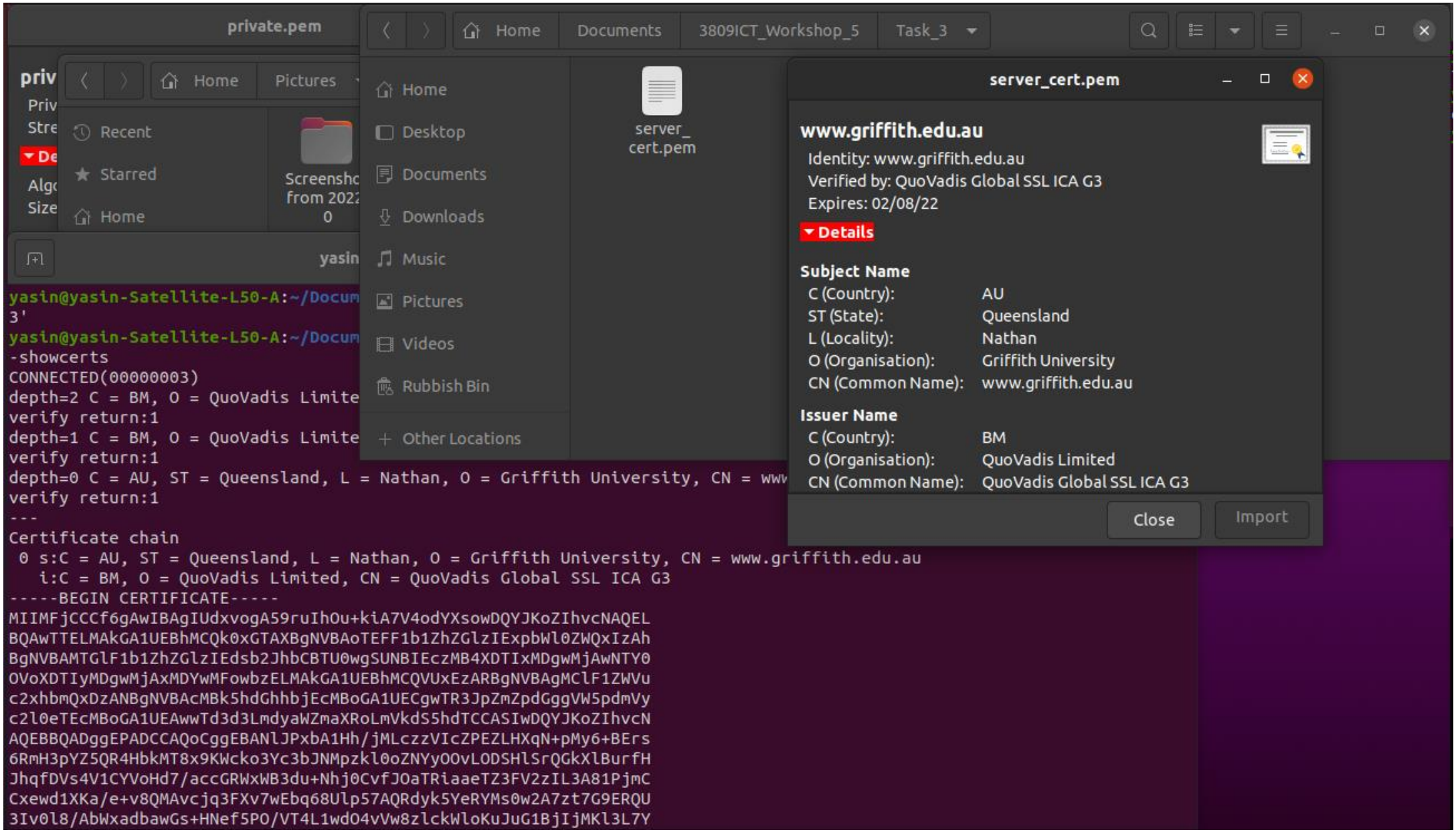
   Answer:

   ```
   Certificates created as per tutors instructions
   ```

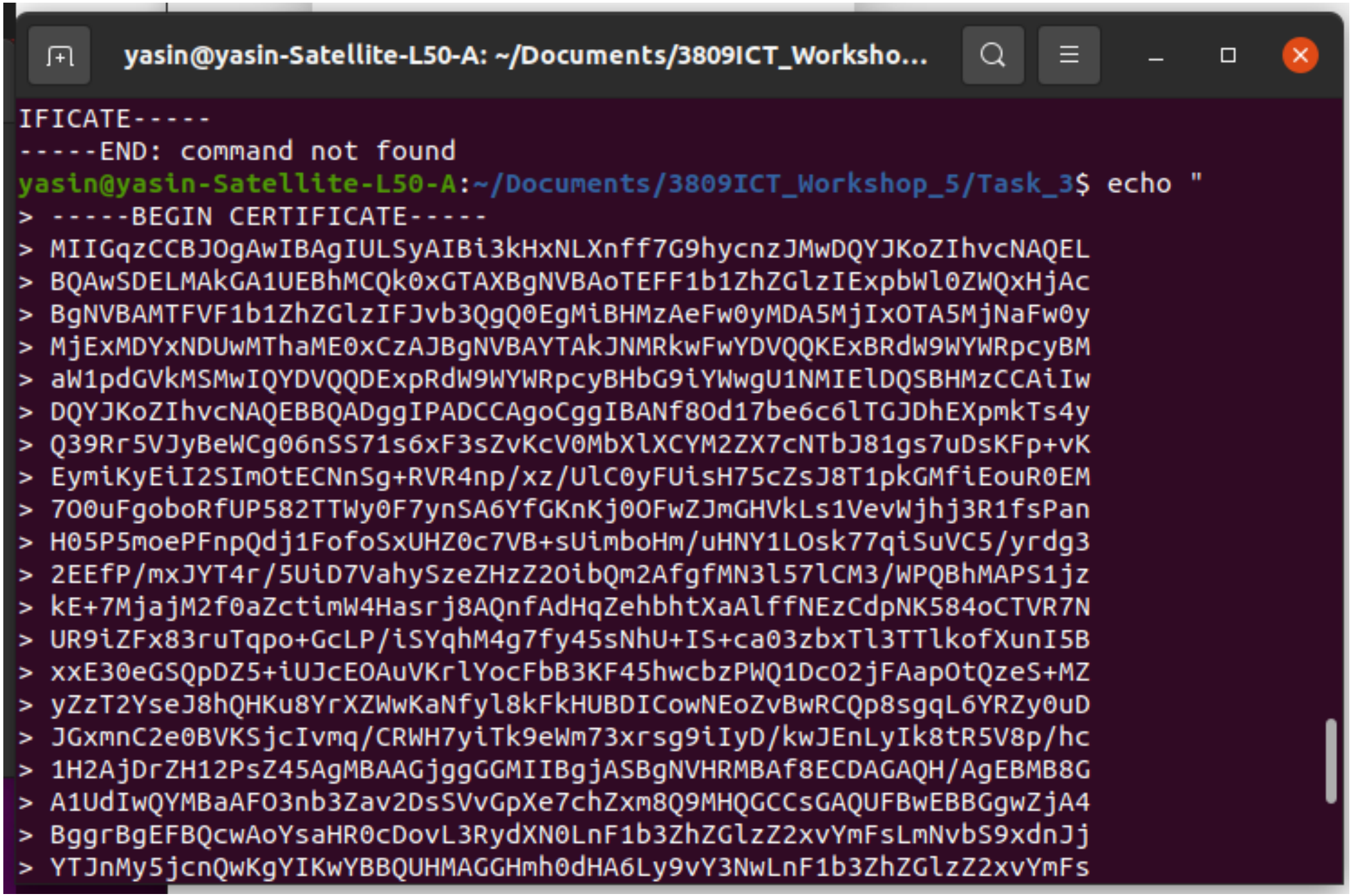

private.pem
Home
Pictures
Recent
Starred
Home
Screensho
from 2022
0
Home
Documents
3809ICT_Workshop_5
Home
Desktop
Documents
Downloads
rsa_verify.c
server_
cert.pem
Task_1
Task_2
Task_3
Task_4
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_3
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_2$ cd '/home/yasin/Documents/3809ICT_Workshop_5/Task_3'
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_3$ openssl s_client -connect www.griffith.edu.au:443 -showcerts
CONNECTED(00000003)
depth=2 C = BM, O = QuoVadis Limited, CN = QuoVadis Root CA 2 G3
verify return:1
depth=1 C = BM, O = QuoVadis Limited, CN = QuoVadis Global SSL ICA G3
verify return:1
depth=0 C = AU, ST = Queensland, L = Nathan, O = Griffith University, CN = www.griffith.edu.au
verify return:1

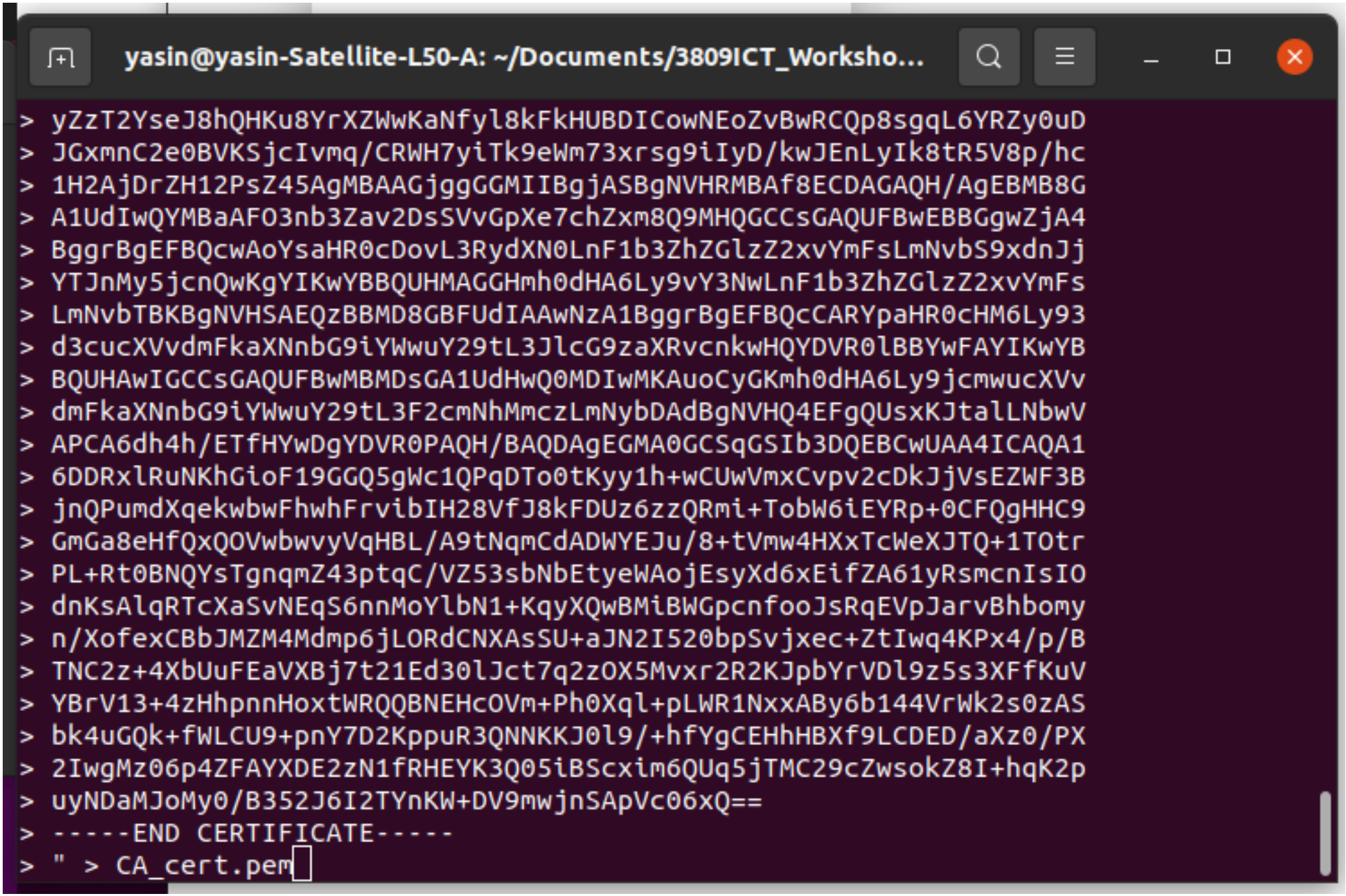
Certificate chain
 0 s:C = AU, ST = Queensland, L = Nathan, O = Griffith University, CN = www.griffith.edu.au
   i:C = BM, O = QuoVadis Limited, CN = QuoVadis Global SSL ICA G3
-----BEGIN CERTIFICATE-----
MIIMFjCCCf6gAwIBAgIUdxvogA59ruIhOu+kiA7V4odYXsowDQYJKoZIhvcNAQEL
BQAwTTELMAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxIzAh
BgNVBAMTGlF1b1ZhZGlzIEdsb2JhbCBTU0wgSUNBIEczMB4XDTIxMDgwMjAwNTY0
OVoXDTIyMDgwMjAxMDYwMFowbzELMAkGA1UEBhMCQVUxEzARBgNVBAgMClF1ZWVu
c2xhbmQxDzANBgNVBAcMBk5hdGhhbjEcMBoGA1UECgwTR3JpZmZpdGggVW5pdmVy
c2l0eTEcMBoGA1UEAwwTd3d3LmdyaWZmaXRoLmVkdS5hdTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBANlJPxbA1Hh/jMLczzVIcZPEZLHXqN+pMy6+BErs
6RmH3pYZ5QR4HbkMT8x9KWcko3Yc3bJNMpzkl0oZNYyOOvLODSHlSrQGkXlBurfH
JhqfDVs4V1CYVoHd7/accGRWxWB3du+Nhj0CvfJOaTRiaaeTZ3FV2zIL3A81PjmC
Cxewd1XKa/e+v8QMAvcjq3FXv7wEbq68Ulp57AQRdyk5YeRYMs0w2A7zt7G9ERQU
3Iv0l8/AbWxadbawGs+HNef5PO/VT4L1wdO4vVw8zlckWloKuJuG1BjIjMKl3L7Y

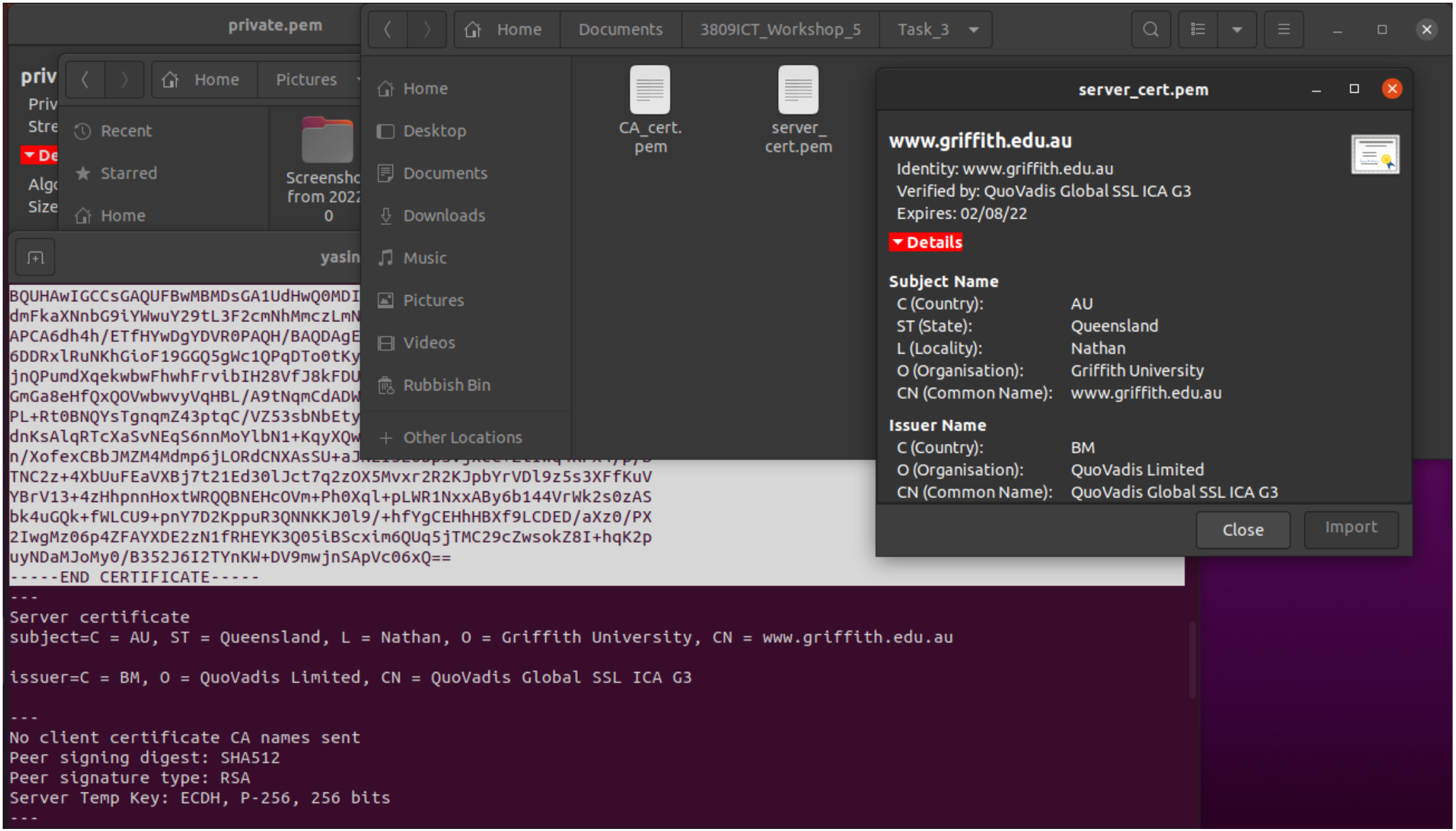

private.pem
Home
Documents
3809ICT_Workshop_5
Task_3
Home
Pictures
Home
Open
server_cert.txt
~/Documents/3809ICT_Workshop_5/Task_3
Save
-----BEGIN CERTIFICATE-----
MIIMFjCCCf6gAwIBAgIUdxvogA59ruIhOu+kiA7V4odYXsowDQYJKoZIhvcNAQEL
BQAwTTELMAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxIzAh
BgNVBAMTGlF1b1ZhZGlzIEdsb2JhbCBTU0wgSUNBIEczMB4XDTIxMDgwMjAwNTY0
OVoXDTIyMDgwMjAxMDYwMFowbzELMAkGA1UEBhMCQVUxEzARBgNVBAgMClF1ZWVu
c2xhbmQxDzANBgNVBAcMBk5hdGhhbjEcMBoGA1UECgwTR3JpZmZpdGggVW5pdmVy
c2l0eTEcMBoGA1UEAwwTd3d3LmdyaWZmaXRoLmVkdS5hdTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBANlJPxbA1Hh/jMLczzVIcZPEZLHXqN+pMy6+BErs
6RmH3pYZ5QR4HbkMT8x9KWcko3Yc3bJNMpzkl0oZNYyOOvLODSHlSrQGkXlBurfH
JhqfDVs4V1CYVoHd7/accGRWxWB3du+Nhj0CvfJOaTRiaaeTZ3FV2zIL3A81PjmC
Cxewd1XKa/e+v8QMAvcjq3FXv7wEbq68Ulp57AQRdyk5YeRYMs0w2A7zt7G9ERQU
3Iv0l8/AbWxadbawGs+HNef5PO/VT4L1wdO4vVw8zlckWloKuJuG1BjIjMKl3L7Y
UZfUhI1jhm0p5qw3I6g6LQEpOGOlAwg43DiK8tBtIkhSkikCAwEAAaOCB8owggfG
MAkGA1UdEwQCMAAwHwYDVR0jBBgwFoAUsxKJtalLNbwVAPCA6dh4h/ETfHYwcwYI
KwYBBQUHAQEEZzBlMDcGCCsGAQUFBzAChitodHRwOi8vdHJ1c3QucXVvdmFkaXNn
bG9iYWwuY29tL3F2c3NsZzMuY3J0MCoGCCsGAQUFBzABhh5odHRwOi8vb2NzcC5x
dW92YWRpc2dsb2JhbC5jb20wggRABgNVHREEggQ3MIIEM4ITd3d3LmdyaWZmaXRo
LmVkdS5hdYIPZ3JpZmZpdGguZWR1LmF1ghR3d3cyLmdyaWZmaXRoLmVkdS5hdYIf
aW50cmFuZXQuc2VjdXJlLmdyaWZmaXRoLmVkdS5hdYISbXkuZ3JpZmZpdGguZWR1
LmF1ghtjbXMtc2FuZHBpdC5ncmlmZml0aC5lZHUuYXWCFnd3dy5mYWlyLWFjY2Vz
cy5uZXQuYXWCHnd3dy50ZWR4Z3JpZmZpdGh1bml2ZXJzaXR5LmNvbYIaY21zLWRl
di5teS5ncmlmZml0aC5lZHUuYXWCGmNtcy1wYXQubXkuZ3JpZmZpdGguZWR1LmF1
ghtjbXMtcGRldi5teS5ncmlmZml0aC5lZHUuYXWCGWNtcy1wcy5teS5ncmlmZml0
aC5lZHUuYXWCG2Ntcy1wc2lkLm15LmdyaWZmaXRoLmVkdS5hdYIbY21zLXBzaXQu
bXkuZ3JpZmZpdGguZWR1LmF1ghtjbXMtcHVhZC5teS5ncmlmZml0aC5lZHUuYXWC
G2Ntcy1wdWF0Lm15LmdyaWZmaXRoLmVkdS5hdYIbY21zLXNpdGQubXkuZ3JpZmZp
Plain Text
Tab Width: 8
Ln 14, Col 65
INS


private.pem
Home
Pictures
Recent
Starred
Home
Screensho
from 2022
0
yasin
Home
Documents
3809ICT_Workshop_5
Task_3
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
server_
cert.pem
server_cert.pem
www.griffith.edu.au
Identity: www.griffith.edu.au
Verified by: QuoVadis Global SSL ICA G3
Expires: 02/08/22
Details
Subject Name
C (Country): AU
ST (State): Queensland
L (Locality): Nathan
O (Organisation): Griffith University
CN (Common Name): www.griffith.edu.au
Issuer Name
C (Country): BM
O (Organisation): QuoVadis Limited
CN (Common Name): QuoVadis Global SSL ICA G3
Close
Import
yasin@yasin-Satellite-L50-A:~/Docum
3'
yasin@yasin-Satellite-L50-A:~/Docum
-showcerts
CONNECTED(00000003)
depth=2 C = BM, O = QuoVadis Limite
verify return:1
depth=1 C = BM, O = QuoVadis Limite
verify return:1
depth=0 C = AU, ST = Queensland, L = Nathan, O = Griffith University, CN = www
verify return:1

Certificate chain
0 s:C = AU, ST = Queensland, L = Nathan, O = Griffith University, CN = www.griffith.edu.au
i:C = BM, O = QuoVadis Limited, CN = QuoVadis Global SSL ICA G3
-----BEGIN CERTIFICATE-----
MIIMFjCCCf6gAwIBAgIUdxvogA59ruIhOu+kiA7V4odYXsowDQYJKoZIhvcNAQEL
BQAwTTELMAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxIzAh
BgNVBAMTGlF1b1ZhZGlzIEdsb2JhbCBTU0wgSUNBIEczMB4XDTIxMDgwMjAwNTY0
OVoXDTIyMDgwMjAxMDYwMFowbzELMAkGA1UEBhMCQVUxEzARBgNVBAgMClF1ZWVu
c2xhbmQxDzANBgNVBAcMBk5hdGhhbjEcMBoGA1UECgwTR3JpZmZpdGggVW5pdmVy
c2l0eTEcMBoGA1UEAwwTd3d3LmdyaWZmaXRoLmVkdS5hdTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBANlJPxbA1Hh/jMLczzVIcZPEZLHXqN+pMy6+BErs
6RmH3pYZ5QR4HbkMT8x9KWcko3Yc3bJNMpzkl0oZNYyOOvLODSHlSrQGkXlBurfH
JhqfDVs4V1CYVoHd7/accGRWxWB3du+Nhj0CvfJOaTRiaaeTZ3FV2zIL3A81PjmC
Cxewd1XKa/e+v8QMAvcjq3FXv7wEbq68Ulp57AQRdyk5YeRYMs0w2A7zt7G9ERQU
3Iv0l8/AbWxadbawGs+HNef5PO/VT4L1wdO4vVw8zlckWloKuJuG1BjIjMKl3L7Y


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Worksho...
IFICATE-----
-----END: command not found
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_3$ echo "
> -----BEGIN CERTIFICATE-----
> MIIGqzCCBJOgAwIBAgIULSyAIBi3kHxNLXnff7G9hycnzJMwDQYJKoZIhvcNAQEL
> BQAwSDELMAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxHjAc
> BgNVBAMTFVF1b1ZhZGlzIFJvb3QgQ0EgMiBHMzAeFw0yMDA5MjIxOTA5MjNaFw0y
> MjExMDYxNDUwMThaME0xCzAJBgNVBAYTAkJNMRkwFwYDVQQKExBRdW9WYWRpcyBM
> aW1pdGVkMSMwIQYDVQQDExpRdW9WYWRpcyBHbG9iYWwgU1NMIElDQSBHMzCCAiIw
> DQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBANf8Od17be6c6lTGJDhEXpmkTs4y
> Q39Rr5VJyBeWCg06nSS71s6xF3sZvKcV0MbXlXCYM2ZX7cNTbJ81gs7uDsKFp+vK
> EymiKyEiI2SImOtECNnSg+RVR4np/xz/UlC0yFUisH75cZsJ8T1pkGMfiEouR0EM
> 7O0uFgoboRfUP582TTWy0F7ynSA6YfGKnKj0OFwZJmGHVkLs1VevWjhj3R1fsPan
> H05P5moePFnpQdj1FofoSxUHZ0c7VB+sUimboHm/uHNY1LOsk77qiSuVC5/yrdg3
> 2EEfP/mxJYT4r/5UiD7VahySzeZHzZ2OibQm2AfgfMN3l57lCM3/WPQBhMAPS1jz
> kE+7MjajM2f0aZctimW4Hasrj8AQnfAdHqZehbhtXaAlffNEzCdpNK584oCTVR7N
> UR9iZFx83ruTqpo+GcLP/iSYqhM4g7fy45sNhU+IS+ca03zbxTl3TTlkofXunI5B
> xxE30eGSQpDZ5+iUJcEOAuVKrlYocFbB3KF45hwcbzPWQ1DcO2jFAapOtQzeS+MZ
> yZzT2YseJ8hQHKu8YrXZWwKaNfyl8kFkHUBDICowNEoZvBwRCQp8sgqL6YRZy0uD
> JGxmnC2e0BVKSjcIvmq/CRWH7yiTk9eWm73xrsg9iIyD/kwJEnLyIk8tR5V8p/hc
> 1H2AjDrZH12PsZ45AgMBAAGjggGGMIIBgjASBgNVHRMBAf8ECDAGAQH/AgEBMB8G
> A1UdIwQYMBaAFO3nb3Zav2DsSVvGpXe7chZxm8Q9MHQGCCsGAQUFBwEBBGgwZjA4
> BggrBgEFBQcwAoYsaHR0cDovL3RydXN0LnF1b3ZhZGlzZ2xvYmFsLmNvbS9xdnJj
> YTJnMy5jcnQwKgYIKwYBBQUHMAGGHmh0dHA6Ly9vY3NwLnF1b3ZhZGlzZ2xvYmFs


