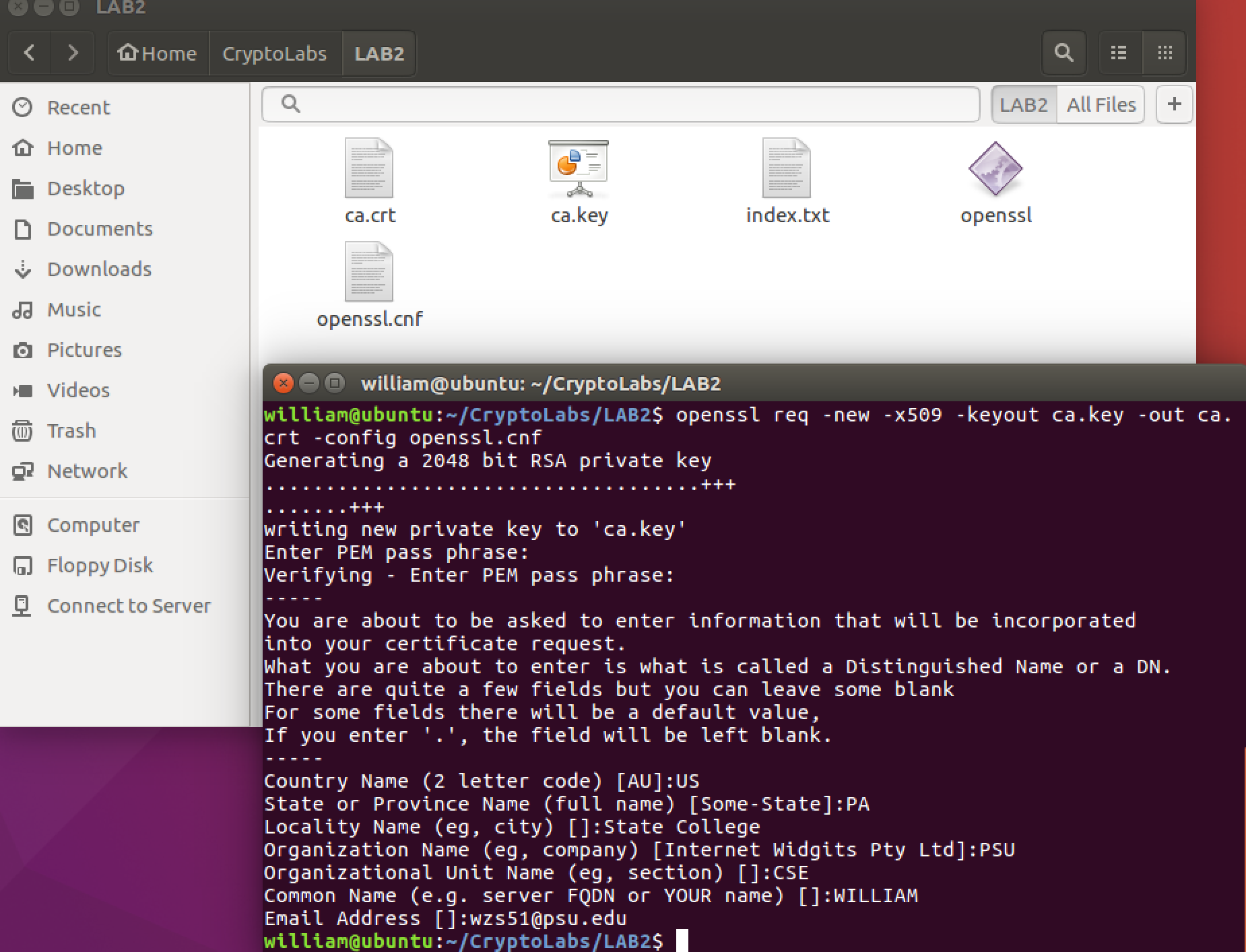
Crypto Lab – Public-Key Cryptography and PKI