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Worksho...
> yZzT2YseJ8hQHKu8YrXZWwKaNfyl8kFkHUBDICowNEoZvBwRCQp8sgqL6YRZy0uD
> JGxmnC2e0BVKSjcIvmq/CRWH7yiTk9eWm73xrsg9iIyD/kwJEnLyIk8tR5V8p/hc
> 1H2AjDrZH12PsZ45AgMBAAGjggGGMIIBgjASBgNVHRMBAf8ECDAGAQH/AgEBMB8G
> A1UdIwQYMBaAFO3nb3Zav2DsSVvGpXe7chZxm8Q9MHQGCCsGAQUFBwEBBGgwZjA4
> BggrBgEFBQcwAoYsaHR0cDovL3RydXN0LnF1b3ZhZGlzZ2xvYmFsLmNvbS9xdnJj
> YTJnMy5jcnQwKgYIKwYBBQUHMAGGHmh0dHA6Ly9vY3NwLnF1b3ZhZGlzZ2xvYmFs
> LmNvbTBKBgNVHSAEQzBBMD8GBFUdIAAwNzA1BggrBgEFBQcCARYpaHR0cHM6Ly93
> d3cucXVvdmFkaXNnbG9iYWwuY29tL3JlcG9zaXRvcnkwHQYDVR0lBBYwFAYIKwYB
> BQUHAwIGCCsGAQUFBwMBMDsGA1UdHwQ0MDIwMKAuoCyGKmh0dHA6Ly9jcmwucXVv
> dmFkaXNnbG9iYWwuY29tL3F2cmNhMmczLmNybDAdBgNVHQ4EFgQUsxKJtalLNbwV
> APCA6dh4h/ETfHYwDgYDVR0PAQH/BAQDAgEGMA0GCSqGSIb3DQEBCwUAA4ICAQA1
> 6DDRxlRuNKhGioF19GGQ5gWc1QPqDTo0tKyy1h+wCUwVmxCvpv2cDkJjVsEZWF3B
> jnQPumdXqekwbwFhwhFrvibIH28VfJ8kFDUz6zzQRmi+TobW6iEYRp+0CFQgHHC9
> GmGa8eHfQxQOVwbwvyVqHBL/A9tNqmCdADWYEJu/8+tVmw4HXxTcWeXJTQ+1TOtr
> PL+Rt0BNQYsTgnqmZ43ptqC/VZ53sbNbEtyeWAojEsyXd6xEifZA61yRsmcnIsIO
> dnKsAlqRTcXaSvNEqS6nnMoYlbN1+KqyXQwBMiBWGpcnfooJsRqEVpJarvBhbomy
> n/XofexCBbJMZM4Mdmp6jLORdCNXAsSU+aJN2I520bpSvjxec+ZtIwq4KPx4/p/B
> TNC2z+4XbUuFEaVXBj7t21Ed30lJct7q2zOX5Mvxr2R2KJpbYrVDl9z5s3XFfKuV
> YBrV13+4zHhpnnHoxtWRQQBNEHcOVm+Ph0Xql+pLWR1NxxABy6b144VrWk2s0zAS
> bk4uGQk+fWLCU9+pnY7D2KppuR3QNNKKJ0l9/+hfYgCEHhHBXf9LCDED/aXz0/PX
> 2IwgMz06p4ZFAYXDE2zN1fRHEYK3Q05iBScxim6QUq5jTMC29cZwsokZ8I+hqK2p
> uyNDaMJoMy0/B352J6I2TYnKW+DV9mwjnSApVc06xQ==
> -----END CERTIFICATE-----
> " > CA_cert.pem


private.pem
Home
Pictures
Recent
Starred
Home
Screensho
from 2022
0
yasin
Home
Documents
3809ICT_Workshop_5
Task_3
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
CA_cert.
pem
server_
cert.pem
server_cert.pem
www.griffith.edu.au
Identity: www.griffith.edu.au
Verified by: QuoVadis Global SSL ICA G3
Expires: 02/08/22
Details
Subject Name
C (Country): AU
ST (State): Queensland
L (Locality): Nathan
O (Organisation): Griffith University
CN (Common Name): www.griffith.edu.au
Issuer Name
C (Country): BM
O (Organisation): QuoVadis Limited
CN (Common Name): QuoVadis Global SSL ICA G3
Close
Import
BQUHAwIGCCsGAQUFBwMBMDsGA1UdHwQ0MDI
dmFkaXNnbG9iYWwuY29tL3F2cmNhMmczLmN
APCA6dh4h/ETfHYwDgYDVR0PAQH/BAQDAgE
6DDRxlRuNKhGioF19GGQ5gWc1QPqDTo0tKy
jnQPumdXqekwbwFhwhFrvibIH28VfJ8kFDU
GmGa8eHfQxQOVwbwvyVqHBL/A9tNqmCdADW
PL+Rt0BNQYsTgnqmZ43ptqC/VZ53sbNbEty
dnKsAlqRTcXaSvNEqS6nnMoYlbN1+KqyXQw
n/XofexCBbJMZM4Mdmp6jLORdCNXAsSU+aJ
TNC2z+4XbUuFEaVXBj7t21Ed30lJct7q2zOX5Mvxr2R2KJpbYrVDl9z5s3XFfKuV
YBrV13+4zHhpnnHoxtWRQQBNEHcOVm+Ph0Xql+pLWR1NxxABy6b144VrWk2s0zAS
bk4uGQk+fWLCU9+pnY7D2KppuR3QNNKKJ0l9/+hfYgCEHhHBXf9LCDED/aXz0/PX
2IwgMz06p4ZFAYXDE2zN1fRHEYK3Q05iBScxim6QUq5jTMC29cZwsokZ8I+hqK2p
uyNDaMJoMy0/B352J6I2TYnKW+DV9mwjnSApVc06xQ==
-----END CERTIFICATE-----

Server certificate
subject=C = AU, ST = Queensland, L = Nathan, O = Griffith University, CN = www.griffith.edu.au
issuer=C = BM, O = QuoVadis Limited, CN = QuoVadis Global SSL ICA G3

No client certificate CA names sent
Peer signing digest: SHA512
Peer signature type: RSA
Server Temp Key: ECDH, P-256, 256 bits
---

2. To verify the validity of server_cert.pem, we need CA's public key (e, n). We extract the modulus n by:

```
$ openssl x509 -in CA_cert.pem -noout -modulus
//return the RSA modulus
```

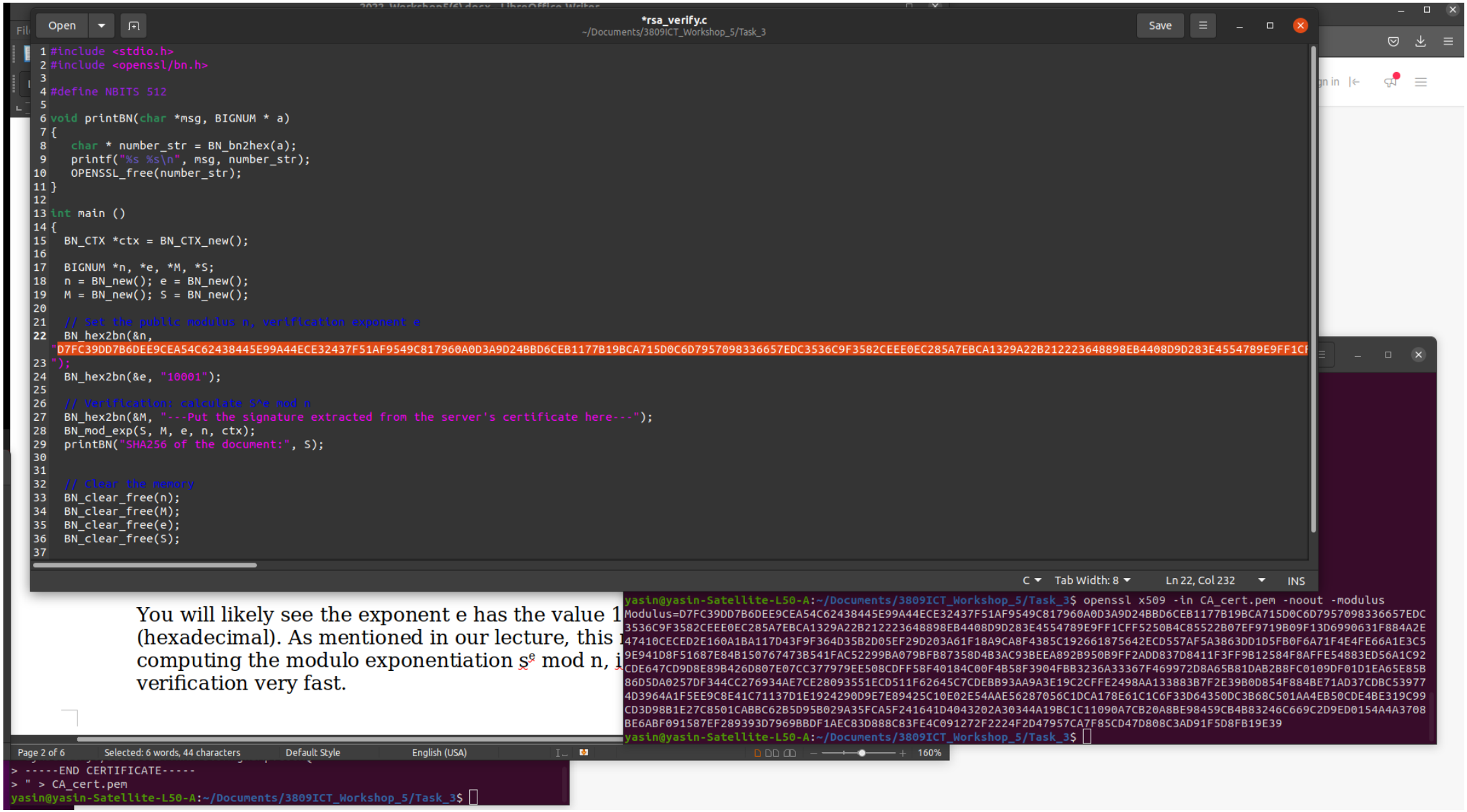
We can display the content of the CA's certificate to see the verification exponent e.

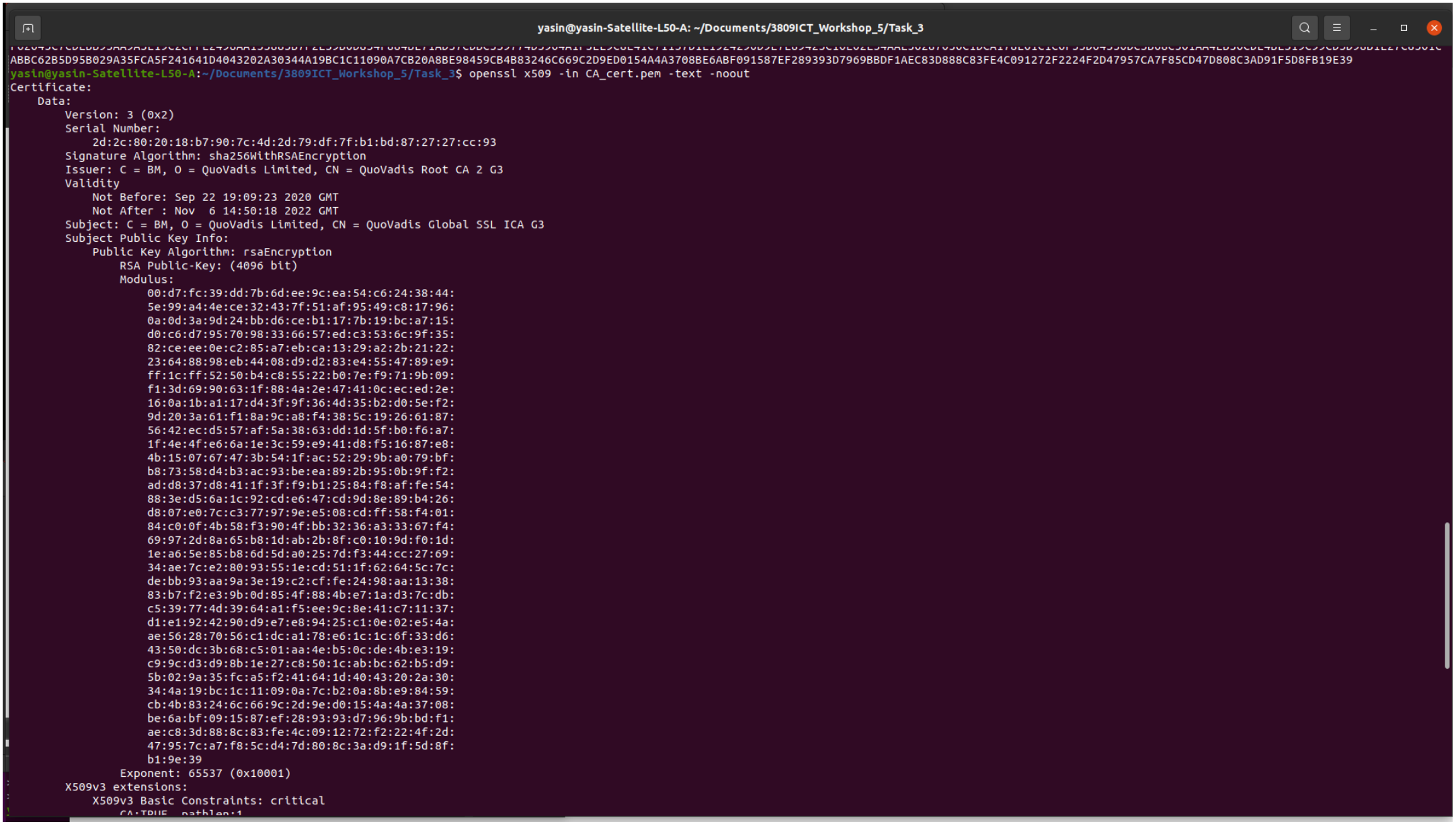
```
$ openssl x509 -in CA_cert.pem -text -noout
```

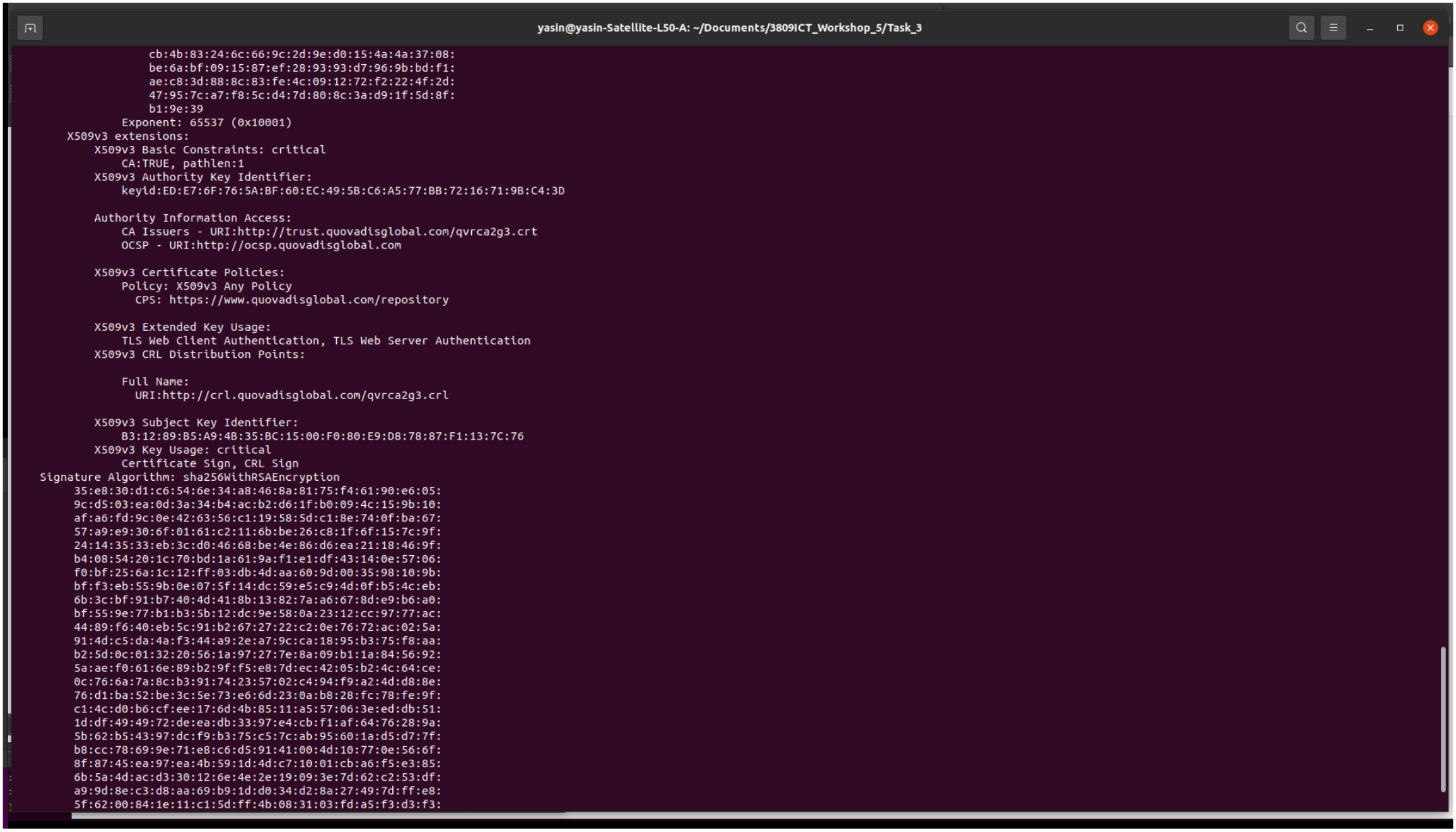
You will likely see the exponent e has the value 10001 (hexadecimal). As mentioned in our lecture, this number makes computing the modulo exponentiation s^e mod n, i.e., signature verification very fast.

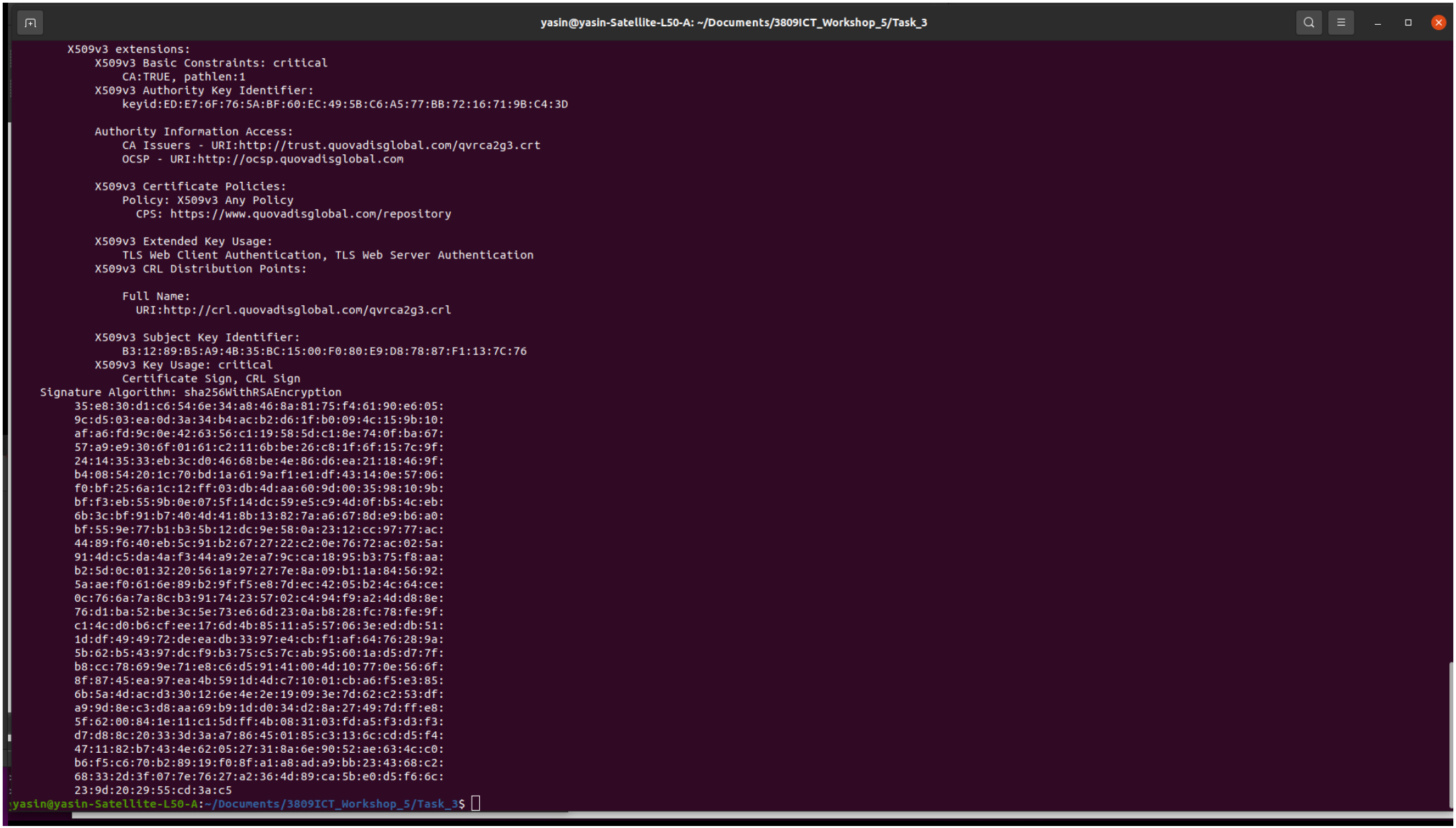
Answer:

In this step the public key from CA_cert.pem to verify the signature of server_cert.pem, PU(e,n) for σ^e mod n to compare with h = H(M)


Open
*rsa_verify.c
~/Documents/3809ICT_Workshop_5/Task_3
Save
#include <stdio.h>
#include <openssl/bn.h>
#define NBITS 512
void printBN(char *msg, BIGNUM * a)
{
char * number_str = BN_bn2hex(a);
printf("%s %s\n", msg, number_str);
OPENSSL_free(number_str);
}
int main ()
{
BN_CTX *ctx = BN_CTX_new();
BIGNUM *n, *e, *M, *S;
n = BN_new(); e = BN_new();
M = BN_new(); S = BN_new();
// Set the public modulus n, verification exponent e
BN_hex2bn(&n,
"D7FC39DD7B6DEE9CEA54C62438445E99A44ECE32437F51AF9549C817960A0D3A9D24BBD6CEB1177B19BCA715D0C6D7957098336657EDC3536C9F3582CEEE0EC285A7EBCA1329A22B212223648898EB4408D9D283E4554789E9FF1CF
");
BN_hex2bn(&e, "10001");
// Verification: calculate 5^e mod n
BN_hex2bn(&M, "---Put the signature extracted from the server's certificate here---");
BN_mod_exp(S, M, e, n, ctx);
printBN("SHA256 of the document:", S);
// Clear the memory
BN_clear_free(n);
BN_clear_free(M);
BN_clear_free(e);
BN_clear_free(S);
C
Tab Width: 8
Ln 22, Col 232
INS
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_3$ openssl x509 -in CA_cert.pem -noout -modulus
Modulus=D7FC39DD7B6DEE9CEA54C62438445E99A44ECE32437F51AF9549C817960A0D3A9D24BBD6CEB1177B19BCA715D0C6D7957098336657EDC
3536C9F3582CEEE0EC285A7EBCA1329A22B212223648898EB4408D9D283E4554789E9FF1CFF5250B4C85522B07EF9719B09F13D6990631F884A2E
47410CECED2E160A1BA117D43F9F364D35B2D05EF29D203A61F18A9CA8F4385C192661875642ECD557AF5A3863DD1D5FB0F6A71F4E4FE66A1E3C5
9E941D8F51687E84B150767473B541FAC52299BA079BFB87358D4B3AC93BEEA892B950B9FF2ADD837D8411F3FF9B12584F8AFFE54883ED56A1C92
CDE647CD9D8E89B426D807E07CC377979EE508CDFF58F40184C00F4B58F3904FBB3236A33367F469972D8A65B81DAB2B8FC0109DF01D1EA65E85B
86D5DA0257DF344CC276934AE7CE28093551ECD511F62645C7CDEBB93AA9A3E19C2CFFE2498AA133883B7F2E39B0D854F884BE71AD37CDBC53977
4D3964A1F5EE9C8E41C71137D1E1924290D9E7E89425C10E02E54AAE56287056C1DCA178E61C1C6F33D64350DC3B68C501AA4EB50CDE4BE319C99
CD3D98B1E27C8501CABBC62B5D95B029A35FCA5F241641D4043202A30344A19BC1C11090A7CB20A8BE98459CB4B83246C669C2D9ED0154A4A3708
BE6ABF091587EF289393D7969BBDF1AEC83D888C83FE4C091272F2224F2D47957CA7F85CD47D808C3AD91F5D8FB19E39
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_3$
You will likely see the exponent e has the value 1
(hexadecimal). As mentioned in our lecture, this
computing the modulo exponentiation s^e mod n, i
verification very fast.
Page 2 of 6
Selected: 6 words, 44 characters
Default Style
English (USA)
160%
> -----END CERTIFICATE-----
> " > CA_cert.pem
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_3$


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_3
ABBC62B5D95B029A35FCA5F241641D4043202A30344A19BC1C11090A7CB20A8BE98459CB4B83246C669C2D9ED0154A4A3708BE6ABF091587EF289393D7969BBDF1AEC83D888C83FE4C091272F2224F2D47957CA7F85CD47D808C3AD91F5D8FB19E39
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_3$ openssl x509 -in CA_cert.pem -text -noout
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
2d:2c:80:20:18:b7:90:7c:4d:2d:79:df:7f:b1:bd:87:27:27:cc:93
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = BM, O = QuoVadis Limited, CN = QuoVadis Root CA 2 G3
Validity
Not Before: Sep 22 19:09:23 2020 GMT
Not After : Nov 6 14:50:18 2022 GMT
Subject: C = BM, O = QuoVadis Limited, CN = QuoVadis Global SSL ICA G3
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (4096 bit)
Modulus:
00:d7:fc:39:dd:7b:6d:ee:9c:ea:54:c6:24:38:44:
5e:99:a4:4e:ce:32:43:7f:51:af:95:49:c8:17:96:
0a:0d:3a:9d:24:bb:d6:ce:b1:17:7b:19:bc:a7:15:
d0:c6:d7:95:70:98:33:66:57:ed:c3:53:6c:9f:35:
82:ce:ee:0e:c2:85:a7:eb:ca:13:29:a2:2b:21:22:
23:64:88:98:eb:44:08:d9:d2:83:e4:55:47:89:e9:
ff:1c:ff:52:50:b4:c8:55:22:b0:7e:f9:71:9b:09:
f1:3d:69:90:63:1f:88:4a:2e:47:41:0c:ec:ed:2e:
16:0a:1b:a1:17:d4:3f:9f:36:4d:35:b2:d0:5e:f2:
9d:20:3a:61:f1:8a:9c:a8:f4:38:5c:19:26:61:87:
56:42:ec:d5:57:af:5a:38:63:dd:1d:5f:b0:f6:a7:
1f:4e:4f:e6:6a:1e:3c:59:e9:41:d8:f5:16:87:e8:
4b:15:07:67:47:3b:54:1f:ac:52:29:9b:a0:79:bf:
b8:73:58:d4:b3:ac:93:be:ea:89:2b:95:0b:9f:f2:
ad:d8:37:d8:41:1f:3f:f9:b1:25:84:f8:af:fe:54:
88:3e:d5:6a:1c:92:cd:e6:47:cd:9d:8e:89:b4:26:
d8:07:e0:7c:c3:77:97:9e:e5:08:cd:ff:58:f4:01:
84:c0:0f:4b:58:f3:90:4f:bb:32:36:a3:33:67:f4:
69:97:2d:8a:65:b8:1d:ab:2b:8f:c0:10:9d:f0:1d:
1e:a6:5e:85:b8:6d:5d:a0:25:7d:f3:44:cc:27:69:
34:ae:7c:e2:80:93:55:1e:cd:51:1f:62:64:5c:7c:
de:bb:93:aa:9a:3e:19:c2:cf:fe:24:98:aa:13:38:
83:b7:f2:e3:9b:0d:85:4f:88:4b:e7:1a:d3:7c:db:
c5:39:77:4d:39:64:a1:f5:ee:9c:8e:41:c7:11:37:
d1:e1:92:42:90:d9:e7:e8:94:25:c1:0e:02:e5:4a:
ae:56:28:70:56:c1:dc:a1:78:e6:1c:1c:6f:33:d6:
43:50:dc:3b:68:c5:01:aa:4e:b5:0c:de:4b:e3:19:
c9:9c:d3:d9:8b:1e:27:c8:50:1c:ab:bc:62:b5:d9:
5b:02:9a:35:fc:a5:f2:41:64:1d:40:43:20:2a:30:
34:4a:19:bc:1c:11:09:0a:7c:b2:0a:8b:e9:84:59:
cb:4b:83:24:6c:66:9c:2d:9e:d0:15:4a:4a:37:08:
be:6a:bf:09:15:87:ef:28:93:93:d7:96:9b:bd:f1:
ae:c8:3d:88:8c:83:fe:4c:09:12:72:f2:22:4f:2d:
47:95:7c:a7:f8:5c:d4:7d:80:8c:3a:d9:1f:5d:8f:
b1:9e:39
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_3
cb:4b:83:24:6c:66:9c:2d:9e:d0:15:4a:4a:37:08:
be:6a:bf:09:15:87:ef:28:93:93:d7:96:9b:bd:f1:
ae:c8:3d:88:8c:83:fe:4c:09:12:72:f2:22:4f:2d:
47:95:7c:a7:f8:5c:d4:7d:80:8c:3a:d9:1f:5d:8f:
b1:9e:39
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:1
X509v3 Authority Key Identifier:
keyid:ED:E7:6F:76:5A:BF:60:EC:49:5B:C6:A5:77:BB:72:16:71:9B:C4:3D
Authority Information Access:
CA Issuers - URI:http://trust.quovadisglobal.com/qvrca2g3.crt
OCSP - URI:http://ocsp.quovadisglobal.com
X509v3 Certificate Policies:
Policy: X509v3 Any Policy
CPS: https://www.quovadisglobal.com/repository
X509v3 Extended Key Usage:
TLS Web Client Authentication, TLS Web Server Authentication
X509v3 CRL Distribution Points:
Full Name:
URI:http://crl.quovadisglobal.com/qvrca2g3.crl
X509v3 Subject Key Identifier:
B3:12:89:B5:A9:4B:35:BC:15:00:F0:80:E9:D8:78:87:F1:13:7C:76
X509v3 Key Usage: critical
Certificate Sign, CRL Sign
Signature Algorithm: sha256WithRSAEncryption
35:e8:30:d1:c6:54:6e:34:a8:46:8a:81:75:f4:61:90:e6:05:
9c:d5:03:ea:0d:3a:34:b4:ac:b2:d6:1f:b0:09:4c:15:9b:10:
af:a6:fd:9c:0e:42:63:56:c1:19:58:5d:c1:8e:74:0f:ba:67:
57:a9:e9:30:6f:01:61:c2:11:6b:be:26:c8:1f:6f:15:7c:9f:
24:14:35:33:eb:3c:d0:46:68:be:4e:86:d6:ea:21:18:46:9f:
b4:08:54:20:1c:70:bd:1a:61:9a:f1:e1:df:43:14:0e:57:06:
f0:bf:25:6a:1c:12:ff:03:db:4d:aa:60:9d:00:35:98:10:9b:
bf:f3:eb:55:9b:0e:07:5f:14:dc:59:e5:c9:4d:0f:b5:4c:eb:
6b:3c:bf:91:b7:40:4d:41:8b:13:82:7a:a6:67:8d:e9:b6:a0:
bf:55:9e:77:b1:b3:5b:12:dc:9e:58:0a:23:12:cc:97:77:ac:
44:89:f6:40:eb:5c:91:b2:67:27:22:c2:0e:76:72:ac:02:5a:
91:4d:c5:da:4a:f3:44:a9:2e:a7:9c:ca:18:95:b3:75:f8:aa:
b2:5d:0c:01:32:20:56:1a:97:27:7e:8a:09:b1:1a:84:56:92:
5a:ae:f0:61:6e:89:b2:9f:f5:e8:7d:ec:42:05:b2:4c:64:ce:
0c:76:6a:7a:8c:b3:91:74:23:57:02:c4:94:f9:a2:4d:d8:8e:
76:d1:ba:52:be:3c:5e:73:e6:6d:23:0a:b8:28:fc:78:fe:9f:
c1:4c:d0:b6:cf:ee:17:6d:4b:85:11:a5:57:06:3e:ed:db:51:
1d:df:49:49:72:de:ea:db:33:97:e4:cb:f1:af:64:76:28:9a:
5b:62:b5:43:97:dc:f9:b3:75:c5:7c:ab:95:60:1a:d5:d7:7f:
b8:cc:78:69:9e:71:e8:c6:d5:91:41:00:4d:10:77:0e:56:6f:
8f:87:45:ea:97:ea:4b:59:1d:4d:c7:10:01:cb:a6:f5:e3:85:
6b:5a:4d:ac:d3:30:12:6e:4e:2e:19:09:3e:7d:62:c2:53:df:
a9:9d:8e:c3:d8:aa:69:b9:1d:d0:34:d2:8a:27:49:7d:ff:e8:
5f:62:00:84:1e:11:c1:5d:ff:4b:08:31:03:fd:a5:f3:d3:f3:


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_3
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:1
X509v3 Authority Key Identifier:
keyid:ED:E7:6F:76:5A:BF:60:EC:49:5B:C6:A5:77:BB:72:16:71:9B:C4:3D
Authority Information Access:
CA Issuers - URI:http://trust.quovadisglobal.com/qvrca2g3.crt
OCSP - URI:http://ocsp.quovadisglobal.com
X509v3 Certificate Policies:
Policy: X509v3 Any Policy
CPS: https://www.quovadisglobal.com/repository
X509v3 Extended Key Usage:
TLS Web Client Authentication, TLS Web Server Authentication
X509v3 CRL Distribution Points:
Full Name:
URI:http://crl.quovadisglobal.com/qvrca2g3.crl
X509v3 Subject Key Identifier:
B3:12:89:B5:A9:4B:35:BC:15:00:F0:80:E9:D8:78:87:F1:13:7C:76
X509v3 Key Usage: critical
Certificate Sign, CRL Sign
Signature Algorithm: sha256WithRSAEncryption
35:e8:30:d1:c6:54:6e:34:a8:46:8a:81:75:f4:61:90:e6:05:
9c:d5:03:ea:0d:3a:34:b4:ac:b2:d6:1f:b0:09:4c:15:9b:10:
af:a6:fd:9c:0e:42:63:56:c1:19:58:5d:c1:8e:74:0f:ba:67:
57:a9:e9:30:6f:01:61:c2:11:6b:be:26:c8:1f:6f:15:7c:9f:
24:14:35:33:eb:3c:d0:46:68:be:4e:86:d6:ea:21:18:46:9f:
b4:08:54:20:1c:70:bd:1a:61:9a:f1:e1:df:43:14:0e:57:06:
f0:bf:25:6a:1c:12:ff:03:db:4d:aa:60:9d:00:35:98:10:9b:
bf:f3:eb:55:9b:0e:07:5f:14:dc:59:e5:c9:4d:0f:b5:4c:eb:
6b:3c:bf:91:b7:40:4d:41:8b:13:82:7a:a6:67:8d:e9:b6:a0:
bf:55:9e:77:b1:b3:5b:12:dc:9e:58:0a:23:12:cc:97:77:ac:
44:89:f6:40:eb:5c:91:b2:67:27:22:c2:0e:76:72:ac:02:5a:
91:4d:c5:da:4a:f3:44:a9:2e:a7:9c:ca:18:95:b3:75:f8:aa:
b2:5d:0c:01:32:20:56:1a:97:27:7e:8a:09:b1:1a:84:56:92:
5a:ae:f0:61:6e:89:b2:9f:f5:e8:7d:ec:42:05:b2:4c:64:ce:
0c:76:6a:7a:8c:b3:91:74:23:57:02:c4:94:f9:a2:4d:d8:8e:
76:d1:ba:52:be:3c:5e:73:e6:6d:23:0a:b8:28:fc:78:fe:9f:
c1:4c:d0:b6:cf:ee:17:6d:4b:85:11:a5:57:06:3e:ed:db:51:
1d:df:49:49:72:de:ea:db:33:97:e4:cb:f1:af:64:76:28:9a:
5b:62:b5:43:97:dc:f9:b3:75:c5:7c:ab:95:60:1a:d5:d7:7f:
b8:cc:78:69:9e:71:e8:c6:d5:91:41:00:4d:10:77:0e:56:6f:
8f:87:45:ea:97:ea:4b:59:1d:4d:c7:10:01:cb:a6:f5:e3:85:
6b:5a:4d:ac:d3:30:12:6e:4e:2e:19:09:3e:7d:62:c2:53:df:
a9:9d:8e:c3:d8:aa:69:b9:1d:d0:34:d2:8a:27:49:7d:ff:e8:
5f:62:00:84:1e:11:c1:5d:ff:4b:08:31:03:fd:a5:f3:d3:f3:
d7:d8:8c:20:33:3d:3a:a7:86:45:01:85:c3:13:6c:cd:d5:f4:
47:11:82:b7:43:4e:62:05:27:31:8a:6e:90:52:ae:63:4c:c0:
b6:f5:c6:70:b2:89:19:f0:8f:a1:a8:ad:a9:bb:23:43:68:c2:
68:33:2d:3f:07:7e:76:27:a2:36:4d:89:ca:5b:e0:d5:f6:6c:
23:9d:20:29:55:cd:3a:c5
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_3$

3. Extracting the signatures from the server's certificate server_cert.pem. To do so, we can again print out all fields of the certificate and copy the signature value into a new file. Issue the following command

   ```
   $ openssl x509 -in server_cert.pem -text -noout
   ```

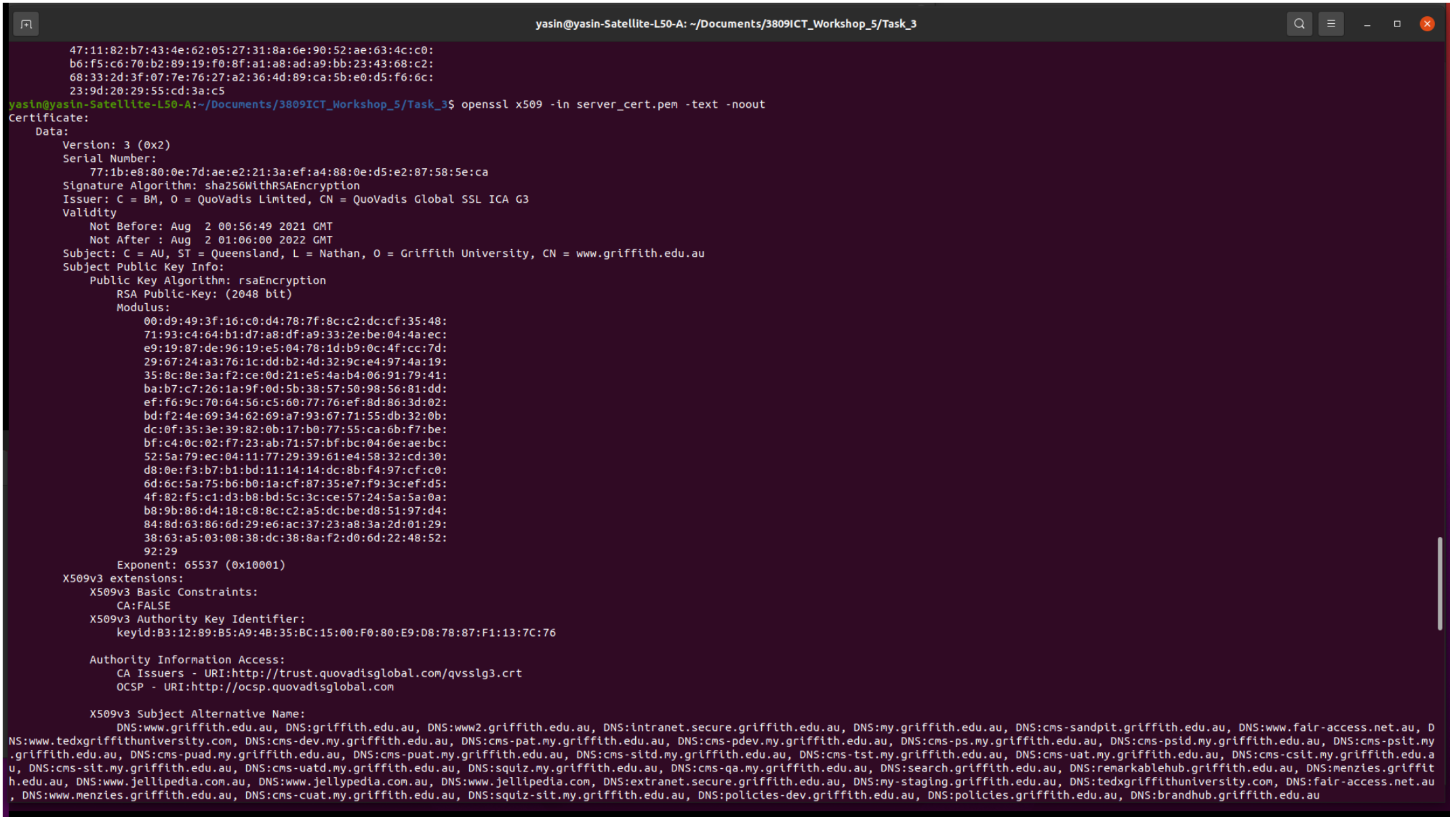
   Scroll down to the field "Signature Algorithm: sha256WithRSAEncryption", copy and paste the content (excluding "Signature Algorithm……") into a new file named signature. Then, we use the following command to delete the ":" and spaces from the content of the file signature.

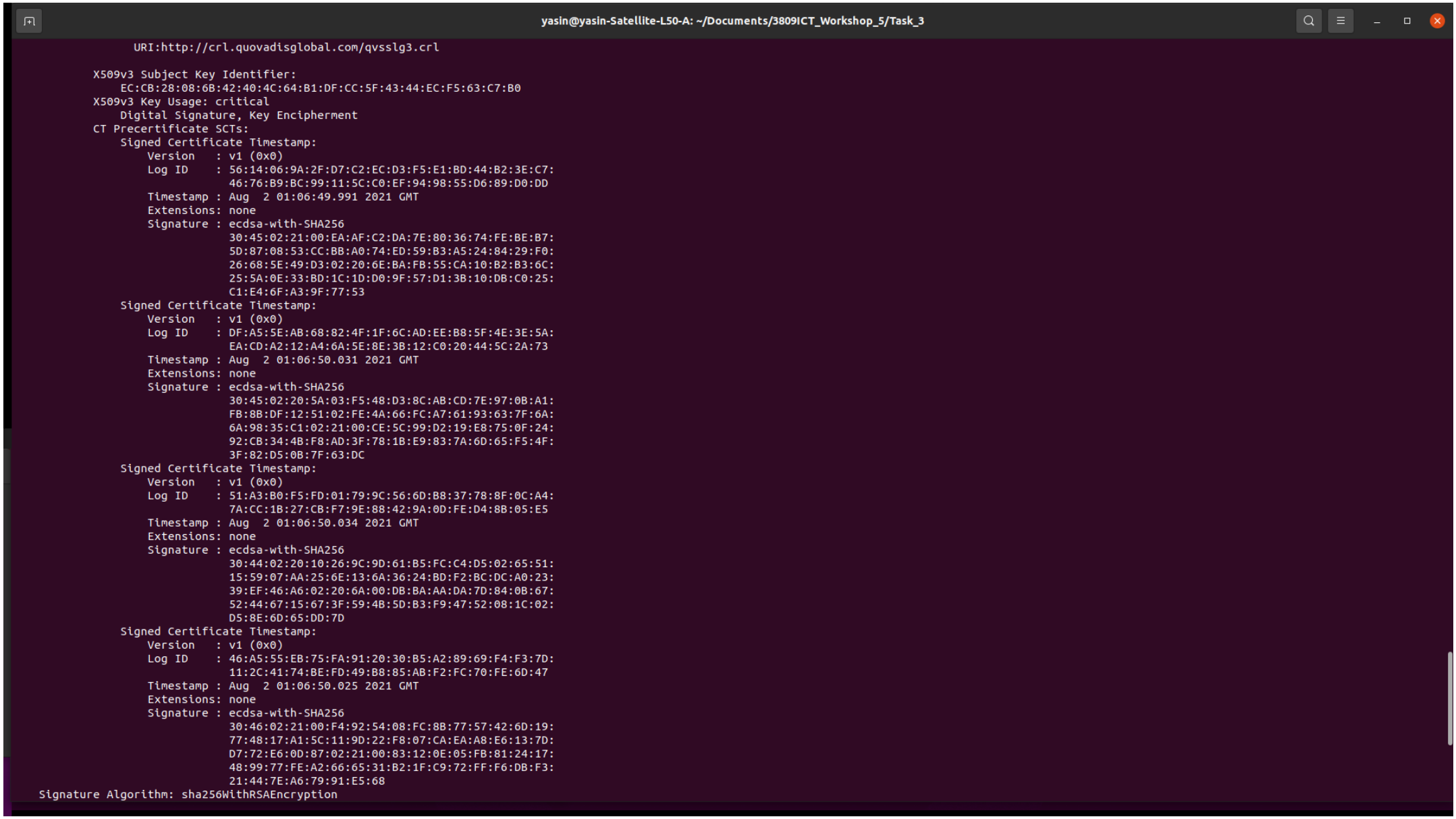
   ```
   $ cat signature | tr -d '[:space:]:'
   ```

   Copy and paste the content into a new file named sig_server_cert.

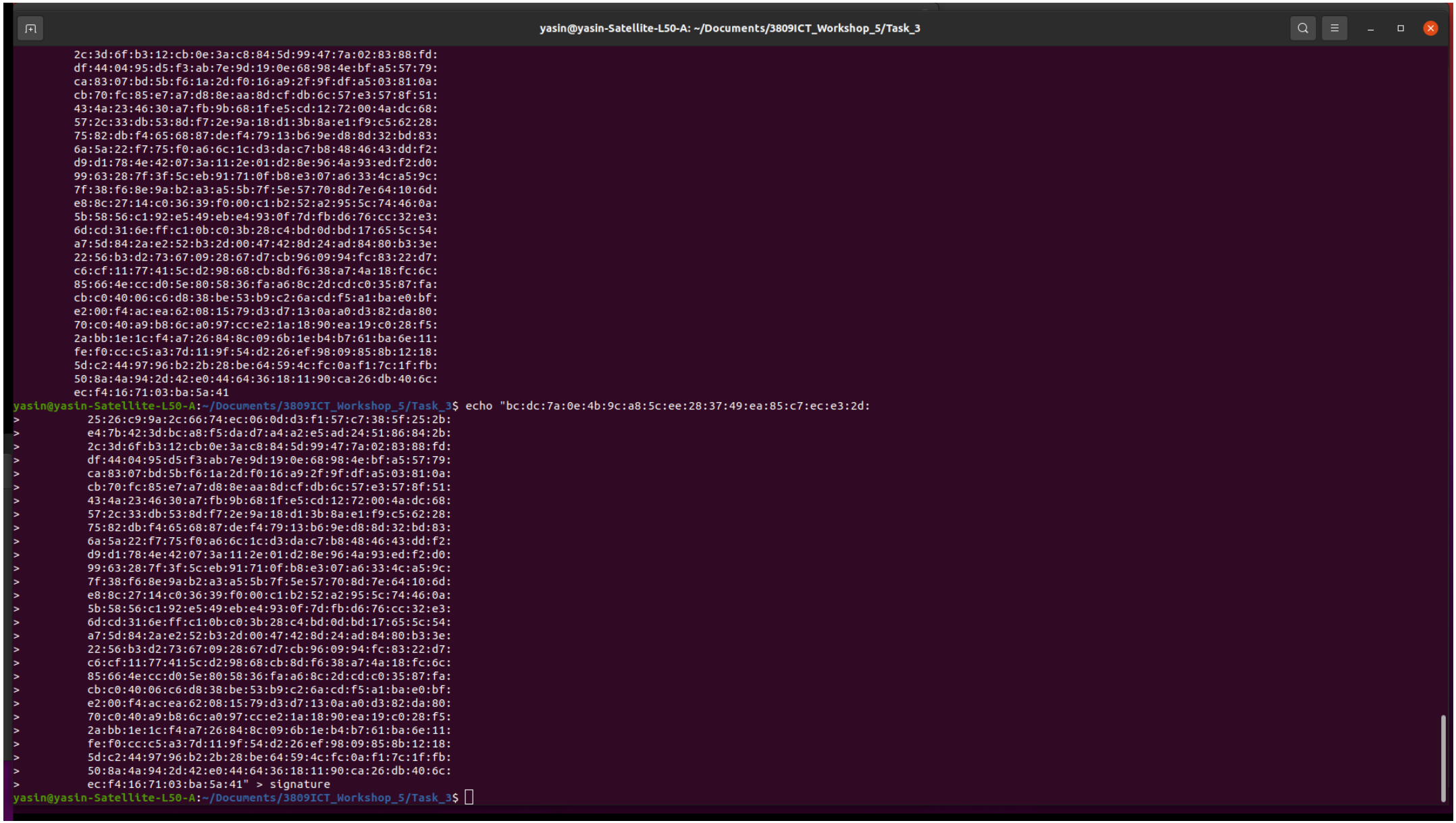
   Answer:

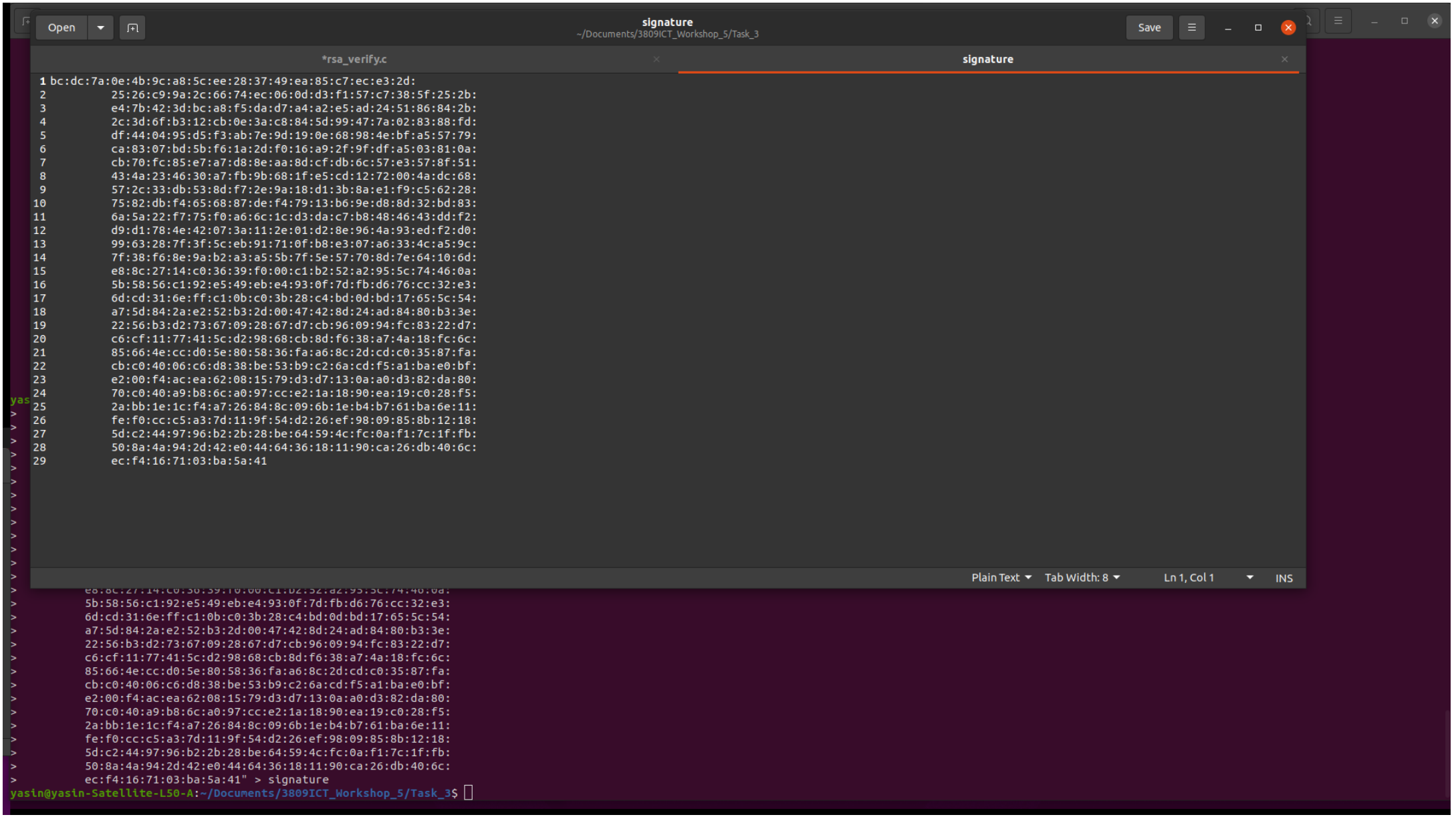
   In this step the signature is obtained σ

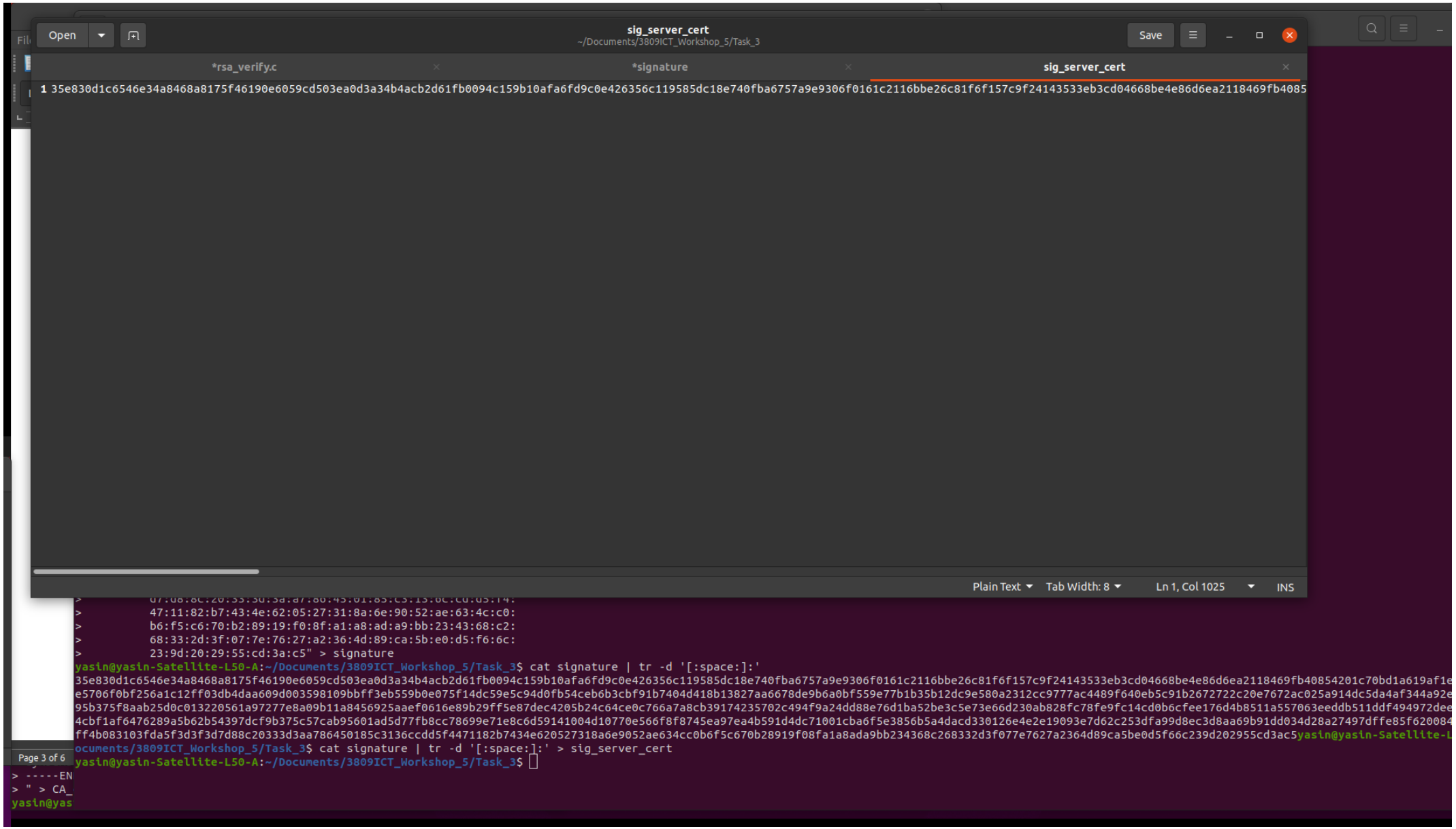

yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_3
47:11:82:b7:43:4e:62:05:27:31:8a:6e:90:52:ae:63:4c:c0:
b6:f5:c6:70:b2:89:19:f0:8f:a1:a8:ad:a9:bb:23:43:68:c2:
68:33:2d:3f:07:7e:76:27:a2:36:4d:89:ca:5b:e0:d5:f6:6c:
23:9d:20:29:55:cd:3a:c5
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_3$ openssl x509 -in server_cert.pem -text -noout
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
77:1b:e8:80:0e:7d:ae:e2:21:3a:ef:a4:88:0e:d5:e2:87:58:5e:ca
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = BM, O = QuoVadis Limited, CN = QuoVadis Global SSL ICA G3
Validity
Not Before: Aug 2 00:56:49 2021 GMT
Not After : Aug 2 01:06:00 2022 GMT
Subject: C = AU, ST = Queensland, L = Nathan, O = Griffith University, CN = www.griffith.edu.au
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
00:d9:49:3f:16:c0:d4:78:7f:8c:c2:dc:cf:35:48:
71:93:c4:64:b1:d7:a8:df:a9:33:2e:be:04:4a:ec:
e9:19:87:de:96:19:e5:04:78:1d:b9:0c:4f:cc:7d:
29:67:24:a3:76:1c:dd:b2:4d:32:9c:e4:97:4a:19:
35:8c:8e:3a:f2:ce:0d:21:e5:4a:b4:06:91:79:41:
ba:b7:c7:26:1a:9f:0d:5b:38:57:50:98:56:81:dd:
ef:f6:9c:70:64:56:c5:60:77:76:ef:8d:86:3d:02:
bd:f2:4e:69:34:62:69:a7:93:67:71:55:db:32:0b:
dc:0f:35:3e:39:82:0b:17:b0:77:55:ca:6b:f7:be:
bf:c4:0c:02:f7:23:ab:71:57:bf:bc:04:6e:ae:bc:
52:5a:79:ec:04:11:77:29:39:61:e4:58:32:cd:30:
d8:0e:f3:b7:b1:bd:11:14:14:dc:8b:f4:97:cf:c0:
6d:6c:5a:75:b6:b0:1a:cf:87:35:e7:f9:3c:ef:d5:
4f:82:f5:c1:d3:b8:bd:5c:3c:ce:57:24:5a:5a:0a:
b8:9b:86:d4:18:c8:8c:c2:a5:dc:be:d8:51:97:d4:
84:8d:63:86:6d:29:e6:ac:37:23:a8:3a:2d:01:29:
38:63:a5:03:08:38:dc:38:8a:f2:d0:6d:22:48:52:
92:29
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
X509v3 Authority Key Identifier:
keyid:B3:12:89:B5:A9:4B:35:BC:15:00:F0:80:E9:D8:78:87:F1:13:7C:76
Authority Information Access:
CA Issuers - URI:http://trust.quovadisglobal.com/qvsslg3.crt
OCSP - URI:http://ocsp.quovadisglobal.com
X509v3 Subject Alternative Name:
DNS:www.griffith.edu.au, DNS:griffith.edu.au, DNS:www2.griffith.edu.au, DNS:intranet.secure.griffith.edu.au, DNS:my.griffith.edu.au, DNS:cms-sandpit.griffith.edu.au, DNS:www.fair-access.net.au, DNS:www.tedxgriffithuniversity.com, DNS:cms-dev.my.griffith.edu.au, DNS:cms-pat.my.griffith.edu.au, DNS:cms-pdev.my.griffith.edu.au, DNS:cms-ps.my.griffith.edu.au, DNS:cms-psid.my.griffith.edu.au, DNS:cms-psit.my.griffith.edu.au, DNS:cms-puad.my.griffith.edu.au, DNS:cms-puat.my.griffith.edu.au, DNS:cms-sitd.my.griffith.edu.au, DNS:cms-tst.my.griffith.edu.au, DNS:cms-uat.my.griffith.edu.au, DNS:cms-csit.my.griffith.edu.au, DNS:cms-sit.my.griffith.edu.au, DNS:cms-uatd.my.griffith.edu.au, DNS:squiz.my.griffith.edu.au, DNS:cms-qa.my.griffith.edu.au, DNS:search.griffith.edu.au, DNS:remarkablehub.griffith.edu.au, DNS:menzies.griffith.edu.au, DNS:www.jellipedia.com.au, DNS:www.jellypedia.com.au, DNS:www.jellipedia.com, DNS:extranet.secure.griffith.edu.au, DNS:my-staging.griffith.edu.au, DNS:tedxgriffithuniversity.com, DNS:fair-access.net.au, DNS:www.menzies.griffith.edu.au, DNS:cms-cuat.my.griffith.edu.au, DNS:squiz-sit.my.griffith.edu.au, DNS:policies-dev.griffith.edu.au, DNS:policies.griffith.edu.au, DNS:brandhub.griffith.edu.au