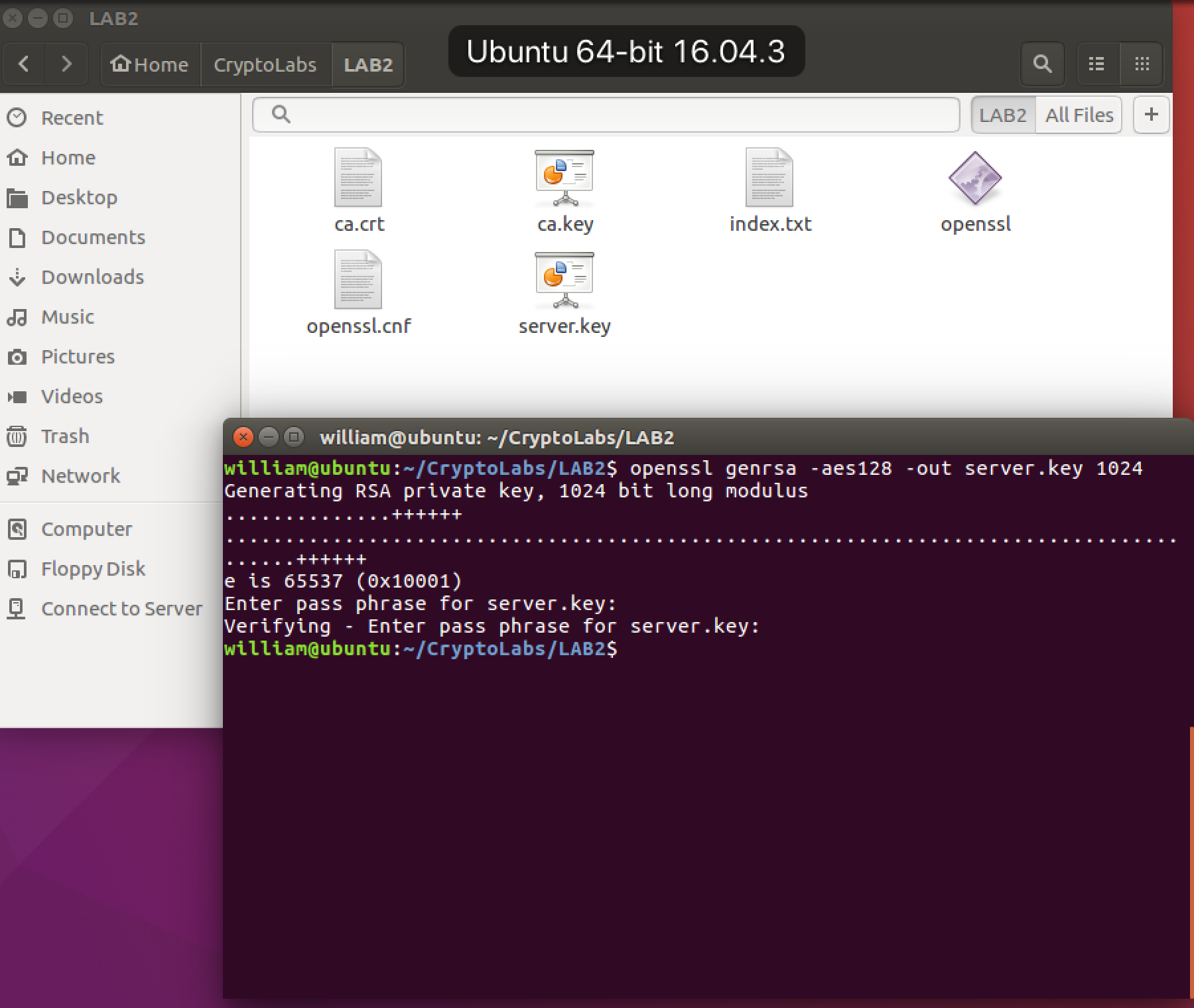
Task 1:

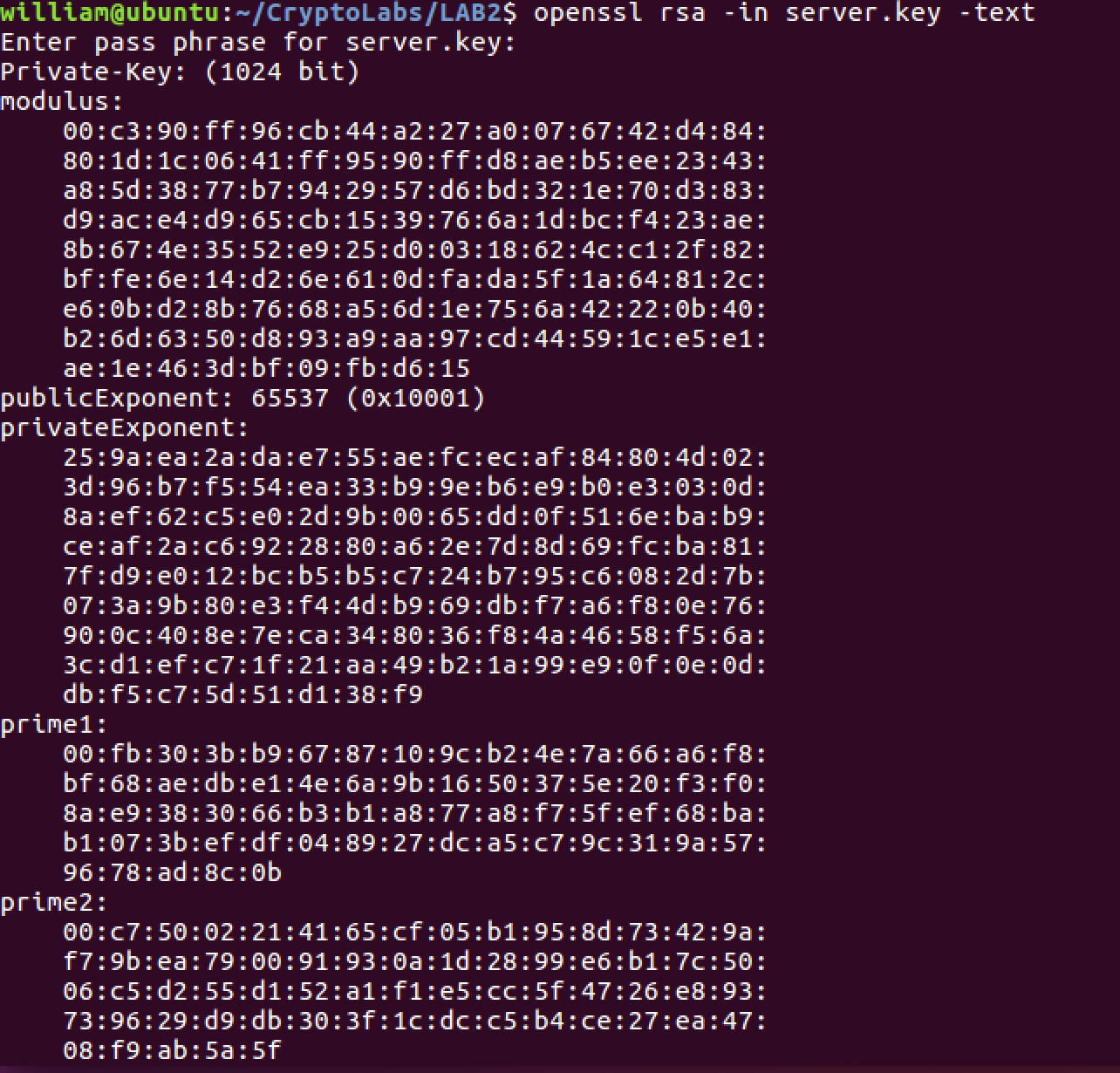


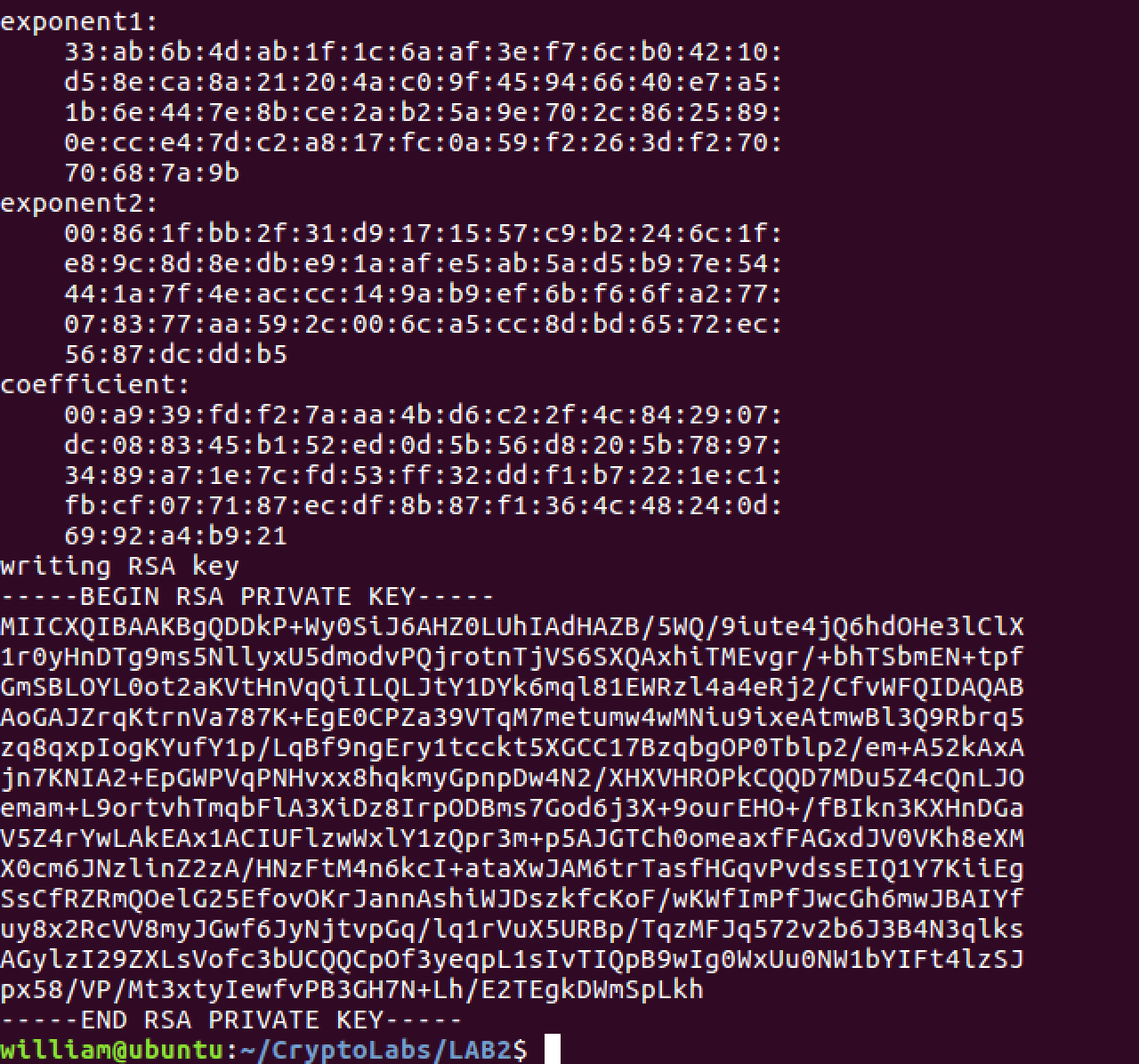
**Observation:**

Public key certificate (ca.crt) and CA’s private key (ca.key) is generated using the openssl and RSA command.