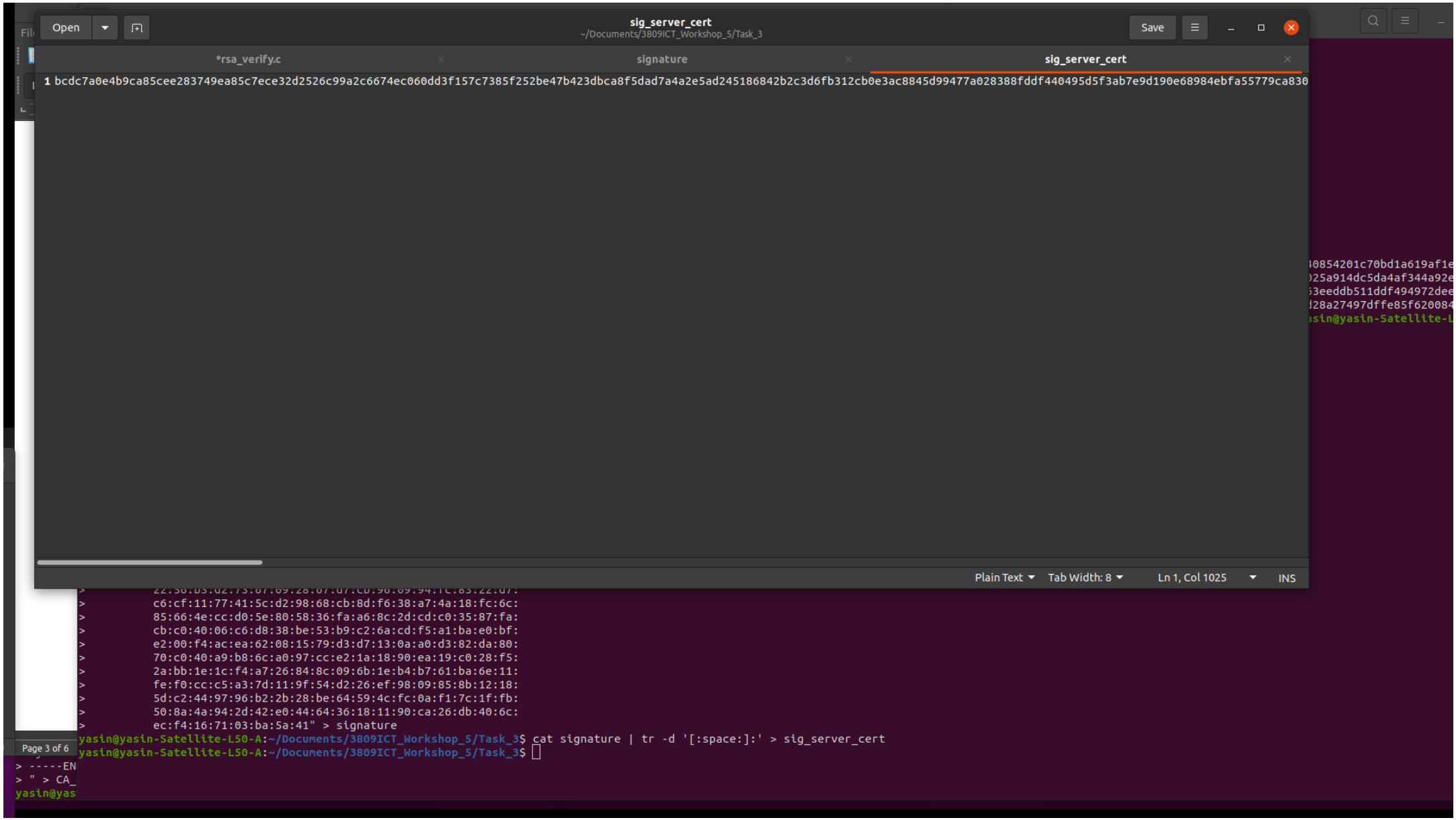

yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_3
URI:http://crl.quovadisglobal.com/qvsslg3.crl
X509v3 Subject Key Identifier:
EC:CB:28:08:6B:42:40:4C:64:B1:DF:CC:5F:43:44:EC:F5:63:C7:B0
X509v3 Key Usage: critical
Digital Signature, Key Encipherment
CT Precertificate SCTs:
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : 56:14:06:9A:2F:D7:C2:EC:D3:F5:E1:BD:44:B2:3E:C7:
46:76:B9:BC:99:11:5C:C0:EF:94:98:55:D6:89:D0:DD
Timestamp : Aug 2 01:06:49.991 2021 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:45:02:21:00:EA:AF:C2:DA:7E:80:36:74:FE:BE:B7:
5D:87:08:53:CC:BB:A0:74:ED:59:B3:A5:24:84:29:F0:
26:68:5E:49:D3:02:20:6E:BA:FB:55:CA:10:B2:B3:6C:
25:5A:0E:33:BD:1C:1D:D0:9F:57:D1:3B:10:DB:C0:25:
C1:E4:6F:A3:9F:77:53
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : DF:A5:5E:AB:68:82:4F:1F:6C:AD:EE:B8:5F:4E:3E:5A:
EA:CD:A2:12:A4:6A:5E:8E:3B:12:C0:20:44:5C:2A:73
Timestamp : Aug 2 01:06:50.031 2021 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:45:02:20:5A:03:F5:48:D3:8C:AB:CD:7E:97:0B:A1:
FB:8B:DF:12:51:02:FE:4A:66:FC:A7:61:93:63:7F:6A:
6A:98:35:C1:02:21:00:CE:5C:99:D2:19:E8:75:0F:24:
92:CB:34:4B:F8:AD:3F:78:1B:E9:83:7A:6D:65:F5:4F:
3F:82:D5:0B:7F:63:DC
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : 51:A3:B0:F5:FD:01:79:9C:56:6D:B8:37:78:8F:0C:A4:
7A:CC:1B:27:CB:F7:9E:88:42:9A:0D:FE:D4:8B:05:E5
Timestamp : Aug 2 01:06:50.034 2021 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:44:02:20:10:26:9C:9D:61:B5:FC:C4:D5:02:65:51:
15:59:07:AA:25:6E:13:6A:36:24:BD:F2:BC:DC:A0:23:
39:EF:46:A6:02:20:6A:00:DB:BA:AA:DA:7D:84:0B:67:
52:44:67:15:67:3F:59:4B:5D:B3:F9:47:52:08:1C:02:
D5:8E:6D:65:DD:7D
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:
11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47
Timestamp : Aug 2 01:06:50.025 2021 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:46:02:21:00:F4:92:54:08:FC:8B:77:57:42:6D:19:
77:48:17:A1:5C:11:9D:22:F8:07:CA:EA:A8:E6:13:7D:
D7:72:E6:0D:87:02:21:00:83:12:0E:05:FB:81:24:17:
48:99:77:FE:A2:66:65:31:B2:1F:C9:72:FF:F6:DB:F3:
21:44:7E:A6:79:91:E5:68
Signature Algorithm: sha256WithRSAEncryption

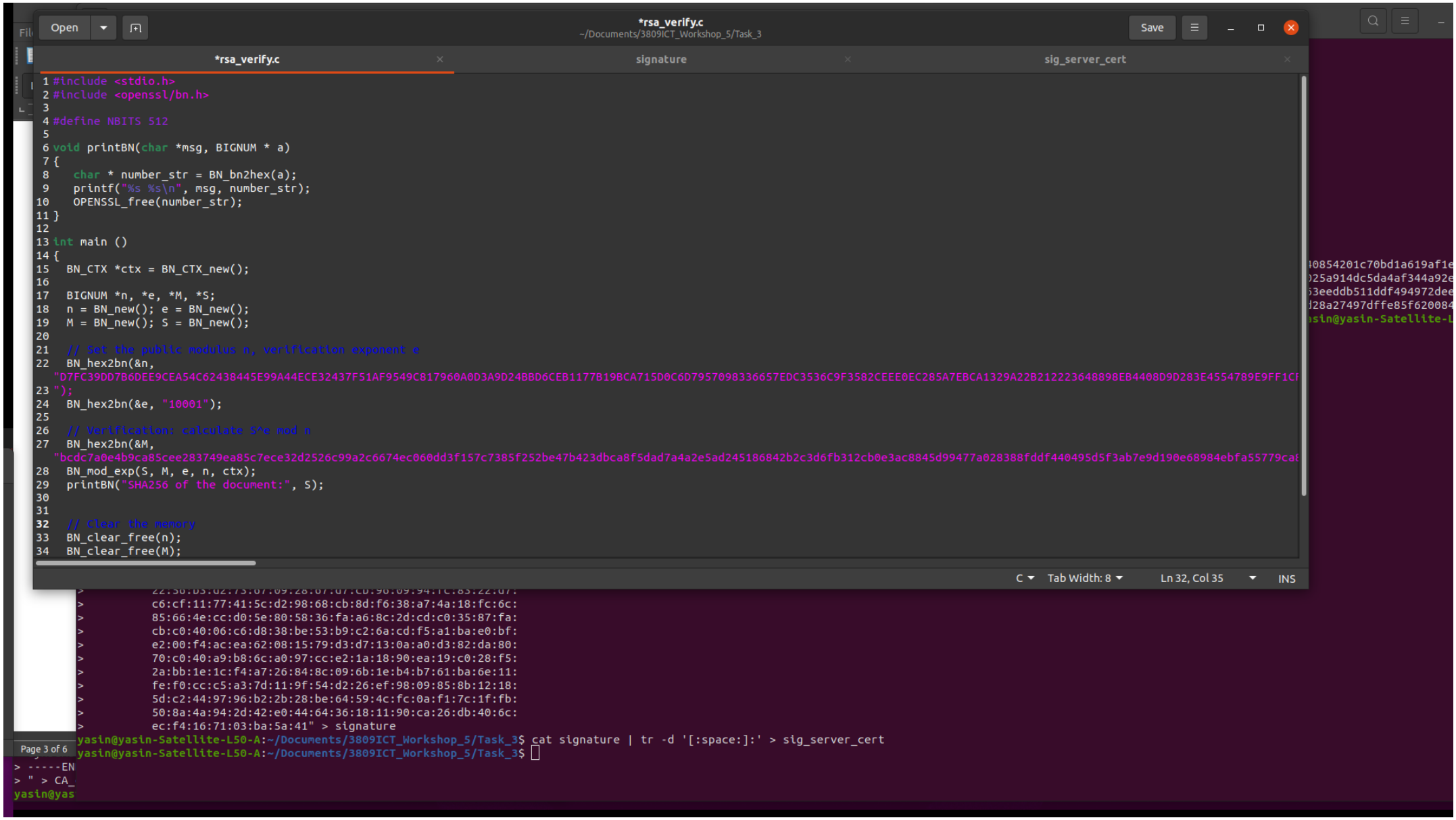
```
                    3F:82:D5:0B:7F:63:DC
            Signed Certificate Timestamp:
                Version   : v1 (0x0)
                Log ID    : 51:A3:B0:F5:FD:01:79:9C:56:6D:B8:37:78:8F:0C:A4:
                            7A:CC:1B:27:CB:F7:9E:88:42:9A:0D:FE:D4:8B:05:E5
                Timestamp : Aug  2 01:06:50.034 2021 GMT
                Extensions: none
                Signature : ecdsa-with-SHA256
                            30:44:02:20:10:26:9C:9D:61:B5:FC:C4:D5:02:65:51:
                            15:59:07:AA:25:6E:13:6A:36:24:BD:F2:BC:DC:A0:23:
                            39:EF:46:A6:02:20:6A:00:DB:BA:AA:DA:7D:84:0B:67:
                            52:44:67:15:67:3F:59:4B:5D:B3:F9:47:52:08:1C:02:
                            D5:8E:6D:65:DD:7D
            Signed Certificate Timestamp:
                Version   : v1 (0x0)
                Log ID    : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:
                            11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47
                Timestamp : Aug  2 01:06:50.025 2021 GMT
                Extensions: none
                Signature : ecdsa-with-SHA256
                            30:46:02:21:00:F4:92:54:08:FC:8B:77:57:42:6D:19:
                            77:48:17:A1:5C:11:9D:22:F8:07:CA:EA:A8:E6:13:7D:
                            D7:72:E6:0D:87:02:21:00:83:12:0E:05:FB:81:24:17:
                            48:99:77:FE:A2:66:65:31:B2:1F:C9:72:FF:F6:DB:F3:
                            21:44:7E:A6:79:91:E5:68
    Signature Algorithm: sha256WithRSAEncryption
         bc:dc:7a:0e:4b:9c:a8:5c:ee:28:37:49:ea:85:c7:ec:e3:2d:
         25:26:c9:9a:2c:66:74:ec:06:0d:d3:f1:57:c7:38:5f:25:2b:
         e4:7b:42:3d:bc:a8:f5:da:d7:a4:a2:e5:ad:24:51:86:84:2b:
         2c:3d:6f:b3:12:cb:0e:3a:c8:84:5d:99:47:7a:02:83:88:fd:
         df:44:04:95:d5:f3:ab:7e:9d:19:0e:68:98:4e:bf:a5:57:79:
         ca:83:07:bd:5b:f6:1a:2d:f0:16:a9:2f:9f:df:a5:03:81:0a:
         cb:70:fc:85:e7:a7:d8:8e:aa:8d:cf:db:6c:57:e3:57:8f:51:
         43:4a:23:46:30:a7:fb:9b:68:1f:e5:cd:12:72:00:4a:dc:68:
         57:2c:33:db:53:8d:f7:2e:9a:18:d1:3b:8a:e1:f9:c5:62:28:
         75:82:db:f4:65:68:87:de:f4:79:13:b6:9e:d8:8d:32:bd:83:
         6a:5a:22:f7:75:f0:a6:6c:1c:d3:da:c7:b8:48:46:43:dd:f2:
         d9:d1:78:4e:42:07:3a:11:2e:01:d2:8e:96:4a:93:ed:f2:d0:
         99:63:28:7f:3f:5c:eb:91:71:0f:b8:e3:07:a6:33:4c:a5:9c:
         7f:38:f6:8e:9a:b2:a3:a5:5b:7f:5e:57:70:8d:7e:64:10:6d:
         e8:8c:27:14:c0:36:39:f0:00:c1:b2:52:a2:95:5c:74:46:0a:
         5b:58:56:c1:92:e5:49:eb:e4:93:0f:7d:fb:d6:76:cc:32:e3:
         6d:cd:31:6e:ff:c1:0b:c0:3b:28:c4:bd:0d:bd:17:65:5c:54:
         a7:5d:84:2a:e2:52:b3:2d:00:47:42:8d:24:ad:84:80:b3:3e:
         22:56:b3:d2:73:67:09:28:67:d7:cb:96:09:94:fc:83:22:d7:
         c6:cf:11:77:41:5c:d2:98:68:cb:8d:f6:38:a7:4a:18:fc:6c:
         85:66:4e:cc:d0:5e:80:58:36:fa:a6:8c:2d:cd:c0:35:87:fa:
         cb:c0:40:06:c6:d8:38:be:53:b9:c2:6a:cd:f5:a1:ba:e0:bf:
         e2:00:f4:ac:ea:62:08:15:79:d3:d7:13:0a:a0:d3:82:da:80:
         70:c0:40:a9:b8:6c:a0:97:cc:e2:1a:18:90:ea:19:c0:28:f5:
         2a:bb:1e:1c:f4:a7:26:84:8c:09:6b:1e:b4:b7:61:ba:6e:11:
         fe:f0:cc:c5:a3:7d:11:9f:54:d2:26:ef:98:09:85:8b:12:18:
         5d:c2:44:97:96:b2:2b:28:be:64:59:4c:fc:0a:f1:7c:1f:fb:
         50:8a:4a:94:2d:42:e0:44:64:36:18:11:90:ca:26:db:40:6c:
         ec:f4:16:71:03:ba:5a:41
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_3$
```


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_3
2c:3d:6f:b3:12:cb:0e:3a:c8:84:5d:99:47:7a:02:83:88:fd:
df:44:04:95:d5:f3:ab:7e:9d:19:0e:68:98:4e:bf:a5:57:79:
ca:83:07:bd:5b:f6:1a:2d:f0:16:a9:2f:9f:df:a5:03:81:0a:
cb:70:fc:85:e7:a7:d8:8e:aa:8d:cf:db:6c:57:e3:57:8f:51:
43:4a:23:46:30:a7:fb:9b:68:1f:e5:cd:12:72:00:4a:dc:68:
57:2c:33:db:53:8d:f7:2e:9a:18:d1:3b:8a:e1:f9:c5:62:28:
75:82:db:f4:65:68:87:de:f4:79:13:b6:9e:d8:8d:32:bd:83:
6a:5a:22:f7:75:f0:a6:6c:1c:d3:da:c7:b8:48:46:43:dd:f2:
d9:d1:78:4e:42:07:3a:11:2e:01:d2:8e:96:4a:93:ed:f2:d0:
99:63:28:7f:3f:5c:eb:91:71:0f:b8:e3:07:a6:33:4c:a5:9c:
7f:38:f6:8e:9a:b2:a3:a5:5b:7f:5e:57:70:8d:7e:64:10:6d:
e8:8c:27:14:c0:36:39:f0:00:c1:b2:52:a2:95:5c:74:46:0a:
5b:58:56:c1:92:e5:49:eb:e4:93:0f:7d:fb:d6:76:cc:32:e3:
6d:cd:31:6e:ff:c1:0b:c0:3b:28:c4:bd:0d:bd:17:65:5c:54:
a7:5d:84:2a:e2:52:b3:2d:00:47:42:8d:24:ad:84:80:b3:3e:
22:56:b3:d2:73:67:09:28:67:d7:cb:96:09:94:fc:83:22:d7:
c6:cf:11:77:41:5c:d2:98:68:cb:8d:f6:38:a7:4a:18:fc:6c:
85:66:4e:cc:d0:5e:80:58:36:fa:a6:8c:2d:cd:c0:35:87:fa:
cb:c0:40:06:c6:d8:38:be:53:b9:c2:6a:cd:f5:a1:ba:e0:bf:
e2:00:f4:ac:ea:62:08:15:79:d3:d7:13:0a:a0:d3:82:da:80:
70:c0:40:a9:b8:6c:a0:97:cc:e2:1a:18:90:ea:19:c0:28:f5:
2a:bb:1e:1c:f4:a7:26:84:8c:09:6b:1e:b4:b7:61:ba:6e:11:
fe:f0:cc:c5:a3:7d:11:9f:54:d2:26:ef:98:09:85:8b:12:18:
5d:c2:44:97:96:b2:2b:28:be:64:59:4c:fc:0a:f1:7c:1f:fb:
50:8a:4a:94:2d:42:e0:44:64:36:18:11:90:ca:26:db:40:6c:
ec:f4:16:71:03:ba:5a:41
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_3$ echo "bc:dc:7a:0e:4b:9c:a8:5c:ee:28:37:49:ea:85:c7:ec:e3:2d:
> 25:26:c9:9a:2c:66:74:ec:06:0d:d3:f1:57:c7:38:5f:25:2b:
> e4:7b:42:3d:bc:a8:f5:da:d7:a4:a2:e5:ad:24:51:86:84:2b:
> 2c:3d:6f:b3:12:cb:0e:3a:c8:84:5d:99:47:7a:02:83:88:fd:
> df:44:04:95:d5:f3:ab:7e:9d:19:0e:68:98:4e:bf:a5:57:79:
> ca:83:07:bd:5b:f6:1a:2d:f0:16:a9:2f:9f:df:a5:03:81:0a:
> cb:70:fc:85:e7:a7:d8:8e:aa:8d:cf:db:6c:57:e3:57:8f:51:
> 43:4a:23:46:30:a7:fb:9b:68:1f:e5:cd:12:72:00:4a:dc:68:
> 57:2c:33:db:53:8d:f7:2e:9a:18:d1:3b:8a:e1:f9:c5:62:28:
> 75:82:db:f4:65:68:87:de:f4:79:13:b6:9e:d8:8d:32:bd:83:
> 6a:5a:22:f7:75:f0:a6:6c:1c:d3:da:c7:b8:48:46:43:dd:f2:
> d9:d1:78:4e:42:07:3a:11:2e:01:d2:8e:96:4a:93:ed:f2:d0:
> 99:63:28:7f:3f:5c:eb:91:71:0f:b8:e3:07:a6:33:4c:a5:9c:
> 7f:38:f6:8e:9a:b2:a3:a5:5b:7f:5e:57:70:8d:7e:64:10:6d:
> e8:8c:27:14:c0:36:39:f0:00:c1:b2:52:a2:95:5c:74:46:0a:
> 5b:58:56:c1:92:e5:49:eb:e4:93:0f:7d:fb:d6:76:cc:32:e3:
> 6d:cd:31:6e:ff:c1:0b:c0:3b:28:c4:bd:0d:bd:17:65:5c:54:
> a7:5d:84:2a:e2:52:b3:2d:00:47:42:8d:24:ad:84:80:b3:3e:
> 22:56:b3:d2:73:67:09:28:67:d7:cb:96:09:94:fc:83:22:d7:
> c6:cf:11:77:41:5c:d2:98:68:cb:8d:f6:38:a7:4a:18:fc:6c:
> 85:66:4e:cc:d0:5e:80:58:36:fa:a6:8c:2d:cd:c0:35:87:fa:
> cb:c0:40:06:c6:d8:38:be:53:b9:c2:6a:cd:f5:a1:ba:e0:bf:
> e2:00:f4:ac:ea:62:08:15:79:d3:d7:13:0a:a0:d3:82:da:80:
> 70:c0:40:a9:b8:6c:a0:97:cc:e2:1a:18:90:ea:19:c0:28:f5:
> 2a:bb:1e:1c:f4:a7:26:84:8c:09:6b:1e:b4:b7:61:ba:6e:11:
> fe:f0:cc:c5:a3:7d:11:9f:54:d2:26:ef:98:09:85:8b:12:18:
> 5d:c2:44:97:96:b2:2b:28:be:64:59:4c:fc:0a:f1:7c:1f:fb:
> 50:8a:4a:94:2d:42:e0:44:64:36:18:11:90:ca:26:db:40:6c:
> ec:f4:16:71:03:ba:5a:41" > signature
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_3$


Open
signature
~/Documents/3809ICT_Workshop_5/Task_3
Save
*rsa_verify.c
signature
1 bc:dc:7a:0e:4b:9c:a8:5c:ee:28:37:49:ea:85:c7:ec:e3:2d:
2 25:26:c9:9a:2c:66:74:ec:06:0d:d3:f1:57:c7:38:5f:25:2b:
3 e4:7b:42:3d:bc:a8:f5:da:d7:a4:a2:e5:ad:24:51:86:84:2b:
4 2c:3d:6f:b3:12:cb:0e:3a:c8:84:5d:99:47:7a:02:83:88:fd:
5 df:44:04:95:d5:f3:ab:7e:9d:19:0e:68:98:4e:bf:a5:57:79:
6 ca:83:07:bd:5b:f6:1a:2d:f0:16:a9:2f:9f:df:a5:03:81:0a:
7 cb:70:fc:85:e7:a7:d8:8e:aa:8d:cf:db:6c:57:e3:57:8f:51:
8 43:4a:23:46:30:a7:fb:9b:68:1f:e5:cd:12:72:00:4a:dc:68:
9 57:2c:33:db:53:8d:f7:2e:9a:18:d1:3b:8a:e1:f9:c5:62:28:
10 75:82:db:f4:65:68:87:de:f4:79:13:b6:9e:d8:8d:32:bd:83:
11 6a:5a:22:f7:75:f0:a6:6c:1c:d3:da:c7:b8:48:46:43:dd:f2:
12 d9:d1:78:4e:42:07:3a:11:2e:01:d2:8e:96:4a:93:ed:f2:d0:
13 99:63:28:7f:3f:5c:eb:91:71:0f:b8:e3:07:a6:33:4c:a5:9c:
14 7f:38:f6:8e:9a:b2:a3:a5:5b:7f:5e:57:70:8d:7e:64:10:6d:
15 e8:8c:27:14:c0:36:39:f0:00:c1:b2:52:a2:95:5c:74:46:0a:
16 5b:58:56:c1:92:e5:49:eb:e4:93:0f:7d:fb:d6:76:cc:32:e3:
17 6d:cd:31:6e:ff:c1:0b:c0:3b:28:c4:bd:0d:bd:17:65:5c:54:
18 a7:5d:84:2a:e2:52:b3:2d:00:47:42:8d:24:ad:84:80:b3:3e:
19 22:56:b3:d2:73:67:09:28:67:d7:cb:96:09:94:fc:83:22:d7:
20 c6:cf:11:77:41:5c:d2:98:68:cb:8d:f6:38:a7:4a:18:fc:6c:
21 85:66:4e:cc:d0:5e:80:58:36:fa:a6:8c:2d:cd:c0:35:87:fa:
22 cb:c0:40:06:c6:d8:38:be:53:b9:c2:6a:cd:f5:a1:ba:e0:bf:
23 e2:00:f4:ac:ea:62:08:15:79:d3:d7:13:0a:a0:d3:82:da:80:
24 70:c0:40:a9:b8:6c:a0:97:cc:e2:1a:18:90:ea:19:c0:28:f5:
25 2a:bb:1e:1c:f4:a7:26:84:8c:09:6b:1e:b4:b7:61:ba:6e:11:
26 fe:f0:cc:c5:a3:7d:11:9f:54:d2:26:ef:98:09:85:8b:12:18:
27 5d:c2:44:97:96:b2:2b:28:be:64:59:4c:fc:0a:f1:7c:1f:fb:
28 50:8a:4a:94:2d:42:e0:44:64:36:18:11:90:ca:26:db:40:6c:
29 ec:f4:16:71:03:ba:5a:41
Plain Text
Tab Width: 8
Ln 1, Col 1
INS
5b:58:56:c1:92:e5:49:eb:e4:93:0f:7d:fb:d6:76:cc:32:e3:
6d:cd:31:6e:ff:c1:0b:c0:3b:28:c4:bd:0d:bd:17:65:5c:54:
a7:5d:84:2a:e2:52:b3:2d:00:47:42:8d:24:ad:84:80:b3:3e:
22:56:b3:d2:73:67:09:28:67:d7:cb:96:09:94:fc:83:22:d7:
c6:cf:11:77:41:5c:d2:98:68:cb:8d:f6:38:a7:4a:18:fc:6c:
85:66:4e:cc:d0:5e:80:58:36:fa:a6:8c:2d:cd:c0:35:87:fa:
cb:c0:40:06:c6:d8:38:be:53:b9:c2:6a:cd:f5:a1:ba:e0:bf:
e2:00:f4:ac:ea:62:08:15:79:d3:d7:13:0a:a0:d3:82:da:80:
70:c0:40:a9:b8:6c:a0:97:cc:e2:1a:18:90:ea:19:c0:28:f5:
2a:bb:1e:1c:f4:a7:26:84:8c:09:6b:1e:b4:b7:61:ba:6e:11:
fe:f0:cc:c5:a3:7d:11:9f:54:d2:26:ef:98:09:85:8b:12:18:
5d:c2:44:97:96:b2:2b:28:be:64:59:4c:fc:0a:f1:7c:1f:fb:
50:8a:4a:94:2d:42:e0:44:64:36:18:11:90:ca:26:db:40:6c:
ec:f4:16:71:03:ba:5a:41" > signature
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_3$


Open
sig_server_cert
~/Documents/3809ICT_Workshop_5/Task_3
Save
*rsa_verify.c
*signature
sig_server_cert
1 35e830d1c6546e34a8468a8175f46190e6059cd503ea0d3a34b4acb2d61fb0094c159b10afa6fd9c0e426356c119585dc18e740fba6757a9e9306f0161c2116bbe26c81f6f157c9f24143533eb3cd04668be4e86d6ea2118469fb4085
Plain Text
Tab Width: 8
Ln 1, Col 1025
INS
> 47:11:82:b7:43:4e:62:05:27:31:8a:6e:90:52:ae:63:4c:c0:
> b6:f5:c6:70:b2:89:19:f0:8f:a1:a8:ad:a9:bb:23:43:68:c2:
> 68:33:2d:3f:07:7e:76:27:a2:36:4d:89:ca:5b:e0:d5:f6:6c:
> 23:9d:20:29:55:cd:3a:c5" > signature
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_3$ cat signature | tr -d '[:space:]:'
35e830d1c6546e34a8468a8175f46190e6059cd503ea0d3a34b4acb2d61fb0094c159b10afa6fd9c0e426356c119585dc18e740fba6757a9e9306f0161c2116bbe26c81f6f157c9f24143533eb3cd04668be4e86d6ea2118469fb40854201c70bd1a619af1e
e5706f0bf256a1c12ff03db4daa609d003598109bbff3eb559b0e075f14dc59e5c94d0fb54ceb6b3cbf91b7404d418b13827aa6678de9b6a0bf559e77b1b35b12dc9e580a2312cc9777ac4489f640eb5c91b2672722c20e7672ac025a914dc5da4af344a92e
95b375f8aab25d0c013220561a97277e8a09b11a8456925aaef0616e89b29ff5e87dec4205b24c64ce0c766a7a8cb39174235702c494f9a24dd88e76d1ba52be3c5e73e66d230ab828fc78fe9fc14cd0b6cfee176d4b8511a557063eeddb511ddf494972dee
4cbf1af6476289a5b62b54397dcf9b375c57cab95601ad5d77fb8cc78699e71e8c6d59141004d10770e566f8f8745ea97ea4b591d4dc71001cba6f5e3856b5a4dacd330126e4e2e19093e7d62c253dfa99d8ec3d8aa69b91dd034d28a27497dffe85f620084
ff4b083103fda5f3d3f3d7d88c20333d3aa786450185c3136ccdd5f4471182b7434e620527318a6e9052ae634cc0b6f5c670b28919f08fa1a8ada9bb234368c268332d3f077e7627a2364d89ca5be0d5f66c239d202955cd3ac5yasin@yasin-Satellite-L
ocuments/3809ICT_Workshop_5/Task_3$ cat signature | tr -d '[:space:]:' > sig_server_cert
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_3$
Page 3 of 6
> -----EN
> " > CA_
yasin@yas


Open
sig_server_cert
~/Documents/3809ICT_Workshop_5/Task_3
Save
*rsa_verify.c
signature
sig_server_cert
1 bcdc7a0e4b9ca85cee283749ea85c7ece32d2526c99a2c6674ec060dd3f157c7385f252be47b423dbca8f5dad7a4a2e5ad245186842b2c3d6fb312cb0e3ac8845d99477a028388fddf440495d5f3ab7e9d190e68984ebfa55779ca830
Plain Text
Tab Width: 8
Ln 1, Col 1025
INS
c6:cf:11:77:41:5c:d2:98:68:cb:8d:f6:38:a7:4a:18:fc:6c:
85:66:4e:cc:d0:5e:80:58:36:fa:a6:8c:2d:cd:c0:35:87:fa:
cb:c0:40:06:c6:d8:38:be:53:b9:c2:6a:cd:f5:a1:ba:e0:bf:
e2:00:f4:ac:ea:62:08:15:79:d3:d7:13:0a:a0:d3:82:da:80:
70:c0:40:a9:b8:6c:a0:97:cc:e2:1a:18:90:ea:19:c0:28:f5:
2a:bb:1e:1c:f4:a7:26:84:8c:09:6b:1e:b4:b7:61:ba:6e:11:
fe:f0:cc:c5:a3:7d:11:9f:54:d2:26:ef:98:09:85:8b:12:18:
5d:c2:44:97:96:b2:2b:28:be:64:59:4c:fc:0a:f1:7c:1f:fb:
50:8a:4a:94:2d:42:e0:44:64:36:18:11:90:ca:26:db:40:6c:
ec:f4:16:71:03:ba:5a:41" > signature
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_3$ cat signature | tr -d '[:space:]:' > sig_server_cert
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_3$
Page 3 of 6


Open
*rsa_verify.c
~/Documents/3809ICT_Workshop_5/Task_3
Save
*rsa_verify.c
signature
sig_server_cert
#include <stdio.h>
#include <openssl/bn.h>
#define NBITS 512
void printBN(char *msg, BIGNUM * a)
{
char * number_str = BN_bn2hex(a);
printf("%s %s\n", msg, number_str);
OPENSSL_free(number_str);
}
int main ()
{
BN_CTX *ctx = BN_CTX_new();
BIGNUM *n, *e, *M, *S;
n = BN_new(); e = BN_new();
M = BN_new(); S = BN_new();
// Set the public modulus n, verification exponent e
BN_hex2bn(&n,
"D7FC39DD7B6DEE9CEA54C62438445E99A44ECE32437F51AF9549C817960A0D3A9D24BBD6CEB1177B19BCA715D0C6D7957098336657EDC3536C9F3582CEEE0EC285A7EBCA1329A22B212223648898EB4408D9D283E4554789E9FF1C
");
BN_hex2bn(&e, "10001");
// Verification: calculate S^e mod n
BN_hex2bn(&M,
"bcdc7a0e4b9ca85cee283749ea85c7ece32d2526c99a2c6674ec060dd3f157c7385f252be47b423dbca8f5dad7a4a2e5ad245186842b2c3d6fb312cb0e3ac8845d99477a028388fddf440495d5f3ab7e9d190e68984ebfa55779ca
BN_mod_exp(S, M, e, n, ctx);
printBN("SHA256 of the document:", S);
// Clear the memory
BN_clear_free(n);
BN_clear_free(M);
C
Tab Width: 8
Ln 32, Col 35
INS
c6:cf:11:77:41:5c:d2:98:68:cb:8d:f6:38:a7:4a:18:fc:6c:
85:66:4e:cc:d0:5e:80:58:36:fa:a6:8c:2d:cd:c0:35:87:fa:
cb:c0:40:06:c6:d8:38:be:53:b9:c2:6a:cd:f5:a1:ba:e0:bf:
e2:00:f4:ac:ea:62:08:15:79:d3:d7:13:0a:a0:d3:82:da:80:
70:c0:40:a9:b8:6c:a0:97:cc:e2:1a:18:90:ea:19:c0:28:f5:
2a:bb:1e:1c:f4:a7:26:84:8c:09:6b:1e:b4:b7:61:ba:6e:11:
fe:f0:cc:c5:a3:7d:11:9f:54:d2:26:ef:98:09:85:8b:12:18:
5d:c2:44:97:96:b2:2b:28:be:64:59:4c:fc:0a:f1:7c:1f:fb:
50:8a:4a:94:2d:42:e0:44:64:36:18:11:90:ca:26:db:40:6c:
ec:f4:16:71:03:ba:5a:41" > signature
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_3$ cat signature | tr -d '[:space:]:' > sig_server_cert
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_3$
Page 3 of 6
> -----EN
> " > CA_
yasin@yas

4. Extracting the body of the server's certificate. The signature (signed by the CA using CA's private key) is based on the SHA256 hash of part of the content from the server's certificate (i.e., the file server_cert.pem). Let's display the content of the server_cert.pem by issuing the following command:

```
$ openssl asn1parse -i -in server_cert.pem
```

From the content displayed, the part between the following two lines is used by the CA to calculate a digital signature:

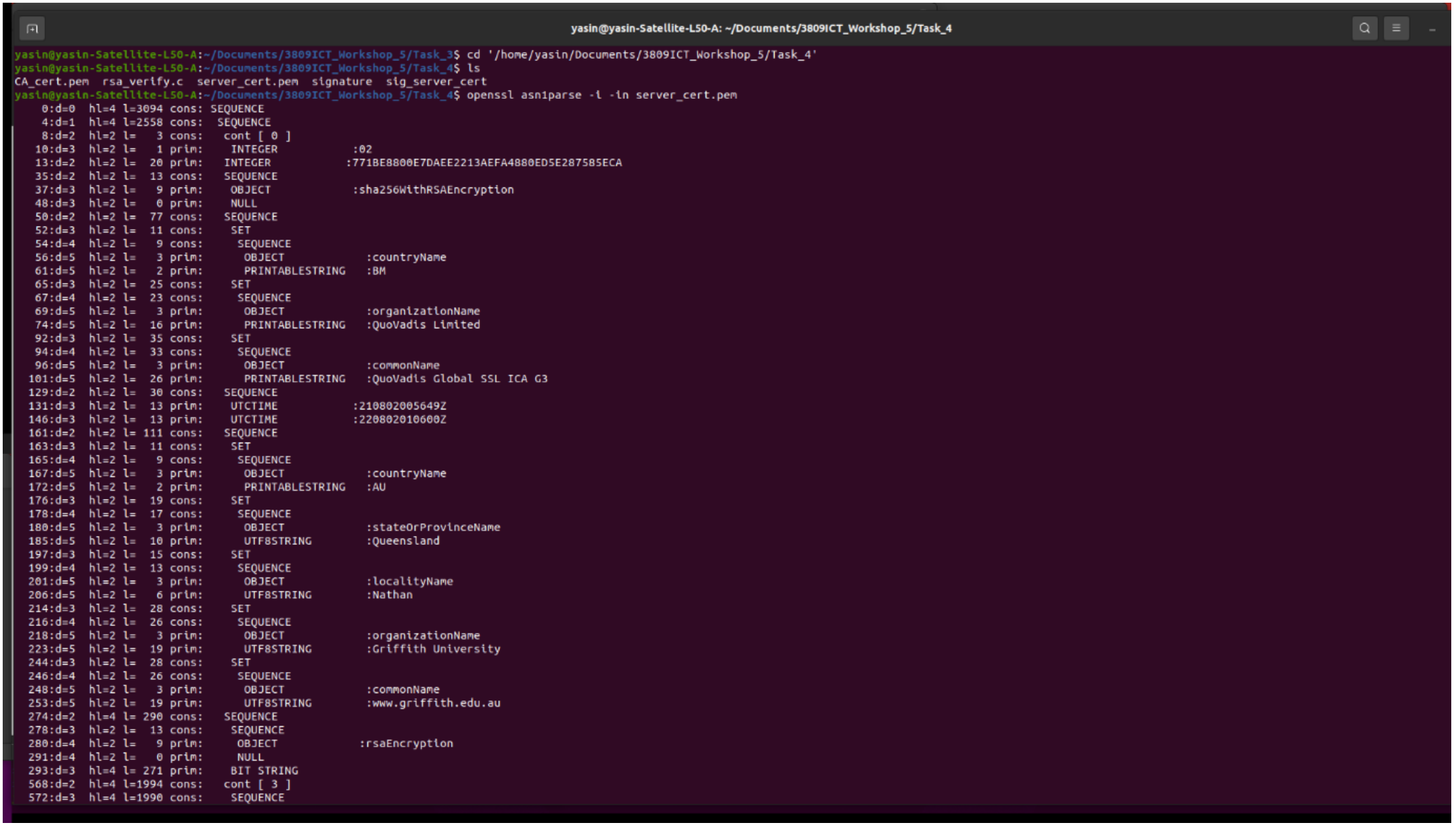
```
   4:d=1  hl=4 l=2558 cons:  SEQUENCE
2568:d=2  hl=2 l=   9 prim:   OBJECT            :sha256WithRSAEncryption
```

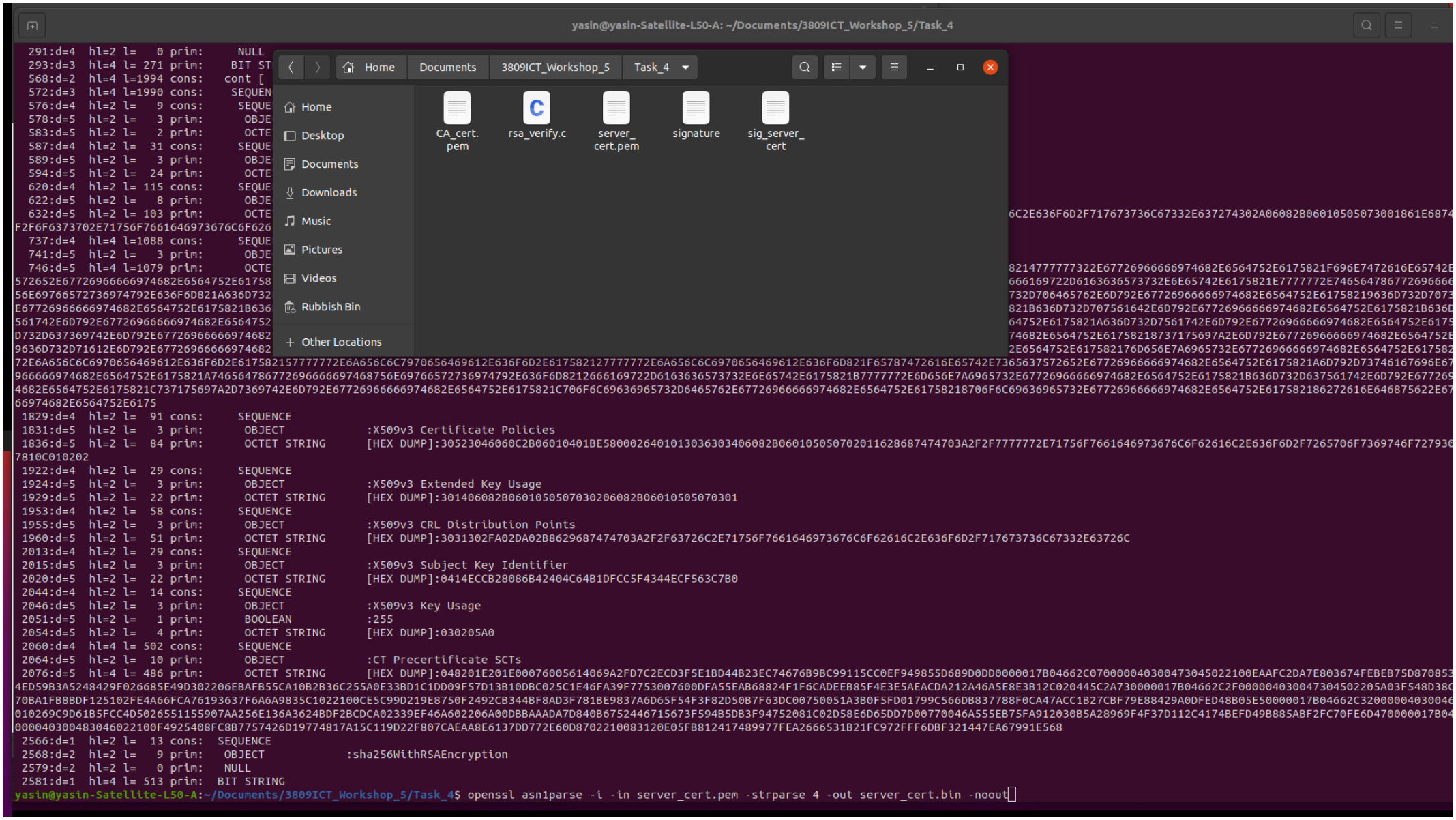
We use the following command to extract such a piece of content into a new file named server_cert.bin, and then calculate the SHA256 hash of it:

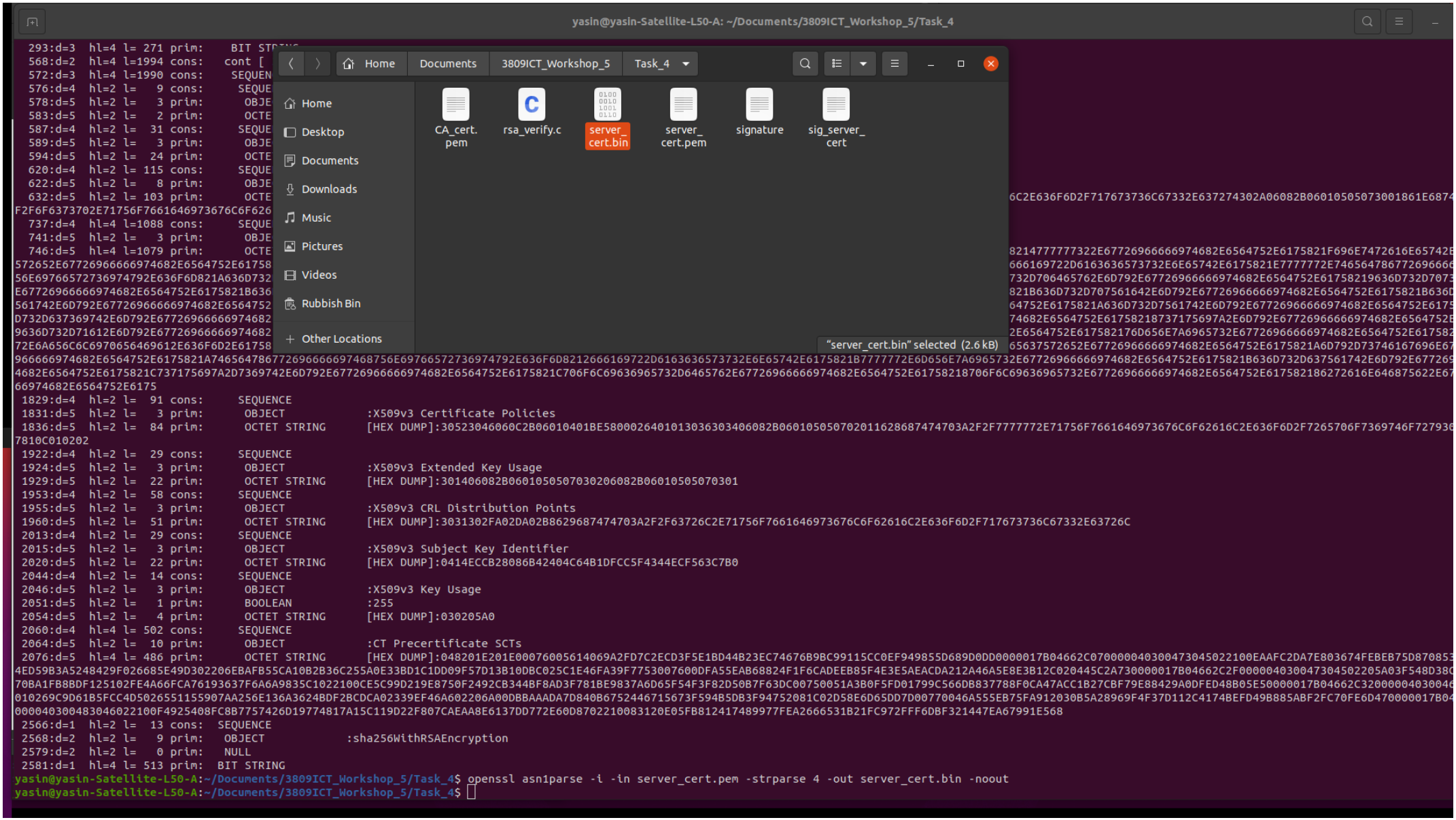
```
$ openssl asn1parse -i -in server_cert.pem -strparse 4 -out server_cert.bin -noout
$ sha256sum server_cert.bin
```

You may want to save this 256-bit hash value for the signature verification in the next step.

Answer:


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_4
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_3$ cd '/home/yasin/Documents/3809ICT_Workshop_5/Task_4'
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ ls
CA_cert.pem rsa_verify.c server_cert.pem signature sig_server_cert
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl asn1parse -i -in server_cert.pem
0:d=0 hl=4 l=3094 cons: SEQUENCE
4:d=1 hl=4 l=2558 cons: SEQUENCE
8:d=2 hl=2 l= 3 cons: cont [0]
10:d=3 hl=2 l= 1 prim: INTEGER :02
13:d=2 hl=2 l= 20 prim: INTEGER :771BE8800E7DAEE2213AEFA4880ED5E287585ECA
35:d=2 hl=2 l= 13 cons: SEQUENCE
37:d=3 hl=2 l= 9 prim: OBJECT :sha256WithRSAEncryption
48:d=3 hl=2 l= 0 prim: NULL
50:d=2 hl=2 l= 77 cons: SEQUENCE
52:d=3 hl=2 l= 11 cons: SET
54:d=4 hl=2 l= 9 cons: SEQUENCE
56:d=5 hl=2 l= 3 prim: OBJECT :countryName
61:d=5 hl=2 l= 2 prim: PRINTABLESTRING :BM
65:d=3 hl=2 l= 25 cons: SET
67:d=4 hl=2 l= 23 cons: SEQUENCE
69:d=5 hl=2 l= 3 prim: OBJECT :organizationName
74:d=5 hl=2 l= 16 prim: PRINTABLESTRING :QuoVadis Limited
92:d=3 hl=2 l= 35 cons: SET
94:d=4 hl=2 l= 33 cons: SEQUENCE
96:d=5 hl=2 l= 3 prim: OBJECT :commonName
101:d=5 hl=2 l= 26 prim: PRINTABLESTRING :QuoVadis Global SSL ICA G3
129:d=2 hl=2 l= 30 cons: SEQUENCE
131:d=3 hl=2 l= 13 prim: UTCTIME :210802005649Z
146:d=3 hl=2 l= 13 prim: UTCTIME :220802010600Z
161:d=2 hl=2 l= 111 cons: SEQUENCE
163:d=3 hl=2 l= 11 cons: SET
165:d=4 hl=2 l= 9 cons: SEQUENCE
167:d=5 hl=2 l= 3 prim: OBJECT :countryName
172:d=5 hl=2 l= 2 prim: PRINTABLESTRING :AU
176:d=3 hl=2 l= 19 cons: SET
178:d=4 hl=2 l= 17 cons: SEQUENCE
180:d=5 hl=2 l= 3 prim: OBJECT :stateOrProvinceName
185:d=5 hl=2 l= 10 prim: UTF8STRING :Queensland
197:d=3 hl=2 l= 15 cons: SET
199:d=4 hl=2 l= 13 cons: SEQUENCE
201:d=5 hl=2 l= 3 prim: OBJECT :localityName
206:d=5 hl=2 l= 6 prim: UTF8STRING :Nathan
214:d=3 hl=2 l= 28 cons: SET
216:d=4 hl=2 l= 26 cons: SEQUENCE
218:d=5 hl=2 l= 3 prim: OBJECT :organizationName
223:d=5 hl=2 l= 19 prim: UTF8STRING :Griffith University
244:d=3 hl=2 l= 28 cons: SET
246:d=4 hl=2 l= 26 cons: SEQUENCE
248:d=5 hl=2 l= 3 prim: OBJECT :commonName
253:d=5 hl=2 l= 19 prim: UTF8STRING :www.griffith.edu.au
274:d=2 hl=4 l= 290 cons: SEQUENCE
278:d=3 hl=2 l= 13 cons: SEQUENCE
280:d=4 hl=2 l= 9 prim: OBJECT :rsaEncryption
291:d=4 hl=2 l= 0 prim: NULL
293:d=3 hl=4 l= 271 prim: BIT STRING
568:d=2 hl=4 l=1994 cons: cont [3]
572:d=3 hl=4 l=1990 cons: SEQUENCE


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_4
Home
Documents
3809ICT_Workshop_5
Task_4
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
CA_cert.pem
rsa_verify.c
server_cert.pem
signature
sig_server_cert
291:d=4 hl=2 l= 0 prim: NULL
293:d=3 hl=4 l= 271 prim: BIT ST
568:d=2 hl=4 l=1994 cons: cont [
572:d=3 hl=4 l=1990 cons: SEQUEN
576:d=4 hl=2 l= 9 cons: SEQUE
578:d=5 hl=2 l= 3 prim: OBJE
583:d=5 hl=2 l= 2 prim: OCTE
587:d=4 hl=2 l= 31 cons: SEQUE
589:d=5 hl=2 l= 3 prim: OBJE
594:d=5 hl=2 l= 24 prim: OCTE
620:d=4 hl=2 l= 115 cons: SEQUE
622:d=5 hl=2 l= 8 prim: OBJE
632:d=5 hl=2 l= 103 prim: OCTE
737:d=4 hl=4 l=1088 cons: SEQUE
741:d=5 hl=2 l= 3 prim: OBJE
746:d=5 hl=4 l=1079 prim: OCTE
1829:d=4 hl=2 l= 91 cons: SEQUENCE
1831:d=5 hl=2 l= 3 prim: OBJECT :X509v3 Certificate Policies
1836:d=5 hl=2 l= 84 prim: OCTET STRING [HEX DUMP]:30523046060C2B06010401BE5800026401013036303406082B0601050507020116286874747703A2F2F7777772E71756F7661646973676C6F62616C2E636F6D2F7265706F7369746F727930
7810C010202
1922:d=4 hl=2 l= 29 cons: SEQUENCE
1924:d=5 hl=2 l= 3 prim: OBJECT :X509v3 Extended Key Usage
1929:d=5 hl=2 l= 22 prim: OCTET STRING [HEX DUMP]:301406082B0601050507030206082B06010505070301
1953:d=4 hl=2 l= 58 cons: SEQUENCE
1955:d=5 hl=2 l= 3 prim: OBJECT :X509v3 CRL Distribution Points
1960:d=5 hl=2 l= 51 prim: OCTET STRING [HEX DUMP]:3031302FA02DA02B8629687474703A2F2F63726C2E71756F7661646973676C6F62616C2E636F6D2F717673736C67332E63726C
2013:d=4 hl=2 l= 29 cons: SEQUENCE
2015:d=5 hl=2 l= 3 prim: OBJECT :X509v3 Subject Key Identifier
2020:d=5 hl=2 l= 22 prim: OCTET STRING [HEX DUMP]:0414ECCB28086B42404C64B1DFCC5F4344ECF563C7B0
2044:d=4 hl=2 l= 14 cons: SEQUENCE
2046:d=5 hl=2 l= 3 prim: OBJECT :X509v3 Key Usage
2051:d=5 hl=2 l= 1 prim: BOOLEAN :255
2054:d=5 hl=2 l= 4 prim: OCTET STRING [HEX DUMP]:030205A0
2060:d=4 hl=4 l= 502 cons: SEQUENCE
2064:d=5 hl=2 l= 10 prim: OBJECT :CT Precertificate SCTs
2076:d=5 hl=4 l= 486 prim: OCTET STRING [HEX DUMP]:048201E201E00076005614069A2FD7C2ECD3F5E1BD44B23EC74676B9BC99115CC0EF949855D689D0DD0000017B04662C0700000403004730450221
2566:d=1 hl=2 l= 13 cons: SEQUENCE
2568:d=2 hl=2 l= 9 prim: OBJECT :sha256WithRSAEncryption
2579:d=2 hl=2 l= 0 prim: NULL
2581:d=1 hl=4 l= 513 prim: BIT STRING
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl asn1parse -i -in server_cert.pem -strparse 4 -out server_cert.bin -noout


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_4
Home
Documents
3809ICT_Workshop_5
Task_4
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
CA_cert.pem
rsa_verify.c
server_cert.bin
server_cert.pem
signature
sig_server_cert
"server_cert.bin" selected (2.6 kB)
293:d=3 hl=4 l= 271 prim: BIT STRING
568:d=2 hl=4 l=1994 cons: cont [
572:d=3 hl=4 l=1990 cons: SEQUEN
576:d=4 hl=2 l= 9 cons: SEQUE
578:d=5 hl=2 l= 3 prim: OBJE
583:d=5 hl=2 l= 2 prim: OCTE
587:d=4 hl=2 l= 31 cons: SEQUE
589:d=5 hl=2 l= 3 prim: OBJE
594:d=5 hl=2 l= 24 prim: OCTE
620:d=4 hl=2 l= 115 cons: SEQUE
622:d=5 hl=2 l= 8 prim: OBJE
632:d=5 hl=2 l= 103 prim: OCTE
737:d=4 hl=4 l=1088 cons: SEQUE
741:d=5 hl=2 l= 3 prim: OBJE
746:d=5 hl=4 l=1079 prim: OCTE
1829:d=4 hl=2 l= 91 cons: SEQUENCE
1831:d=5 hl=2 l= 3 prim: OBJECT :X509v3 Certificate Policies
1836:d=5 hl=2 l= 84 prim: OCTET STRING [HEX DUMP]:30523046060C2B06010401BE5800026401013036303406082B06010505070201162868747470 3A2F2F7777772E71756F7661646973676C6F62616C2E636F6D2F7265706F7369746F727930
1922:d=4 hl=2 l= 29 cons: SEQUENCE
1924:d=5 hl=2 l= 3 prim: OBJECT :X509v3 Extended Key Usage
1929:d=5 hl=2 l= 22 prim: OCTET STRING [HEX DUMP]:30140608 2B06010505070302060 82B06010505070301
1953:d=4 hl=2 l= 58 cons: SEQUENCE
1955:d=5 hl=2 l= 3 prim: OBJECT :X509v3 CRL Distribution Points
1960:d=5 hl=2 l= 51 prim: OCTET STRING [HEX DUMP]:3031302FA02DA02B8629687474703A2F2F63726C2E71756F7661646973676C6F62616C2E636F6D2F717673736C67332E63726C
2013:d=4 hl=2 l= 29 cons: SEQUENCE
2015:d=5 hl=2 l= 3 prim: OBJECT :X509v3 Subject Key Identifier
2020:d=5 hl=2 l= 22 prim: OCTET STRING [HEX DUMP]:0414ECCB28086B42404C64B1DFCC5F4344ECF563C7B0
2044:d=4 hl=2 l= 14 cons: SEQUENCE
2046:d=5 hl=2 l= 3 prim: OBJECT :X509v3 Key Usage
2051:d=5 hl=2 l= 1 prim: BOOLEAN :255
2054:d=5 hl=2 l= 4 prim: OCTET STRING [HEX DUMP]:030205A0
2060:d=4 hl=4 l= 502 cons: SEQUENCE
2064:d=5 hl=2 l= 10 prim: OBJECT :CT Precertificate SCTs
2076:d=5 hl=4 l= 486 prim: OCTET STRING [HEX DUMP]:048201E201E00076005614069A2FD7C2ECD3F5E1BD44B23EC74676B9BC99115CC0EF949855D689D0DD0000017B04662C0700000403004730450221 00EAAFC2DA7E803674FEBEB75D870853
2566:d=1 hl=2 l= 13 cons: SEQUENCE
2568:d=2 hl=2 l= 9 prim: OBJECT :sha256WithRSAEncryption
2579:d=2 hl=2 l= 0 prim: NULL
2581:d=1 hl=4 l= 513 prim: BIT STRING
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl asn1parse -i -in server_cert.pem -strparse 4 -out server_cert.bin -noout
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$

5. Now we have obtained the CA's public key (e, n), the server's certificate content signed by CA with its private key (we may represent it as M), the signature of that content (represented as S) and the hash of the content (i.e., SHA256(M)).