Task 2

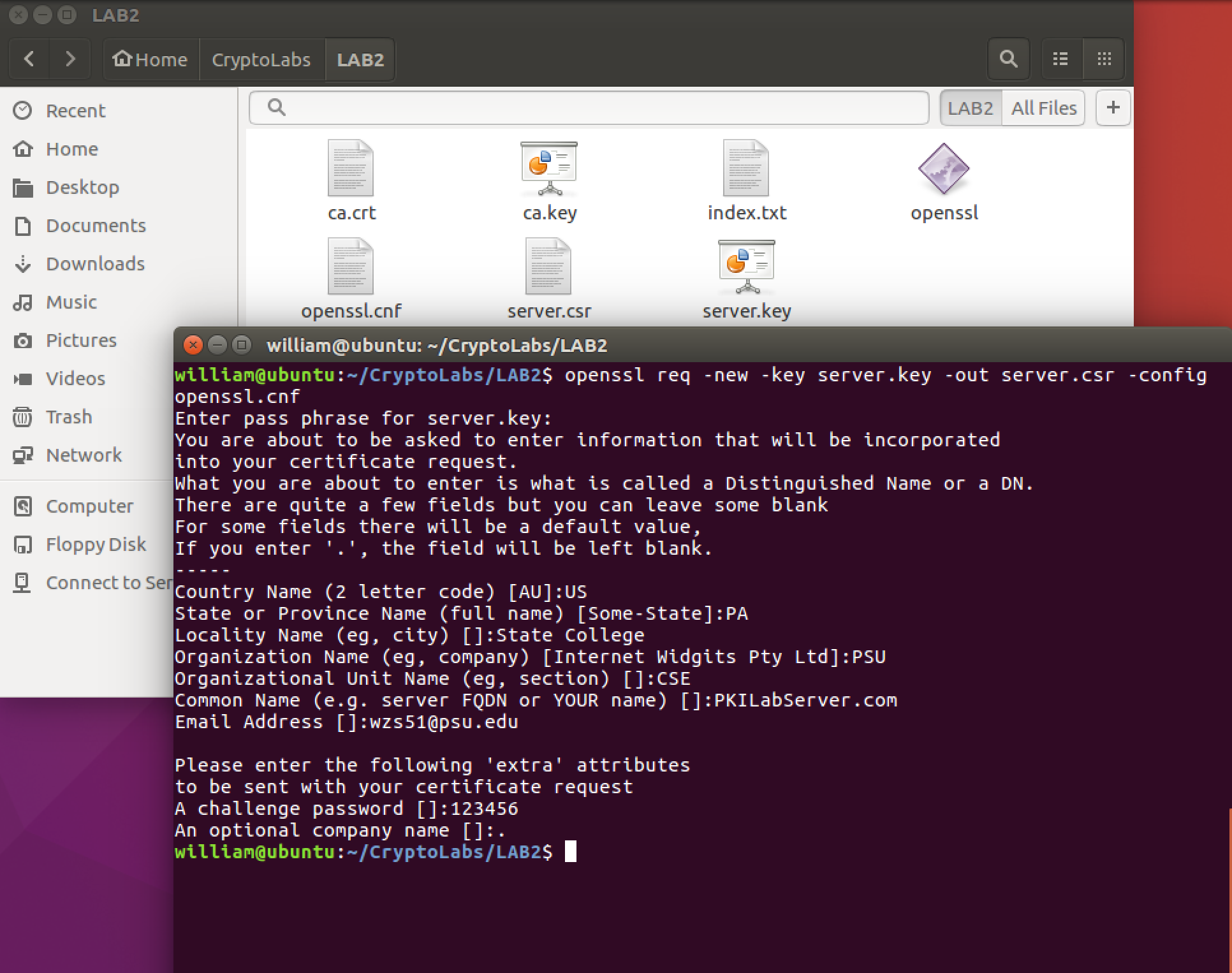
****





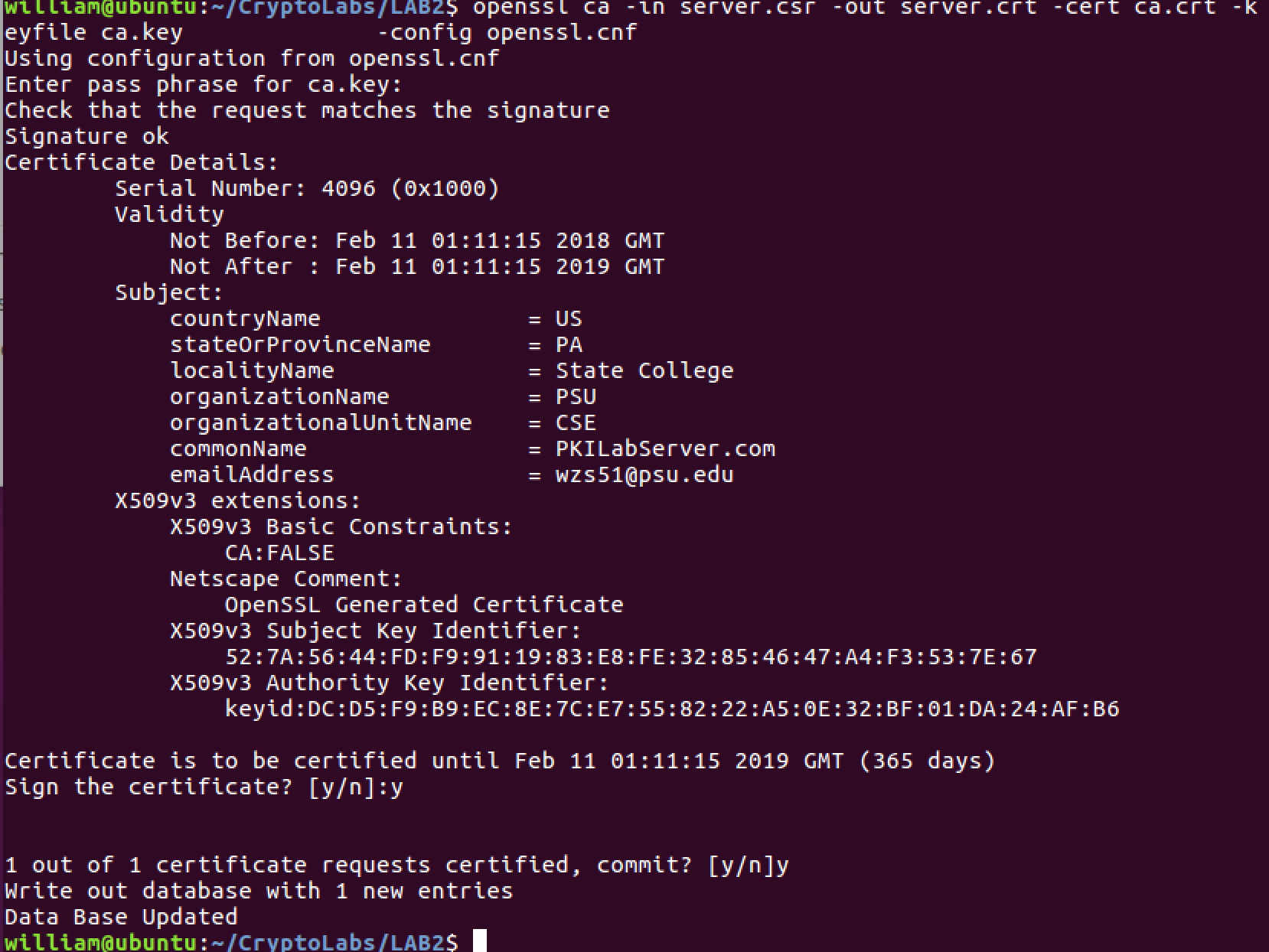
**Observation:**

A RSA key pair is generated using openssl and it is stored in server.key.



**Observation:**

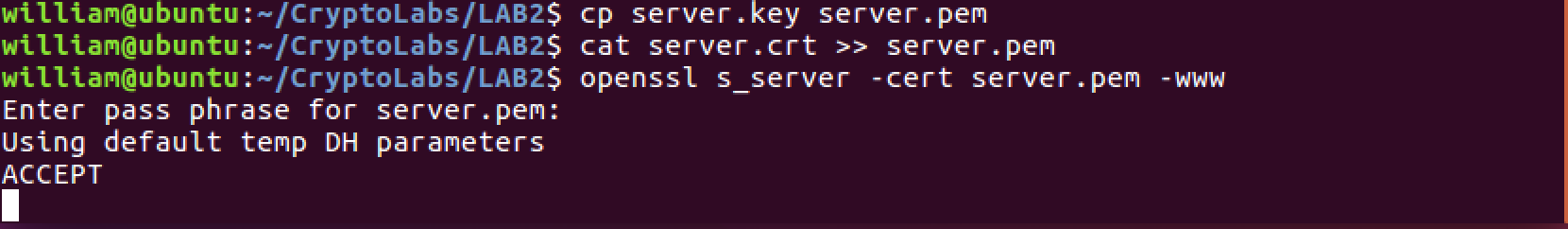
The Certificate Signing Request (CSR) is generated from server.key which is used to generate certificate for the key.