   Recall that the encryption algorithm the RSA encryption system is essentially identical to the verification algorithm of the RSA digital signature system. So, we can use the c program for RSA encryption from workshop 4 Run hybrid_dec.sh to decrypt the ciphertext. Check if the decryption worked.

   Here the verification checks if S^e mod n equals SHA256(M) or not. Copying the the values of n, S, e to the program rsa_verify.c (which can be found from the Week 6 folder on http://networksecurity.griffith.internal/ via the VM's web browser.)

   Then compile the c source file, execute the obtained executable and check if you recovered the value SHA256(M), i.e., the 256-bit hash value of server_cert_body.bin.

   (Note: You may find some other data apart from the hash value. That is due to some padding operations and can be ignored for this task.)

   Answer:

```
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ gcc rsa_verify.c -lcrypto
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ ./a.out
SHA256 of the document: 01FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF003031300D060960864801650304020105000420A8F6739C2E728C8B03486B1940525A08DE7725F0D7205B7D8BDFFAB63E503AAD
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ sha256sum server_cert.bin
a8f6739c2e728c8b03486b1940525a08de7725f0d7205b7d8bdffab63e503aad  server_cert.bin
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$
```

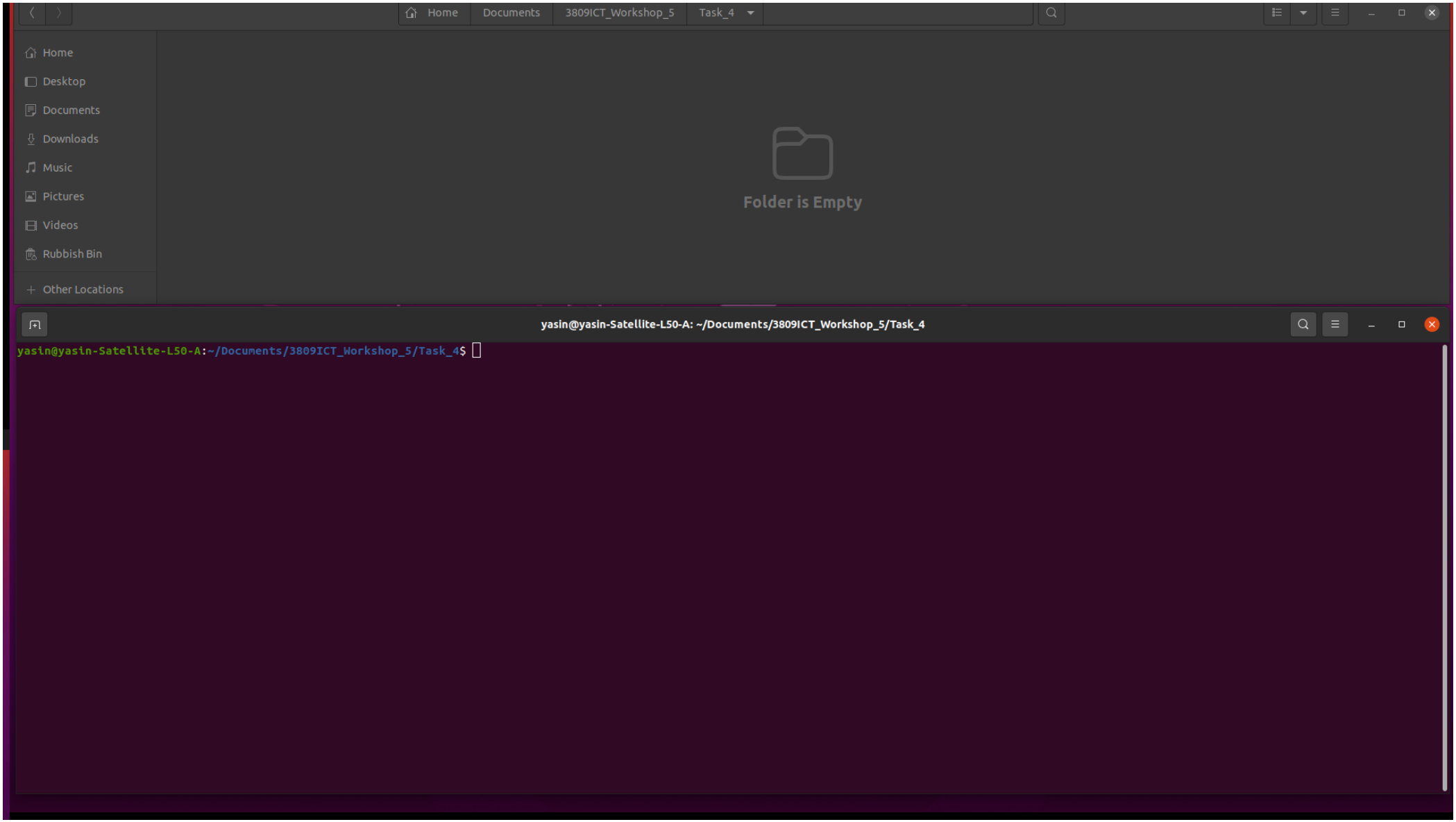
Task 4: Diffie-Hellman Key-Exchange from OpenSSL

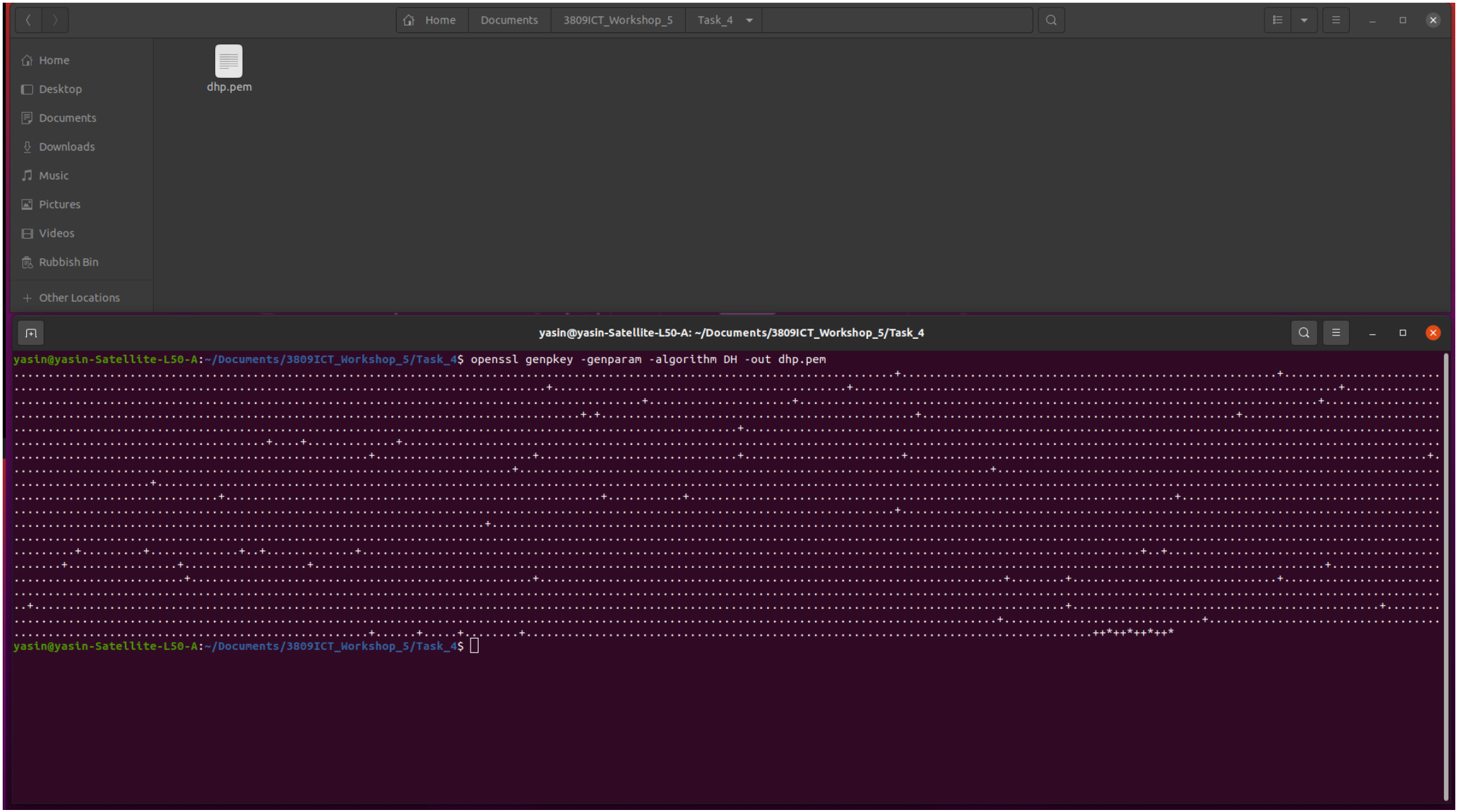
In this task, we see how does the basic Diffie-Hellman Key Exchange work with OpenSSL

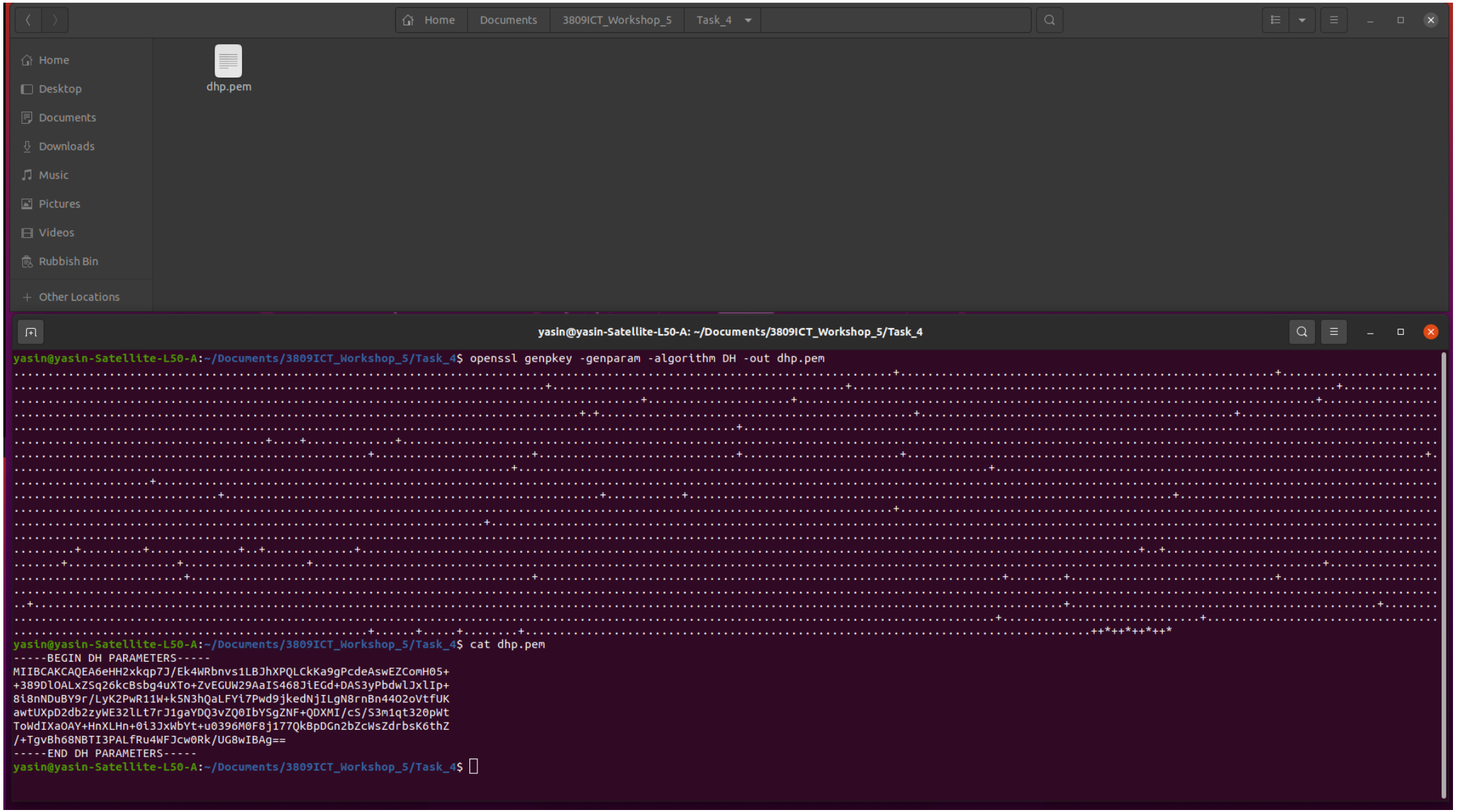
1. Recall that Diffile-Hellman (DH) Key-Exchange protocol needs two parameters that are publicly available to every user. They are a prime number p which is at least 2048 bits long, and a generator g which generates the set {0,1,..., p-1} by running through g^i mod p for i = {0,1,2,...,p-1}. We invoke the following command to generate these DH parameters:

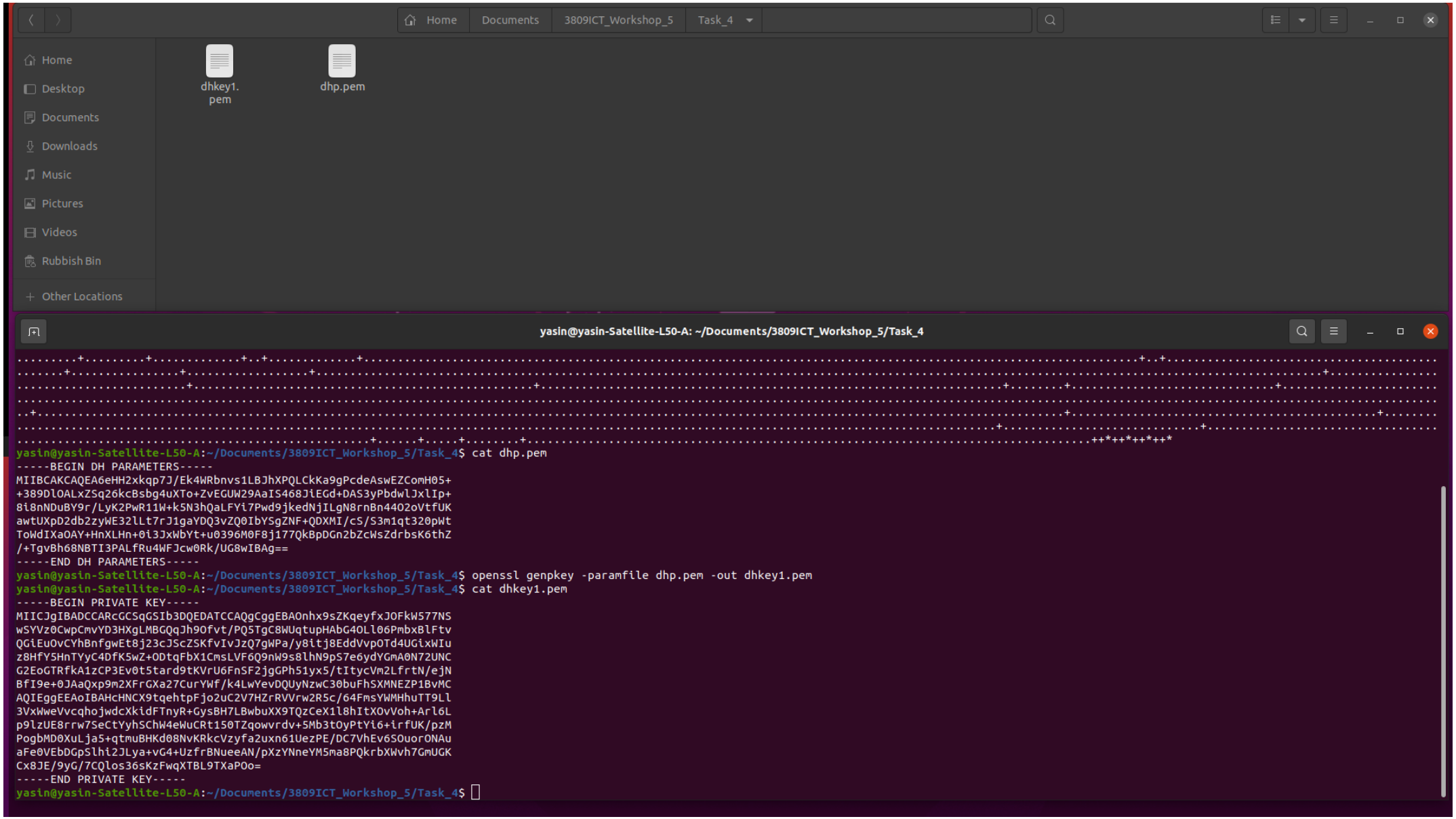
   ```
   $ openssl genpkey -genparam -algorithm DH -out dhp.pem
   ```

   Answer:


Home
Documents
3809ICT_Workshop_5
Task_4
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
Folder is Empty
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_4
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$


Home
Documents
3809ICT_Workshop_5
Task_4
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
dhp.pem
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_4
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl genpkey -genparam -algorithm DH -out dhp.pem
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$


Home
Documents
3809ICT_Workshop_5
Task_4
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
dhp.pem
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_4
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl genpkey -genparam -algorithm DH -out dhp.pem
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ cat dhp.pem
-----BEGIN DH PARAMETERS-----
MIIBCAKCAQEA6eHH2xkqp7J/Ek4WRbnvs1LBJhXPQLCkKa9gPcdeAswEZComH05+
+389DlOALxZSq26kcBsbg4uXTo+ZvEGUW29AaIS468JiEGd+DAS3yPbdwlJxlIp+
8i8nNDuBY9r/LyK2PwR11W+k5N3hQaLFYi7Pwd9jkedNjILgN8rnBn44O2oVtfUK
awtUXpD2db2zyWE32lLt7rJ1gaYDQ3vZQ0IbYSgZNF+QDXMI/cS/S3m1qt320pWt
ToWdIXaOAY+HnXLHn+0i3JxWbYt+u0396M0F8j177QkBpDGn2bZcWsZdrbsK6thZ
/+TgvBh68NBTI3PALfRu4WFJcw0Rk/UG8wIBAg==
-----END DH PARAMETERS-----
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$


Home
Documents
3809ICT_Workshop_5
Task_4
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
dhkey1.pem
dhp.pem
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_4
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ cat dhp.pem
-----BEGIN DH PARAMETERS-----
MIIBCAKCAQEA6eHH2xkqp7J/Ek4WRbnvs1LBJhXPQLCkKa9gPcdeAswEZComH05+
+389DlOALxZSq26kcBsbg4uXTo+ZvEGUW29AaIS468JiEGd+DAS3yPbdwlJxlIp+
8i8nNDuBY9r/LyK2PwR11W+k5N3hQaLFYi7Pwd9jkedNjILgN8rnBn44O2oVtfUK
awtUXpD2db2zyWE32lLt7rJ1gaYDQ3vZQ0IbYSgZNF+QDXMI/cS/S3m1qt320pWt
ToWdIXaOAY+HnXLHn+0i3JxWbYt+u0396M0F8j177QkBpDGn2bZcWsZdrbsK6thZ
/+TgvBh68NBTI3PALfRu4WFJcw0Rk/UG8wIBAg==
-----END DH PARAMETERS-----
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl genpkey -paramfile dhp.pem -out dhkey1.pem
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ cat dhkey1.pem
-----BEGIN PRIVATE KEY-----
MIICJgIBADCCARcGCSqGSIb3DQEDATCCAQgCggEBAOnhx9sZKqeyfxJOFkW577NS
wSYVz0CwpCmvYD3HXgLMBGQqJh9Ofvt/PQ5TgC8WUqtupHAbG4OLl06PmbxBlFtv
QGiEuOvCYhBnfgwEt8j23cJScZSKfvIvJzQ7gWPa/y8itj8EddVvpOTd4UGixWIu
z8HfY5HnTYyC4DfK5wZ+ODtqFbX1CmsLVF6Q9nW9s8lhN9pS7e6ydYGmA0N72UNC
G2EoGTRfkA1zCP3Ev0t5tard9tKVrU6FnSF2jgGPh51yx5/tItycVm2LfrtN/ejN
BfI9e+0JAaQxp9m2XFrGXa27CurYWf/k4LwYevDQUyNzwC30buFhSXMNEZP1BvMC
AQIEggEEAoIBAHcHNCX9tqehtpFjo2uC2V7HZrRVVrw2R5c/64FmsYWMHhuTT9Ll
3VxWweVvcqhojwdcXkidFTnyR+GysBH7LBwbuXX9TQzCeX1l8hItXOvVoh+Arl6L
p9lzUE8rrw7SeCtYyhSChW4eWuCRt150TZqowvrdv+5Mb3tOyPtYi6+irfUK/pzM
PogbMD0XuLja5+qtmuBHKd08NvKRkcVzyfa2uxn61UezPE/DC7VhEv6SOuorONAu
aFe0VEbDGpSlhi2JLya+vG4+UzfrBNueeAN/pXzYNneYM5ma8PQkrbXWvh7GmUGK
Cx8JE/9yG/7CQlos36sKzFwqXTBL9TXaPOo=
-----END PRIVATE KEY-----
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$

2. Next, we generate two DH public/private key pairs (for two users). The user 1 runs

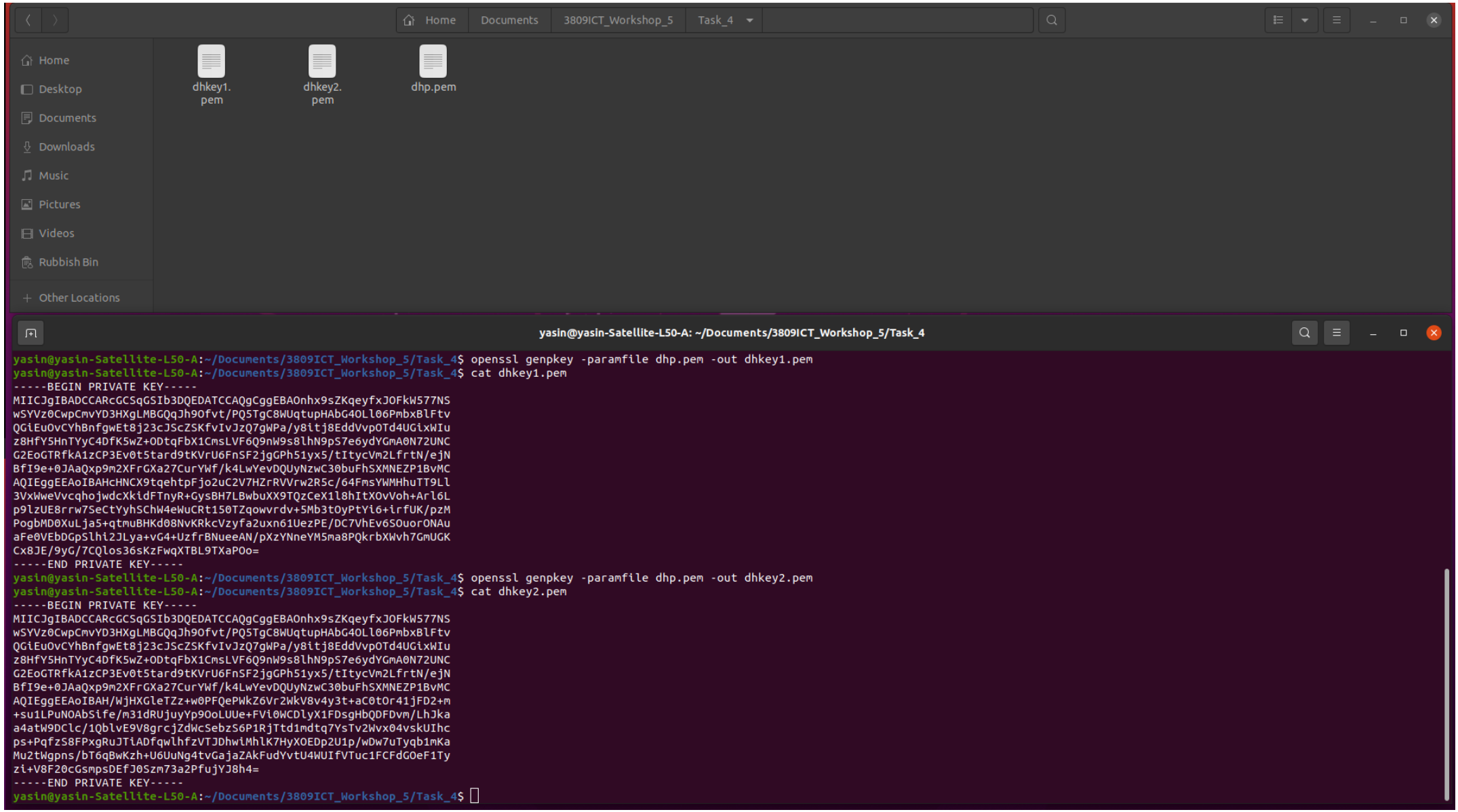
   ```
   $ openssl genpkey -paramfile dhp.pem -out dhkey1.pem
   ```

   and keeps dhkey1.pem. User 2 runs

   ```
   $ openssl genpkey -paramfile dhp.pem -out dhkey2.pem
   ```

   and keeps dhkey2.pem.

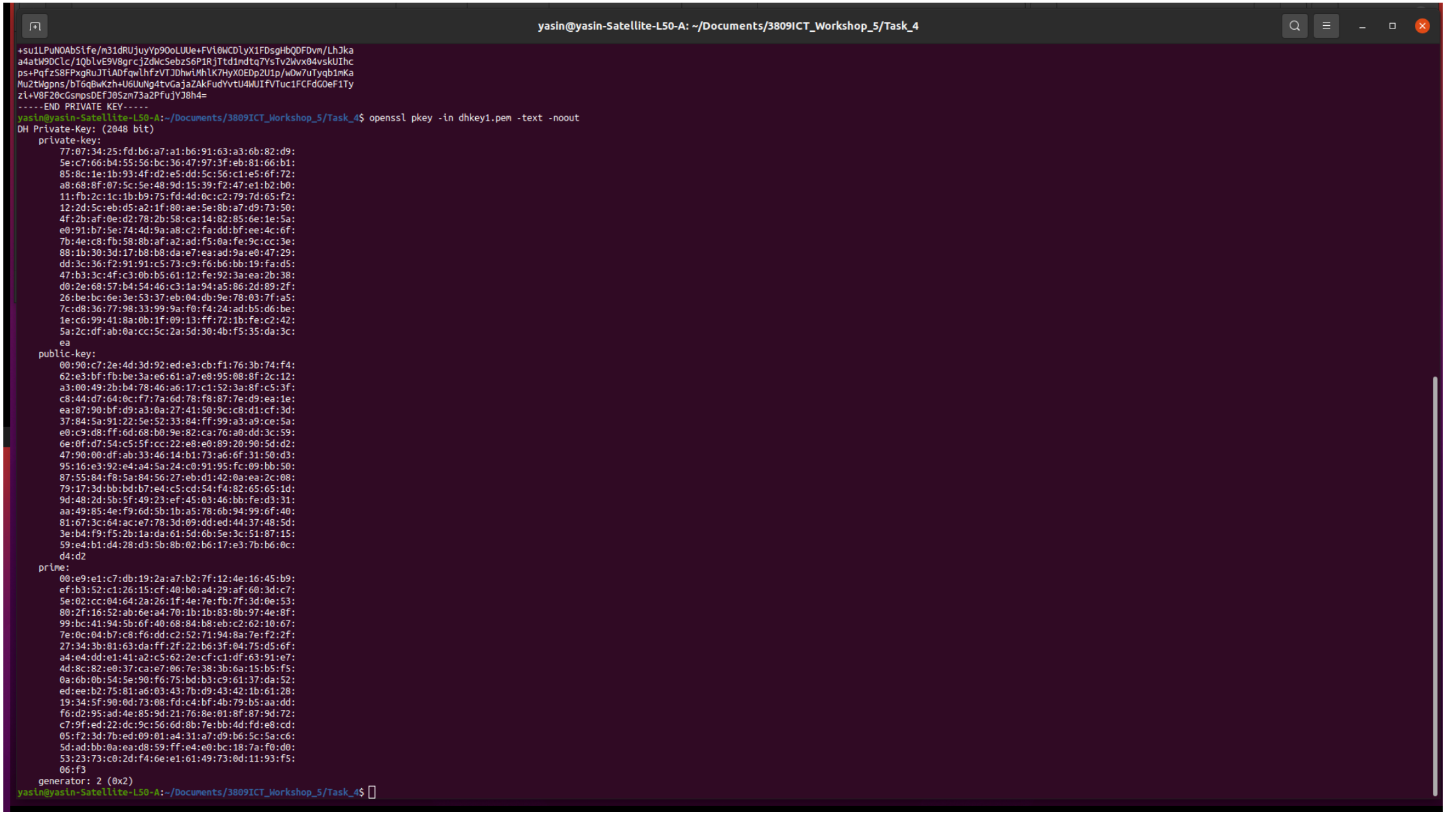
   Answer:

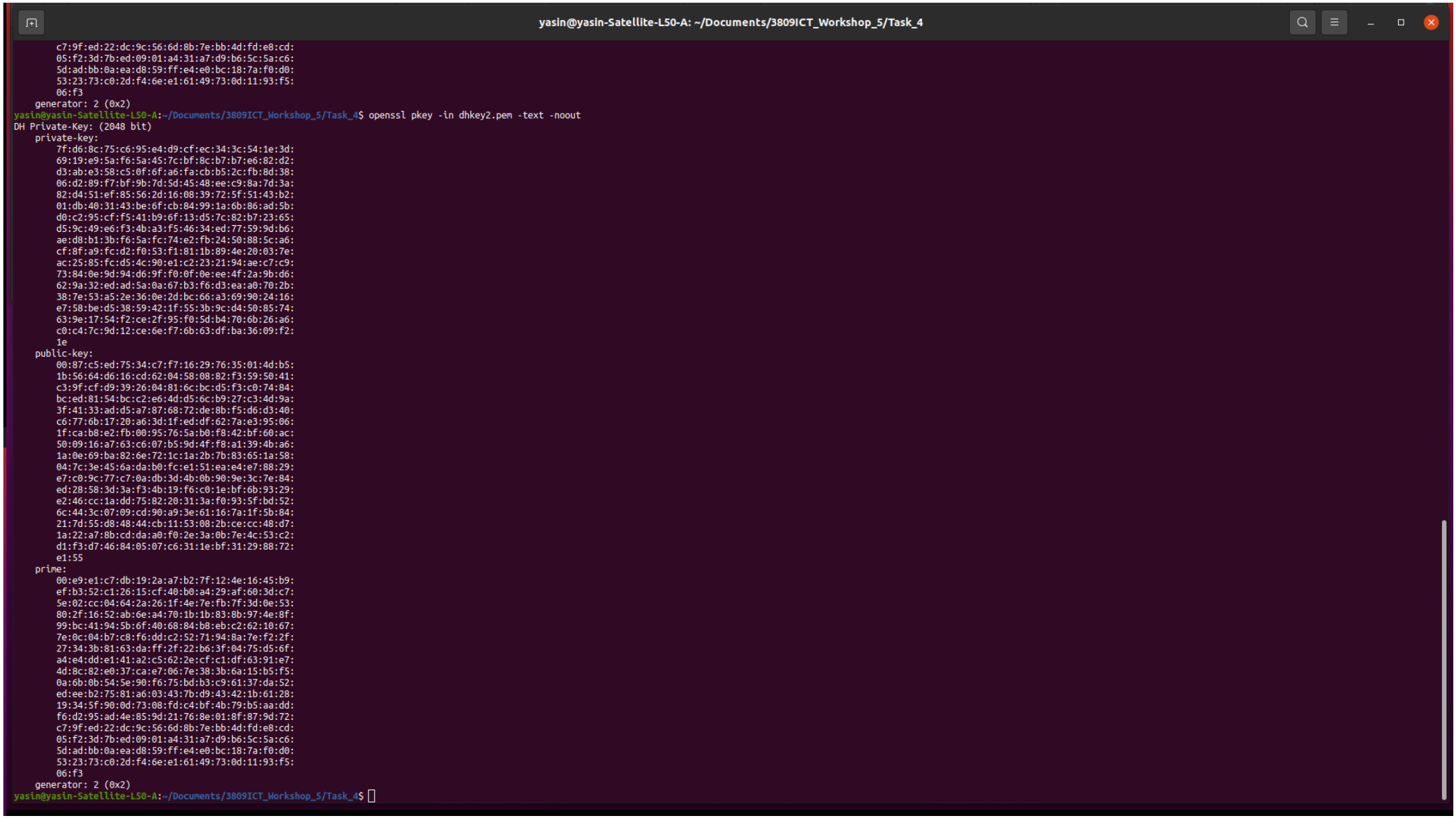

Home
Documents
3809ICT_Workshop_5
Task_4
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
dhkey1.pem
dhkey2.pem
dhp.pem
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_4
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl genpkey -paramfile dhp.pem -out dhkey1.pem
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ cat dhkey1.pem
-----BEGIN PRIVATE KEY-----
MIICJgIBADCCARcGCSqGSIb3DQEDATCCAQgCggEBAOnhx9sZKqeyfxJOFkW577NS
wSYVz0CwpCmvYD3HXgLMBGQqJh9Ofvt/PQ5TgC8WUqtupHAbG4OLl06PmbxBlFtv
QGiEuOvCYhBnfgwEt8j23cJScZSKfvIvJzQ7gWPa/y8itj8EddVvpOTd4UGixWIu
z8HfY5HnTYyC4DfK5wZ+ODtqFbX1CmsLVF6Q9nW9s8lhN9pS7e6ydYGmA0N72UNC
G2EoGTRfkA1zCP3Ev0t5tard9tKVrU6FnSF2jgGPh51yx5/tItycVm2LfrtN/ejN
BfI9e+0JAaQxp9m2XFrGXa27CurYWf/k4LwYevDQUyNzwC30buFhSXMNEZP1BvMC
AQIEggEEAoIBAHcHNCX9tqehtpFjo2uC2V7HZrRVVrw2R5c/64FmsYWMHhuTT9Ll
3VxWweVvcqhojwdcXkidFTnyR+GysBH7LBwbuXX9TQzCeX1l8hItXOvVoh+Arl6L
p9lzUE8rrw7SeCtYyhSChW4eWuCRt150TZqowvrdv+5Mb3tOyPtYi6+irfUK/pzM
PogbMD0XuLja5+qtmuBHKd08NvKRkcVzyfa2uxn61UezPE/DC7VhEv6SOuorONAu
aFe0VEbDGpSlhi2JLya+vG4+UzfrBNueeAN/pXzYNneYM5ma8PQkrbXWvh7GmUGK
Cx8JE/9yG/7CQlos36sKzFwqXTBL9TXaPOo=
-----END PRIVATE KEY-----
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl genpkey -paramfile dhp.pem -out dhkey2.pem
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ cat dhkey2.pem
-----BEGIN PRIVATE KEY-----
MIICJgIBADCCARcGCSqGSIb3DQEDATCCAQgCggEBAOnhx9sZKqeyfxJOFkW577NS
wSYVz0CwpCmvYD3HXgLMBGQqJh9Ofvt/PQ5TgC8WUqtupHAbG4OLl06PmbxBlFtv
QGiEuOvCYhBnfgwEt8j23cJScZSKfvIvJzQ7gWPa/y8itj8EddVvpOTd4UGixWIu
z8HfY5HnTYyC4DfK5wZ+ODtqFbX1CmsLVF6Q9nW9s8lhN9pS7e6ydYGmA0N72UNC
G2EoGTRfkA1zCP3Ev0t5tard9tKVrU6FnSF2jgGPh51yx5/tItycVm2LfrtN/ejN
BfI9e+0JAaQxp9m2XFrGXa27CurYWf/k4LwYevDQUyNzwC30buFhSXMNEZP1BvMC
AQIEggEEAoIBAH/WjHXGleTZz+w0PFQePWkZ6Vr2WkV8v4y3t+aC0tOr41jFD2+m
+su1LPuNOAbSife/m31dRUjuyYp9OoLUUe+FVi0WCDlyX1FDsgHbQDFDvm/LhJka
a4atW9DClc/1QblvE9V8grcjZdWcSebzS6P1RjTtd1mdtq7YsTv2Wvx04vskUIhc
ps+PqfzS8FPxgRuJTiADfqwlhfzVTJDhwiMhlK7HyXOEDp2U1p/wDw7uTyqb1mKa
Mu2tWgpns/bT6qBwKzh+U6UuNg4tvGajaZAkFudYvtU4WUIfVTuc1FCFdGOeF1Ty
zi+V8F20cGsmpsDEfJ0Szm73a2PfujYJ8h4=
-----END PRIVATE KEY-----
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$

3. We can display the keys by:

   $ openssl pkey -in dhkey1.pem -text -noout
   $ openssl pkey -in dhkey2.pem -text -noout

   Answer:


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_4
+su1LPuNOAbSife/m31dRUjuyYp9OoLUUe+FVi0WCDlyX1FDsgHbQDFDvm/LhJka
a4atW9DClc/1QblvE9V8grcjZdWcSebzS6P1RjTtd1mdtq7YsTv2Wvx04vskUIhc
ps+PqfzS8FPxgRuJTiADfqwlhfzVTJDhwiMhlK7HyXOEDp2U1p/wDw7uTyqb1mKa
Mu2tWgpns/bT6qBwKzh+U6UuNg4tvGajaZAkFudYvtU4WUIfVTuc1FCFdGOeF1Ty
zi+V8F20cGsmpsDEfJ0Szm73a2PfujYJ8h4=
-----END PRIVATE KEY-----
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl pkey -in dhkey1.pem -text -noout
DH Private-Key: (2048 bit)
private-key:
77:07:34:25:fd:b6:a7:a1:b6:91:63:a3:6b:82:d9:
5e:c7:66:b4:55:56:bc:36:47:97:3f:eb:81:66:b1:
85:8c:1e:1b:93:4f:d2:e5:dd:5c:56:c1:e5:6f:72:
a8:68:8f:07:5c:5e:48:9d:15:39:f2:47:e1:b2:b0:
11:fb:2c:1c:1b:b9:75:fd:4d:0c:c2:79:7d:65:f2:
12:2d:5c:eb:d5:a2:1f:80:ae:5e:8b:a7:d9:73:50:
4f:2b:af:0e:d2:78:2b:58:ca:14:82:85:6e:1e:5a:
e0:91:b7:5e:74:4d:9a:a8:c2:fa:dd:bf:ee:4c:6f:
7b:4e:c8:fb:58:8b:af:a2:ad:f5:0a:fe:9c:cc:3e:
88:1b:30:3d:17:b8:b8:da:e7:ea:ad:9a:e0:47:29:
dd:3c:36:f2:91:91:c5:73:c9:f6:b6:bb:19:fa:d5:
47:b3:3c:4f:c3:0b:b5:61:12:fe:92:3a:ea:2b:38:
d0:2e:68:57:b4:54:46:c3:1a:94:a5:86:2d:89:2f:
26:be:bc:6e:3e:53:37:eb:04:db:9e:78:03:7f:a5:
7c:d8:36:77:98:33:99:9a:f0:f4:24:ad:b5:d6:be:
1e:c6:99:41:8a:0b:1f:09:13:ff:72:1b:fe:c2:42:
5a:2c:df:ab:0a:cc:5c:2a:5d:30:4b:f5:35:da:3c:
ea
public-key:
00:90:c7:2e:4d:3d:92:ed:e3:cb:f1:76:3b:74:f4:
62:e3:bf:fb:be:3a:e6:61:a7:e8:95:08:8f:2c:12:
a3:00:49:2b:b4:78:46:a6:17:c1:52:3a:8f:c5:3f:
c8:44:d7:64:0c:f7:7a:6d:78:f8:87:7e:d9:ea:1e:
ea:87:90:bf:d9:a3:0a:27:41:50:9c:c8:d1:cf:3d:
37:84:5a:91:22:5e:52:33:84:ff:99:a3:a9:ce:5a:
e0:c9:d8:ff:6d:68:b0:9e:82:ca:76:a0:dd:3c:59:
6e:0f:d7:54:c5:5f:cc:22:e8:e0:89:20:90:5d:d2:
47:90:00:df:ab:33:46:14:b1:73:a6:6f:31:50:d3:
95:16:e3:92:e4:a4:5a:24:c0:91:95:fc:09:bb:50:
87:55:84:f8:5a:84:56:27:eb:d1:42:0a:ea:2c:08:
79:17:3d:bb:bd:b7:e4:c5:cd:54:f4:82:65:65:1d:
9d:48:2d:5b:5f:49:23:ef:45:03:46:bb:fe:d3:31:
aa:49:85:4e:f9:6d:5b:1b:a5:78:6b:94:99:6f:40:
81:67:3c:64:ac:e7:78:3d:09:dd:ed:44:37:48:5d:
3e:b4:f9:f5:2b:1a:da:61:5d:6b:5e:3c:51:87:15:
59:e4:b1:d4:28:d3:5b:8b:02:b6:17:e3:7b:b6:0c:
d4:d2
prime:
00:e9:e1:c7:db:19:2a:a7:b2:7f:12:4e:16:45:b9:
ef:b3:52:c1:26:15:cf:40:b0:a4:29:af:60:3d:c7:
5e:02:cc:04:64:2a:26:1f:4e:7e:fb:7f:3d:0e:53:
80:2f:16:52:ab:6e:a4:70:1b:1b:83:8b:97:4e:8f:
99:bc:41:94:5b:6f:40:68:84:b8:eb:c2:62:10:67:
7e:0c:04:b7:c8:f6:dd:c2:52:71:94:8a:7e:f2:2f:
27:34:3b:81:63:da:ff:2f:22:b6:3f:04:75:d5:6f:
a4:e4:dd:e1:41:a2:c5:62:2e:cf:c1:df:63:91:e7:
4d:8c:82:e0:37:ca:e7:06:7e:38:3b:6a:15:b5:f5:
0a:6b:0b:54:5e:90:f6:75:bd:b3:c9:61:37:da:52:
ed:ee:b2:75:81:a6:03:43:7b:d9:43:42:1b:61:28:
19:34:5f:90:0d:73:08:fd:c4:bf:4b:79:b5:aa:dd:
f6:d2:95:ad:4e:85:9d:21:76:8e:01:8f:87:9d:72:
c7:9f:ed:22:dc:9c:56:6d:8b:7e:bb:4d:fd:e8:cd:
05:f2:3d:7b:ed:09:01:a4:31:a7:d9:b6:5c:5a:c6:
5d:ad:bb:0a:ea:d8:59:ff:e4:e0:bc:18:7a:f0:d0:
53:23:73:c0:2d:f4:6e:e1:61:49:73:0d:11:93:f5:
06:f3
generator: 2 (0x2)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_4
c7:9f:ed:22:dc:9c:56:6d:8b:7e:bb:4d:fd:e8:cd:
05:f2:3d:7b:ed:09:01:a4:31:a7:d9:b6:5c:5a:c6:
5d:ad:bb:0a:ea:d8:59:ff:e4:e0:bc:18:7a:f0:d0:
53:23:73:c0:2d:f4:6e:e1:61:49:73:0d:11:93:f5:
06:f3
generator: 2 (0x2)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl pkey -in dhkey2.pem -text -noout
DH Private-Key: (2048 bit)
private-key:
7f:d6:8c:75:c6:95:e4:d9:cf:ec:34:3c:54:1e:3d:
69:19:e9:5a:f6:5a:45:7c:bf:8c:b7:b7:e6:82:d2:
d3:ab:e3:58:c5:0f:6f:a6:fa:cb:b5:2c:fb:8d:38:
06:d2:89:f7:bf:9b:7d:5d:45:48:ee:c9:8a:7d:3a:
82:d4:51:ef:85:56:2d:16:08:39:72:5f:51:43:b2:
01:db:40:31:43:be:6f:cb:84:99:1a:6b:86:ad:5b:
d0:c2:95:cf:f5:41:b9:6f:13:d5:7c:82:b7:23:65:
d5:9c:49:e6:f3:4b:a3:f5:46:34:ed:77:59:9d:b6:
ae:d8:b1:3b:f6:5a:fc:74:e2:fb:24:50:88:5c:a6:
cf:8f:a9:fc:d2:f0:53:f1:81:1b:89:4e:20:03:7e:
ac:25:85:fc:d5:4c:90:e1:c2:23:21:94:ae:c7:c9:
73:84:0e:9d:94:d6:9f:f0:0f:0e:ee:4f:2a:9b:d6:
62:9a:32:ed:ad:5a:0a:67:b3:f6:d3:ea:a0:70:2b:
38:7e:53:a5:2e:36:0e:2d:bc:66:a3:69:90:24:16:
e7:58:be:d5:38:59:42:1f:55:3b:9c:d4:50:85:74:
63:9e:17:54:f2:ce:2f:95:f0:5d:b4:70:6b:26:a6:
c0:c4:7c:9d:12:ce:6e:f7:6b:63:df:ba:36:09:f2:
1e
public-key:
00:87:c5:ed:75:34:c7:f7:16:29:76:35:01:4d:b5:
1b:56:64:d6:16:cd:62:04:58:08:82:f3:59:50:41:
c3:9f:cf:d9:39:26:04:81:6c:bc:d5:f3:c0:74:84:
bc:ed:81:54:bc:c2:e6:4d:d5:6c:b9:27:c3:4d:9a:
3f:41:33:ad:d5:a7:87:68:72:de:8b:f5:d6:d3:40:
c6:77:6b:17:20:a6:3d:1f:ed:df:62:7a:e3:95:06:
1f:ca:b8:e2:fb:00:95:76:5a:b0:f8:42:bf:60:ac:
50:09:16:a7:63:c6:07:b5:9d:4f:f8:a1:39:4b:a6:
1a:0e:69:ba:82:6e:72:1c:1a:2b:7b:83:65:1a:58:
04:7c:3e:45:6a:da:b0:fc:e1:51:ea:e4:e7:88:29:
e7:c0:9c:77:c7:0a:db:3d:4b:0b:90:9e:3c:7e:84:
ed:28:58:3d:3a:f3:4b:19:f6:c0:1e:bf:6b:93:29:
e2:46:cc:1a:dd:75:82:20:31:3a:f0:93:5f:bd:52:
6c:44:3c:07:09:cd:90:a9:3e:61:16:7a:1f:5b:84:
21:7d:55:d8:48:44:cb:11:53:08:2b:ce:cc:48:d7:
1a:22:a7:8b:cd:da:a0:f0:2e:3a:0b:7e:4c:53:c2:
d1:f3:d7:46:84:05:07:c6:31:1e:bf:31:29:88:72:
e1:55
prime:
00:e9:e1:c7:db:19:2a:a7:b2:7f:12:4e:16:45:b9:
ef:b3:52:c1:26:15:cf:40:b0:a4:29:af:60:3d:c7:
5e:02:cc:04:64:2a:26:1f:4e:7e:fb:7f:3d:0e:53:
80:2f:16:52:ab:6e:a4:70:1b:1b:83:8b:97:4e:8f:
99:bc:41:94:5b:6f:40:68:84:b8:eb:c2:62:10:67:
7e:0c:04:b7:c8:f6:dd:c2:52:71:94:8a:7e:f2:2f:
27:34:3b:81:63:da:ff:2f:22:b6:3f:04:75:d5:6f:
a4:e4:dd:e1:41:a2:c5:62:2e:cf:c1:df:63:91:e7:
4d:8c:82:e0:37:ca:e7:06:7e:38:3b:6a:15:b5:f5:
0a:6b:0b:54:5e:90:f6:75:bd:b3:c9:61:37:da:52:
ed:ee:b2:75:81:a6:03:43:7b:d9:43:42:1b:61:28:
19:34:5f:90:0d:73:08:fd:c4:bf:4b:79:b5:aa:dd:
f6:d2:95:ad:4e:85:9d:21:76:8e:01:8f:87:9d:72:
c7:9f:ed:22:dc:9c:56:6d:8b:7e:bb:4d:fd:e8:cd:
05:f2:3d:7b:ed:09:01:a4:31:a7:d9:b6:5c:5a:c6:
5d:ad:bb:0a:ea:d8:59:ff:e4:e0:bc:18:7a:f0:d0:
53:23:73:c0:2d:f4:6e:e1:61:49:73:0d:11:93:f5:
06:f3
generator: 2 (0x2)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$

4. To compute a shared secret key, the public keys need to be extracted and share by the two users. To extract the public keys from the key files dhkey1.pem and dhkey2.pem, user 1 does:

   ```
   $ openssl pkey -in dhkey1.pem -pubout -out pub1.pem
   ```

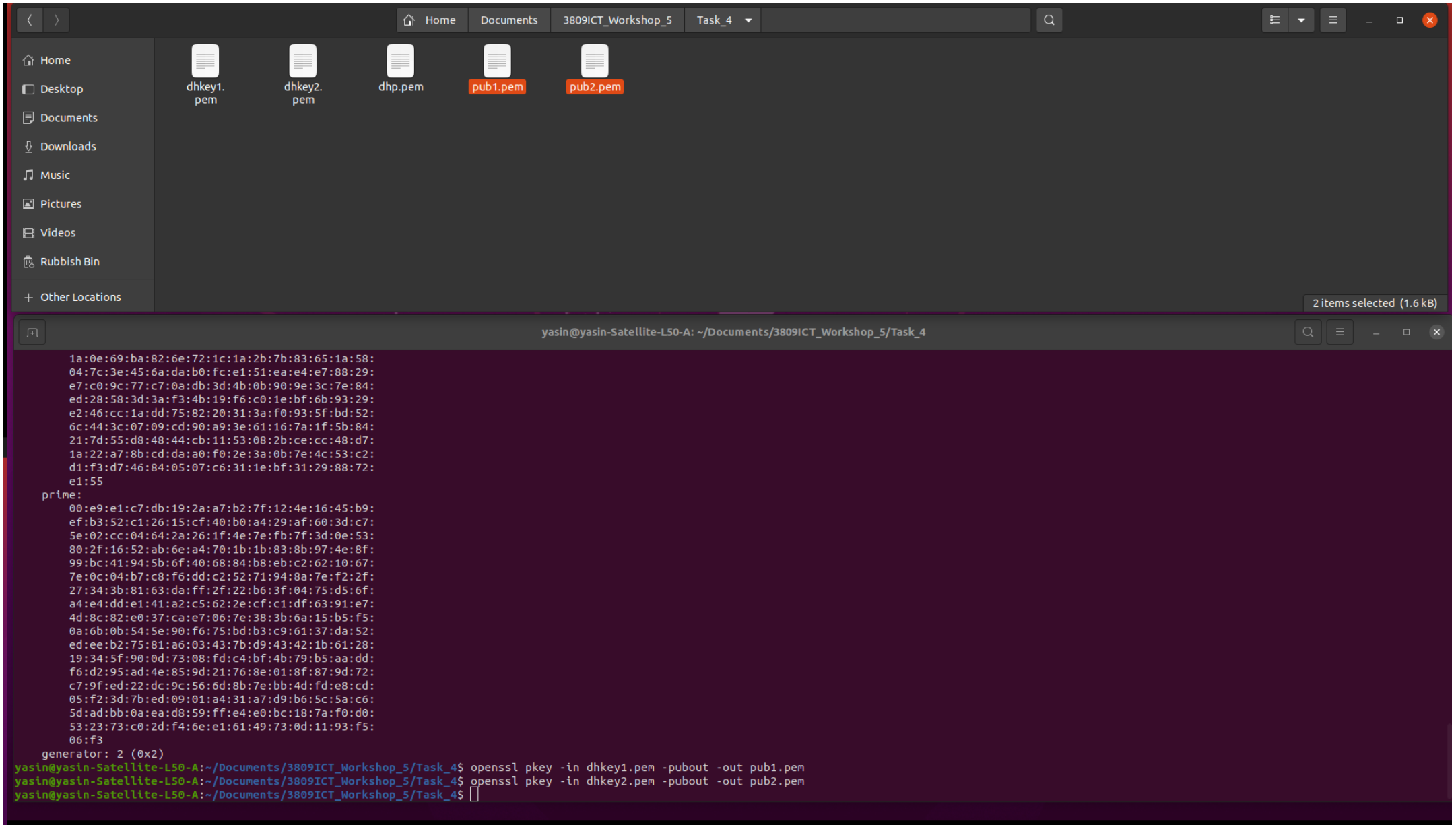
   and sends it through to user 2. Even an attacker captures pub1.pem, she won't be able to figure out dhkey1.pem as she needs to solve discrete logarithm problem, which is known to be computationally infeasible. User 2 does:

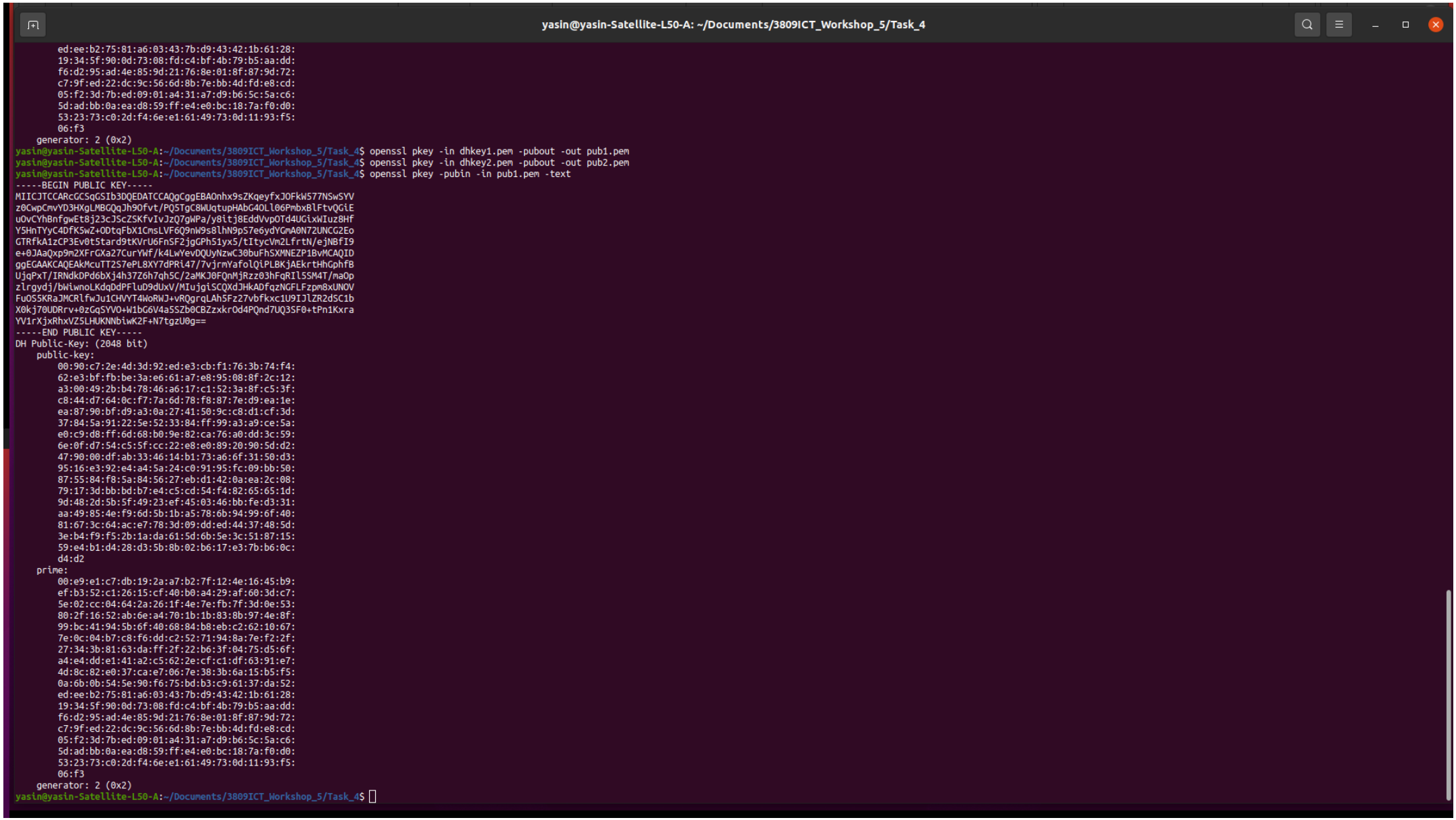
   ```
   $ openssl pkey -in dhkey2.pem -pubout -out pub2.pem
   ```

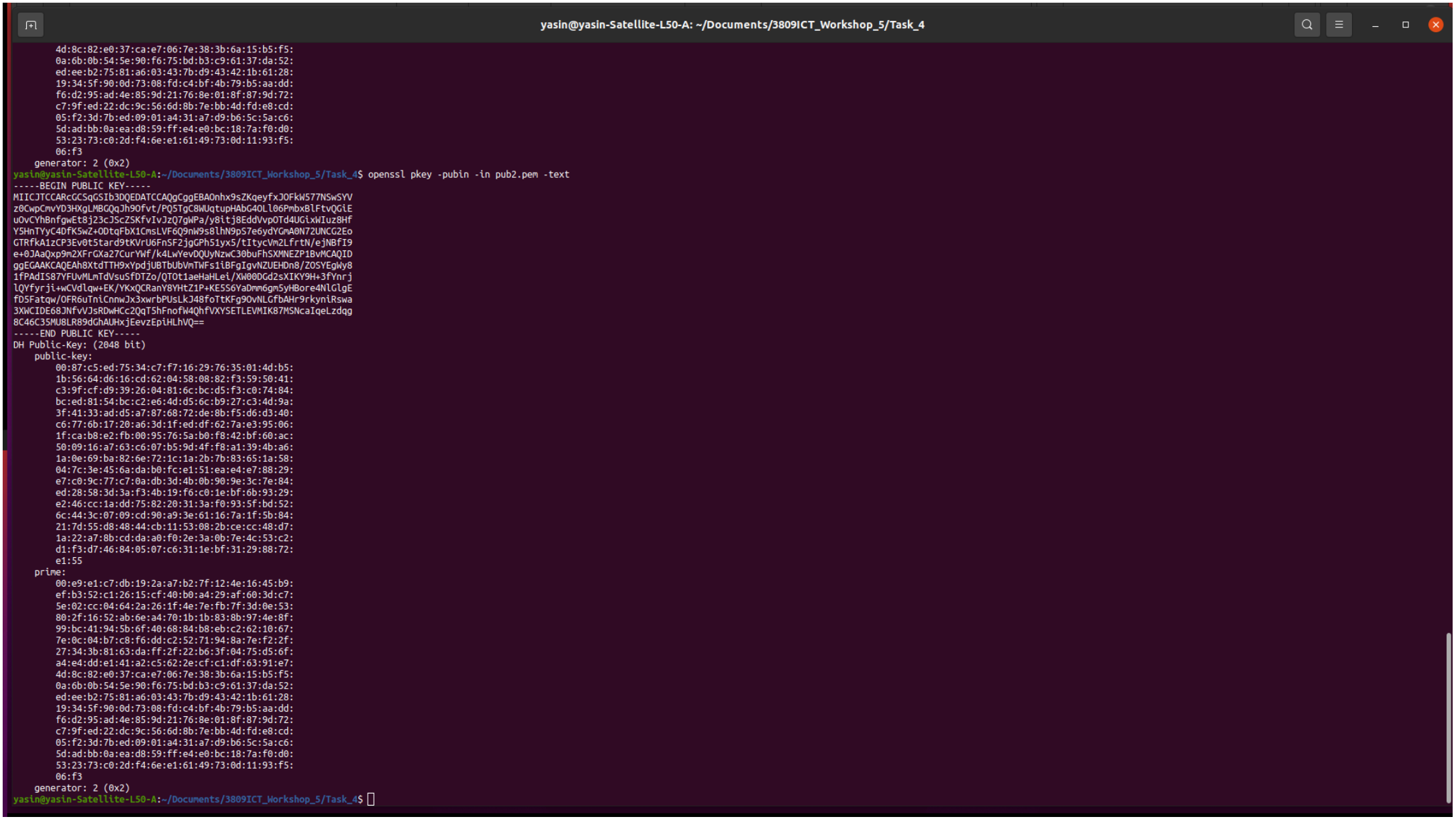
   and again, pub2.pem is not much useful in finding the private key. We can display them by the commands:

   $ openssl pkey -pubin -in pub1.pem -text
   $ openssl pkey -pubin -in pub2.pem -text

   Answer:


Home
Documents
3809ICT_Workshop_5
Task_4
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
dhkey1.pem
dhkey2.pem
dhp.pem
pub1.pem
pub2.pem
2 items selected (1.6 kB)
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_4
1a:0e:69:ba:82:6e:72:1c:1a:2b:7b:83:65:1a:58:
04:7c:3e:45:6a:da:b0:fc:e1:51:ea:e4:e7:88:29:
e7:c0:9c:77:c7:0a:db:3d:4b:0b:90:9e:3c:7e:84:
ed:28:58:3d:3a:f3:4b:19:f6:c0:1e:bf:6b:93:29:
e2:46:cc:1a:dd:75:82:20:31:3a:f0:93:5f:bd:52:
6c:44:3c:07:09:cd:90:a9:3e:61:16:7a:1f:5b:84:
21:7d:55:d8:48:44:cb:11:53:08:2b:ce:cc:48:d7:
1a:22:a7:8b:cd:da:a0:f0:2e:3a:0b:7e:4c:53:c2:
d1:f3:d7:46:84:05:07:c6:31:1e:bf:31:29:88:72:
e1:55
prime:
00:e9:e1:c7:db:19:2a:a7:b2:7f:12:4e:16:45:b9:
ef:b3:52:c1:26:15:cf:40:b0:a4:29:af:60:3d:c7:
5e:02:cc:04:64:2a:26:1f:4e:7e:fb:7f:3d:0e:53:
80:2f:16:52:ab:6e:a4:70:1b:1b:83:8b:97:4e:8f:
99:bc:41:94:5b:6f:40:68:84:b8:eb:c2:62:10:67:
7e:0c:04:b7:c8:f6:dd:c2:52:71:94:8a:7e:f2:2f:
27:34:3b:81:63:da:ff:2f:22:b6:3f:04:75:d5:6f:
a4:e4:dd:e1:41:a2:c5:62:2e:cf:c1:df:63:91:e7:
4d:8c:82:e0:37:ca:e7:06:7e:38:3b:6a:15:b5:f5:
0a:6b:0b:54:5e:90:f6:75:bd:b3:c9:61:37:da:52:
ed:ee:b2:75:81:a6:03:43:7b:d9:43:42:1b:61:28:
19:34:5f:90:0d:73:08:fd:c4:bf:4b:79:b5:aa:dd:
f6:d2:95:ad:4e:85:9d:21:76:8e:01:8f:87:9d:72:
c7:9f:ed:22:dc:9c:56:6d:8b:7e:bb:4d:fd:e8:cd:
05:f2:3d:7b:ed:09:01:a4:31:a7:d9:b6:5c:5a:c6:
5d:ad:bb:0a:ea:d8:59:ff:e4:e0:bc:18:7a:f0:d0:
53:23:73:c0:2d:f4:6e:e1:61:49:73:0d:11:93:f5:
06:f3
generator: 2 (0x2)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl pkey -in dhkey1.pem -pubout -out pub1.pem
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl pkey -in dhkey2.pem -pubout -out pub2.pem
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_4
ed:ee:b2:75:81:a6:03:43:7b:d9:43:42:1b:61:28:
19:34:5f:90:0d:73:08:fd:c4:bf:4b:79:b5:aa:dd:
f6:d2:95:ad:4e:85:9d:21:76:8e:01:8f:87:9d:72:
c7:9f:ed:22:dc:9c:56:6d:8b:7e:bb:4d:fd:e8:cd:
05:f2:3d:7b:ed:09:01:a4:31:a7:d9:b6:5c:5a:c6:
5d:ad:bb:0a:ea:d8:59:ff:e4:e0:bc:18:7a:f0:d0:
53:23:73:c0:2d:f4:6e:e1:61:49:73:0d:11:93:f5:
06:f3
generator: 2 (0x2)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl pkey -in dhkey1.pem -pubout -out pub1.pem
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl pkey -in dhkey2.pem -pubout -out pub2.pem
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl pkey -pubin -in pub1.pem -text
-----BEGIN PUBLIC KEY-----
MIICJTCCARcGCSqGSIb3DQEDATCCAQgCggEBAOnhx9sZKqeyfxJOFkW577NSwSYV
z0CwpCmvYD3HXgLMBGQqJh9Ofvt/PQ5TgC8WUqtupHAbG4OLl06PmbxBlFtvQGiE
uOvCYhBnfgwEt8j23cJScZSKfvIvJzQ7gWPa/y8itj8EddVvpOTd4UGixWIuz8Hf
Y5HnTYyC4DfK5wZ+ODtqFbX1CmsLVF6Q9nW9s8lhN9pS7e6ydYGmA0N72UNCG2Eo
GTRfkA1zCP3Ev0t5tard9tKVrU6FnSF2jgGPh51yx5/tItycVm2LfrtN/ejNBfI9
e+0JAaQxp9m2XFrGXa27CurYWf/k4LwYevDQUyNzwC30buFhSXMNEZP1BvMCAQID
ggEGAAKCAQEAkMcuTT2S7ePL8XY7dPRi47/7vjrmYafolQiPLBKjAEkrtHhGphfB
UjqPxT/IRNdkDPd6bXj4h37Z6h7qh5C/2aMKJ0FQnMjRzz03hFqRIl5SM4T/maOp
zlrgydj/bWiwnoLKdqDdPFluD9dUxV/MIujgiSCQXdJHkADfqzNGFLFzpm8xUNOV
FuOS5KRaJMCRlfwJu1CHVYT4WoRWJ+vRQgrqLAh5Fz27vbfkxc1U9IJlZR2dSC1b
X0kj70UDRrv+0zGqSYVO+W1bG6V4a5SZb0CBZzxkrOd4PQnd7UQ3SF0+tPn1Kxra
YV1rXjxRhxVZ5LHUKNNbiwK2F+N7tgzU0g==
-----END PUBLIC KEY-----
DH Public-Key: (2048 bit)
public-key:
00:90:c7:2e:4d:3d:92:ed:e3:cb:f1:76:3b:74:f4:
62:e3:bf:fb:be:3a:e6:61:a7:e8:95:08:8f:2c:12:
a3:00:49:2b:b4:78:46:a6:17:c1:52:3a:8f:c5:3f:
c8:44:d7:64:0c:f7:7a:6d:78:f8:87:7e:d9:ea:1e:
ea:87:90:bf:d9:a3:0a:27:41:50:9c:c8:d1:cf:3d:
37:84:5a:91:22:5e:52:33:84:ff:99:a3:a9:ce:5a:
e0:c9:d8:ff:6d:68:b0:9e:82:ca:76:a0:dd:3c:59:
6e:0f:d7:54:c5:5f:cc:22:e8:e0:89:20:90:5d:d2:
47:90:00:df:ab:33:46:14:b1:73:a6:6f:31:50:d3:
95:16:e3:92:e4:a4:5a:24:c0:91:95:fc:09:bb:50:
87:55:84:f8:5a:84:56:27:eb:d1:42:0a:ea:2c:08:
79:17:3d:bb:bd:b7:e4:c5:cd:54:f4:82:65:65:1d:
9d:48:2d:5b:5f:49:23:ef:45:03:46:bb:fe:d3:31:
aa:49:85:4e:f9:6d:5b:1b:a5:78:6b:94:99:6f:40:
81:67:3c:64:ac:e7:78:3d:09:dd:ed:44:37:48:5d:
3e:b4:f9:f5:2b:1a:da:61:5d:6b:5e:3c:51:87:15:
59:e4:b1:d4:28:d3:5b:8b:02:b6:17:e3:7b:b6:0c:
d4:d2
prime:
00:e9:e1:c7:db:19:2a:a7:b2:7f:12:4e:16:45:b9:
ef:b3:52:c1:26:15:cf:40:b0:a4:29:af:60:3d:c7:
5e:02:cc:04:64:2a:26:1f:4e:7e:fb:7f:3d:0e:53:
80:2f:16:52:ab:6e:a4:70:1b:1b:83:8b:97:4e:8f:
99:bc:41:94:5b:6f:40:68:84:b8:eb:c2:62:10:67:
7e:0c:04:b7:c8:f6:dd:c2:52:71:94:8a:7e:f2:2f:
27:34:3b:81:63:da:ff:2f:22:b6:3f:04:75:d5:6f:
a4:e4:dd:e1:41:a2:c5:62:2e:cf:c1:df:63:91:e7:
4d:8c:82:e0:37:ca:e7:06:7e:38:3b:6a:15:b5:f5:
0a:6b:0b:54:5e:90:f6:75:bd:b3:c9:61:37:da:52:
ed:ee:b2:75:81:a6:03:43:7b:d9:43:42:1b:61:28:
19:34:5f:90:0d:73:08:fd:c4:bf:4b:79:b5:aa:dd:
f6:d2:95:ad:4e:85:9d:21:76:8e:01:8f:87:9d:72:
c7:9f:ed:22:dc:9c:56:6d:8b:7e:bb:4d:fd:e8:cd:
05:f2:3d:7b:ed:09:01:a4:31:a7:d9:b6:5c:5a:c6:
5d:ad:bb:0a:ea:d8:59:ff:e4:e0:bc:18:7a:f0:d0:
53:23:73:c0:2d:f4:6e:e1:61:49:73:0d:11:93:f5:
06:f3
generator: 2 (0x2)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_4
4d:8c:82:e0:37:ca:e7:06:7e:38:3b:6a:15:b5:f5:
0a:6b:0b:54:5e:90:f6:75:bd:b3:c9:61:37:da:52:
ed:ee:b2:75:81:a6:03:43:7b:d9:43:42:1b:61:28:
19:34:5f:90:0d:73:08:fd:c4:bf:4b:79:b5:aa:dd:
f6:d2:95:ad:4e:85:9d:21:76:8e:01:8f:87:9d:72:
c7:9f:ed:22:dc:9c:56:6d:8b:7e:bb:4d:fd:e8:cd:
05:f2:3d:7b:ed:09:01:a4:31:a7:d9:b6:5c:5a:c6:
5d:ad:bb:0a:ea:d8:59:ff:e4:e0:bc:18:7a:f0:d0:
53:23:73:c0:2d:f4:6e:e1:61:49:73:0d:11:93:f5:
06:f3
generator: 2 (0x2)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl pkey -pubin -in pub2.pem -text
-----BEGIN PUBLIC KEY-----
MIICJTCCARcGCSqGSIb3DQEDATCCAQgCggEBAOnhx9sZKqeyfxJOFkW577NSwSYV
z0CwpCmvYD3HXgLMBGQqJh9Ofvt/PQ5TgC8WUqtupHAbG4OLl06PmbxBlFtvQGiE
uOvCYhBnfgwEt8j23cJScZSKfvIvJzQ7gWPa/y8itj8EddVvpOTd4UGixWIuz8Hf
Y5HnTYyC4DfK5wZ+ODtqFbX1CmsLVF6Q9nW9s8lhN9pS7e6ydYGmA0N72UNCG2Eo
GTRfkA1zCP3Ev0t5tard9tKVrU6FnSF2jgGPh51yx5/tItycVm2LfrtN/ejNBfI9
e+0JAaQxp9m2XFrGXa27CurYWf/k4LwYevDQUyNzwC30buFhSXMNEZP1BvMCAQID
ggEGAAKCAQEAh8XtdTTH9xYpdjUBTbUbVmTWFs1iBFgIgvNZUEHDn8/ZOSYEgWy8
1fPAdIS87YFUvMLmTdVsuSfDTZo/QTOt1aeHaHLei/XW00DGd2sXIKY9H+3fYnrj
lQYfyrji+wCVdlqw+EK/YKxQCRanY8YHtZ1P+KE556YaDmm6gm5yHBore4NlGlgE
fD5Fatqw/OFR6uTniCnnwJx3xwrbPUsLkJ48foTtKFg9OvNLGfbAHr9rkyniRswa
3XWCIDE68JNfvVJsRDwHCc2QqT5hFnofW4QhfVXYSETLEVMIK87MSNcaIqeLzdqg
8C46C35MU8LR89dGhAUHxjEevzEpiHLhVQ==
-----END PUBLIC KEY-----
DH Public-Key: (2048 bit)
public-key:
00:87:c5:ed:75:34:c7:f7:16:29:76:35:01:4d:b5:
1b:56:64:d6:16:cd:62:04:58:08:82:f3:59:50:41:
c3:9f:cf:d9:39:26:04:81:6c:bc:d5:f3:c0:74:84:
bc:ed:81:54:bc:c2:e6:4d:d5:6c:b9:27:c3:4d:9a:
3f:41:33:ad:d5:a7:87:68:72:de:8b:f5:d6:d3:40:
c6:77:6b:17:20:a6:3d:1f:ed:df:62:7a:e3:95:06:
1f:ca:b8:e2:fb:00:95:76:5a:b0:f8:42:bf:60:ac:
50:09:16:a7:63:c6:07:b5:9d:4f:f8:a1:39:4b:a6:
1a:0e:69:ba:82:6e:72:1c:1a:2b:7b:83:65:1a:58:
04:7c:3e:45:6a:da:b0:fc:e1:51:ea:e4:e7:88:29:
e7:c0:9c:77:c7:0a:db:3d:4b:0b:90:9e:3c:7e:84:
ed:28:58:3d:3a:f3:4b:19:f6:c0:1e:bf:6b:93:29:
e2:46:cc:1a:dd:75:82:20:31:3a:f0:93:5f:bd:52:
6c:44:3c:07:09:cd:90:a9:3e:61:16:7a:1f:5b:84:
21:7d:55:d8:48:44:cb:11:53:08:2b:ce:cc:48:d7:
1a:22:a7:8b:cd:da:a0:f0:2e:3a:0b:7e:4c:53:c2:
d1:f3:d7:46:84:05:07:c6:31:1e:bf:31:29:88:72:
e1:55
prime:
00:e9:e1:c7:db:19:2a:a7:b2:7f:12:4e:16:45:b9:
ef:b3:52:c1:26:15:cf:40:b0:a4:29:af:60:3d:c7:
5e:02:cc:04:64:2a:26:1f:4e:7e:fb:7f:3d:0e:53:
80:2f:16:52:ab:6e:a4:70:1b:1b:83:8b:97:4e:8f:
99:bc:41:94:5b:6f:40:68:84:b8:eb:c2:62:10:67:
7e:0c:04:b7:c8:f6:dd:c2:52:71:94:8a:7e:f2:2f:
27:34:3b:81:63:da:ff:2f:22:b6:3f:04:75:d5:6f:
a4:e4:dd:e1:41:a2:c5:62:2e:cf:c1:df:63:91:e7:
4d:8c:82:e0:37:ca:e7:06:7e:38:3b:6a:15:b5:f5:
0a:6b:0b:54:5e:90:f6:75:bd:b3:c9:61:37:da:52:
ed:ee:b2:75:81:a6:03:43:7b:d9:43:42:1b:61:28:
19:34:5f:90:0d:73:08:fd:c4:bf:4b:79:b5:aa:dd:
f6:d2:95:ad:4e:85:9d:21:76:8e:01:8f:87:9d:72:
c7:9f:ed:22:dc:9c:56:6d:8b:7e:bb:4d:fd:e8:cd:
05:f2:3d:7b:ed:09:01:a4:31:a7:d9:b6:5c:5a:c6:
5d:ad:bb:0a:ea:d8:59:ff:e4:e0:bc:18:7a:f0:d0:
53:23:73:c0:2d:f4:6e:e1:61:49:73:0d:11:93:f5:
06:f3
generator: 2 (0x2)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$

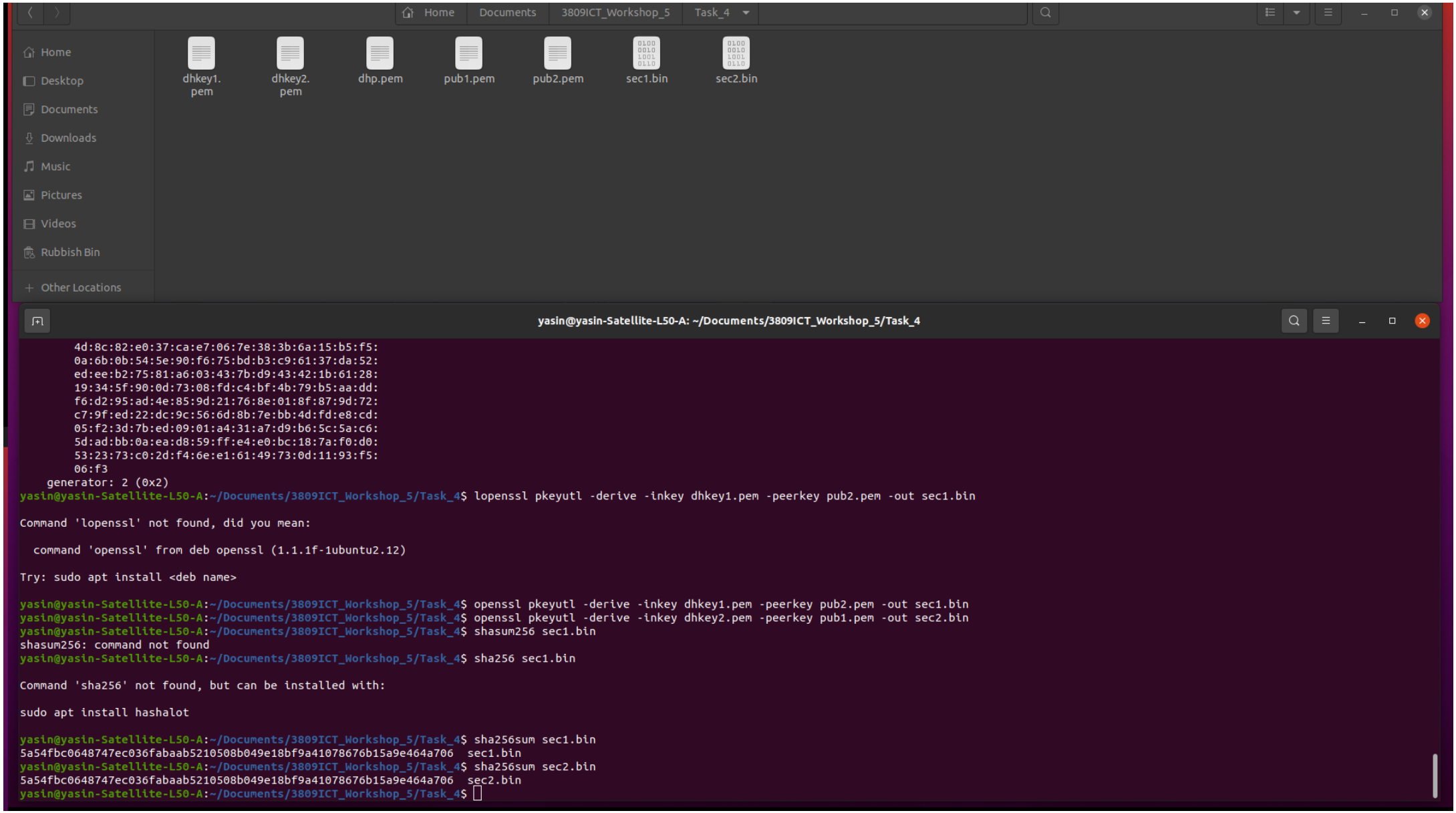
5. Deriving the shared key. User 1 obtains user 2's public key pub2.pem and runs the following command to generate a secret key sec1.bin:

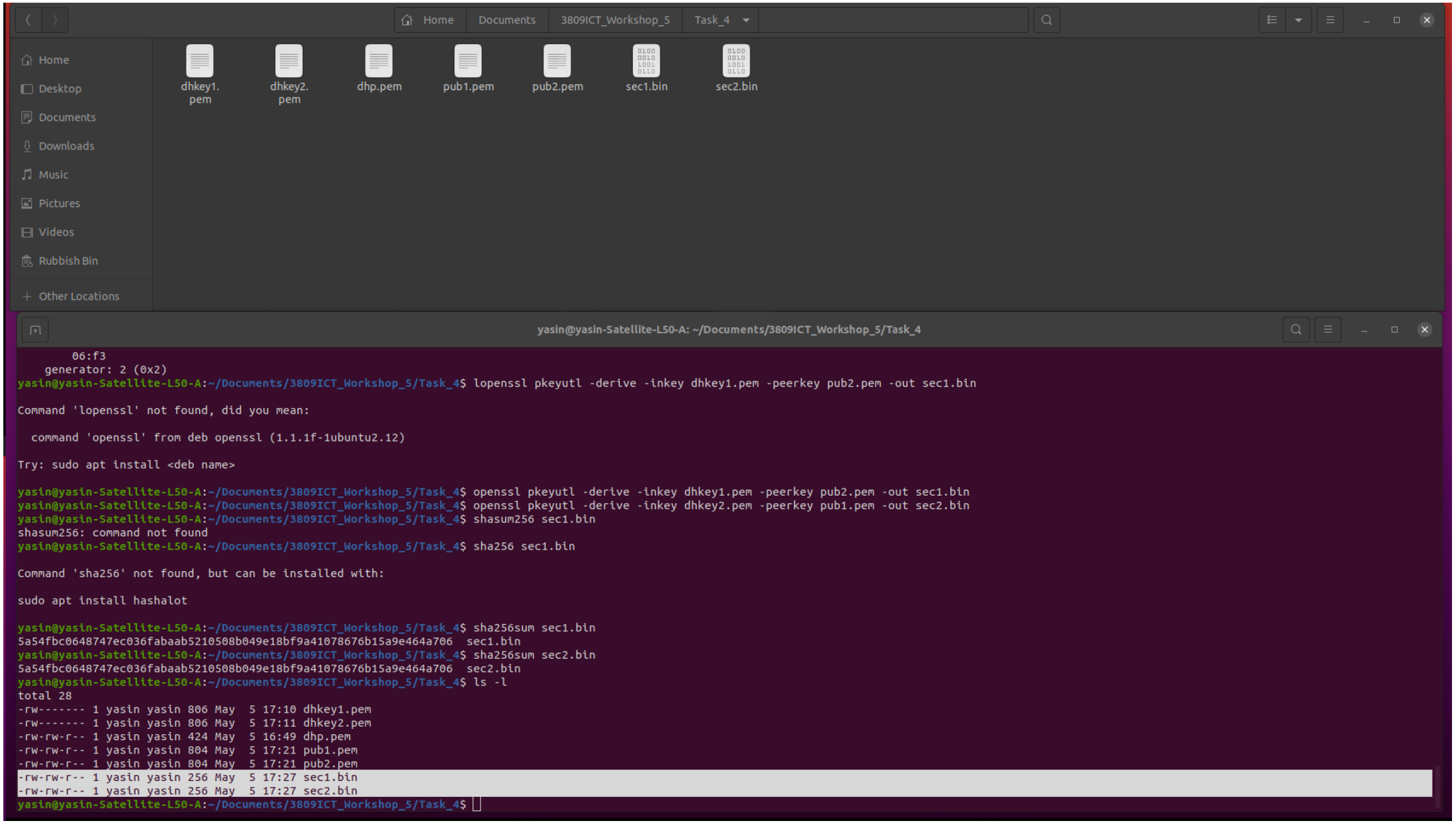
   $ openssl pkeyutl -derive -inkey dhkey1.pem -peerkey pub2.pem -out sec1.bin

   User 2 will run

   $ openssl pkeyutl -derive -inkey dhkey2.pem -peerkey pub1.pem -out sec2.bin

   Answer:


Home
Documents
3809ICT_Workshop_5
Task_4
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
dhkey1.pem
dhkey2.pem
dhp.pem
pub1.pem
pub2.pem
sec1.bin
sec2.bin
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_4
4d:8c:82:e0:37:ca:e7:06:7e:38:3b:6a:15:b5:f5:
0a:6b:0b:54:5e:90:f6:75:bd:b3:c9:61:37:da:52:
ed:ee:b2:75:81:a6:03:43:7b:d9:43:42:1b:61:28:
19:34:5f:90:0d:73:08:fd:c4:bf:4b:79:b5:aa:dd:
f6:d2:95:ad:4e:85:9d:21:76:8e:01:8f:87:9d:72:
c7:9f:ed:22:dc:9c:56:6d:8b:7e:bb:4d:fd:e8:cd:
05:f2:3d:7b:ed:09:01:a4:31:a7:d9:b6:5c:5a:c6:
5d:ad:bb:0a:ea:d8:59:ff:e4:e0:bc:18:7a:f0:d0:
53:23:73:c0:2d:f4:6e:e1:61:49:73:0d:11:93:f5:
06:f3
generator: 2 (0x2)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ lopenssl pkeyutl -derive -inkey dhkey1.pem -peerkey pub2.pem -out sec1.bin
Command 'lopenssl' not found, did you mean:
command 'openssl' from deb openssl (1.1.1f-1ubuntu2.12)
Try: sudo apt install <deb name>
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl pkeyutl -derive -inkey dhkey1.pem -peerkey pub2.pem -out sec1.bin
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl pkeyutl -derive -inkey dhkey2.pem -peerkey pub1.pem -out sec2.bin
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ shasum256 sec1.bin
shasum256: command not found
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ sha256 sec1.bin
Command 'sha256' not found, but can be installed with:
sudo apt install hashalot
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ sha256sum sec1.bin
5a54fbc0648747ec036fabaab5210508b049e18bf9a41078676b15a9e464a706 sec1.bin
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ sha256sum sec2.bin
5a54fbc0648747ec036fabaab5210508b049e18bf9a41078676b15a9e464a706 sec2.bin
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$


Home
Documents
3809ICT_Workshop_5
Task_4
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
dhkey1.pem
dhkey2.pem
dhp.pem
pub1.pem
pub2.pem
sec1.bin
sec2.bin
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_5/Task_4
06:f3
generator: 2 (0x2)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ lopenssl pkeyutl -derive -inkey dhkey1.pem -peerkey pub2.pem -out sec1.bin
Command 'lopenssl' not found, did you mean:
command 'openssl' from deb openssl (1.1.1f-1ubuntu2.12)
Try: sudo apt install <deb name>
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl pkeyutl -derive -inkey dhkey1.pem -peerkey pub2.pem -out sec1.bin
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ openssl pkeyutl -derive -inkey dhkey2.pem -peerkey pub1.pem -out sec2.bin
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ shasum256 sec1.bin
shasum256: command not found
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ sha256 sec1.bin
Command 'sha256' not found, but can be installed with:
sudo apt install hashalot
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ sha256sum sec1.bin
5a54fbc0648747ec036fabaab5210508b049e18bf9a41078676b15a9e464a706 sec1.bin
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ sha256sum sec2.bin
5a54fbc0648747ec036fabaab5210508b049e18bf9a41078676b15a9e464a706 sec2.bin
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$ ls -l
total 28
-rw------- 1 yasin yasin 806 May 5 17:10 dhkey1.pem
-rw------- 1 yasin yasin 806 May 5 17:11 dhkey2.pem
-rw-rw-r-- 1 yasin yasin 424 May 5 16:49 dhp.pem
-rw-rw-r-- 1 yasin yasin 804 May 5 17:21 pub1.pem
-rw-rw-r-- 1 yasin yasin 804 May 5 17:21 pub2.pem
-rw-rw-r-- 1 yasin yasin 256 May 5 17:27 sec1.bin
-rw-rw-r-- 1 yasin yasin 256 May 5 17:27 sec2.bin
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_5/Task_4$

Q: Can you check to see whether sec1.bin is identical to sec2.bin?

Answer:
The two files are exactly identical in value as they both produce the same hash digest with the SHA-256 algorithm

Q: What is the bit size of sec1.bin (and sec2.bin), why?

Answer:
The bit size of sec1.bin and sec2.bin are both 256bytes whish is equivalent to bits in size. This is because the size of the modulo, n, is 2048 bits in size.

Q: (Optional) The above implementation suffers from a man-in-the-middle (MIM) attack. Signed Diffie-Hellman Key Exchange protocol can prevent that. Can you use the commands from Task 2 and Task 4 to implement a signed Diffie-Hellman Key-Exchange protocol?

Acknowledgement: This lab instruction is partially based on the SEED labs from the SEED project led by Professor Wenliang Du, Syracuse University.