**Observation:**

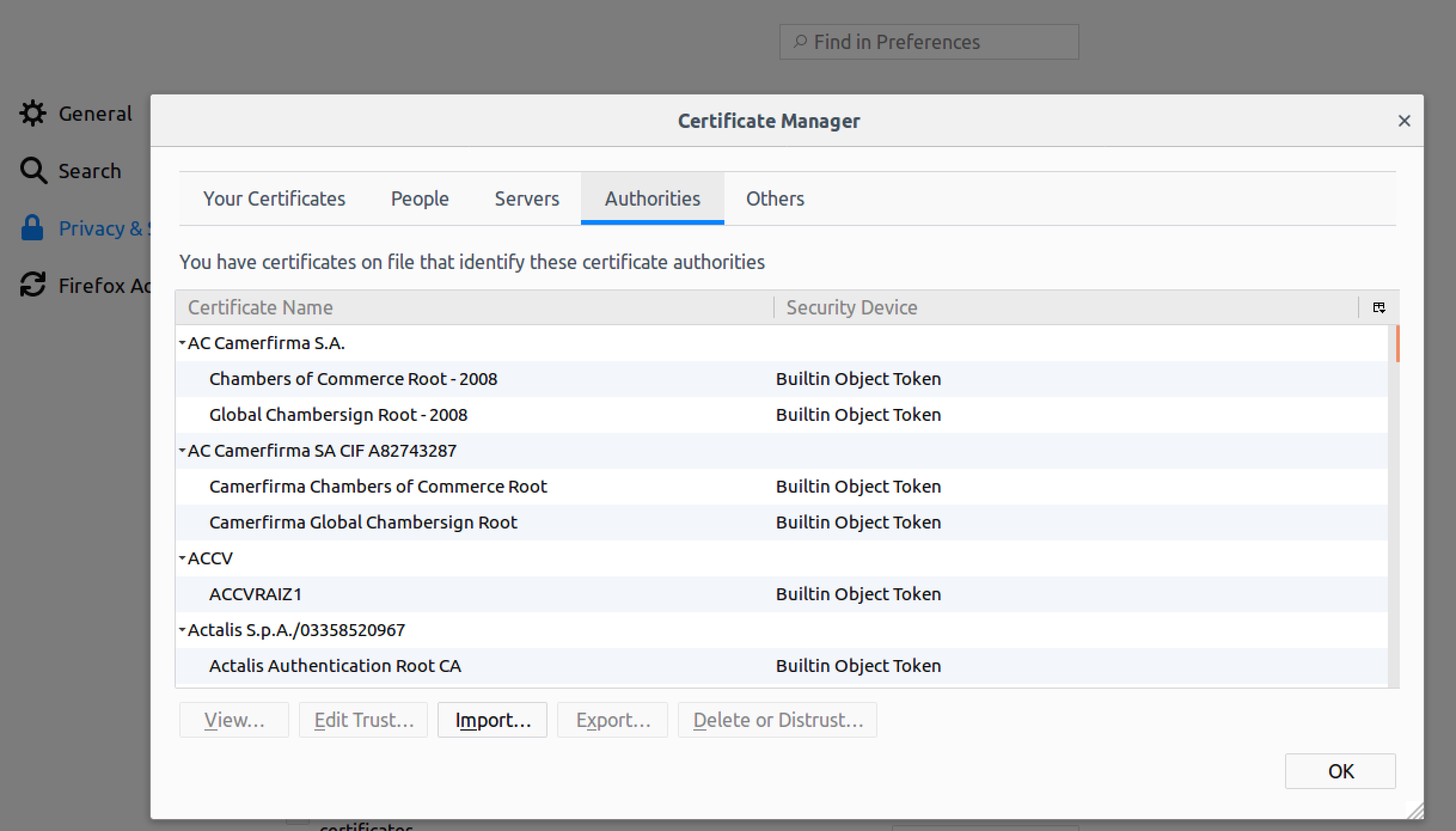
The CSR file is sent to the CA and it is signed using cs.crt and ca.key to generate server.crt certificate for PKILabServer.com

Task 3



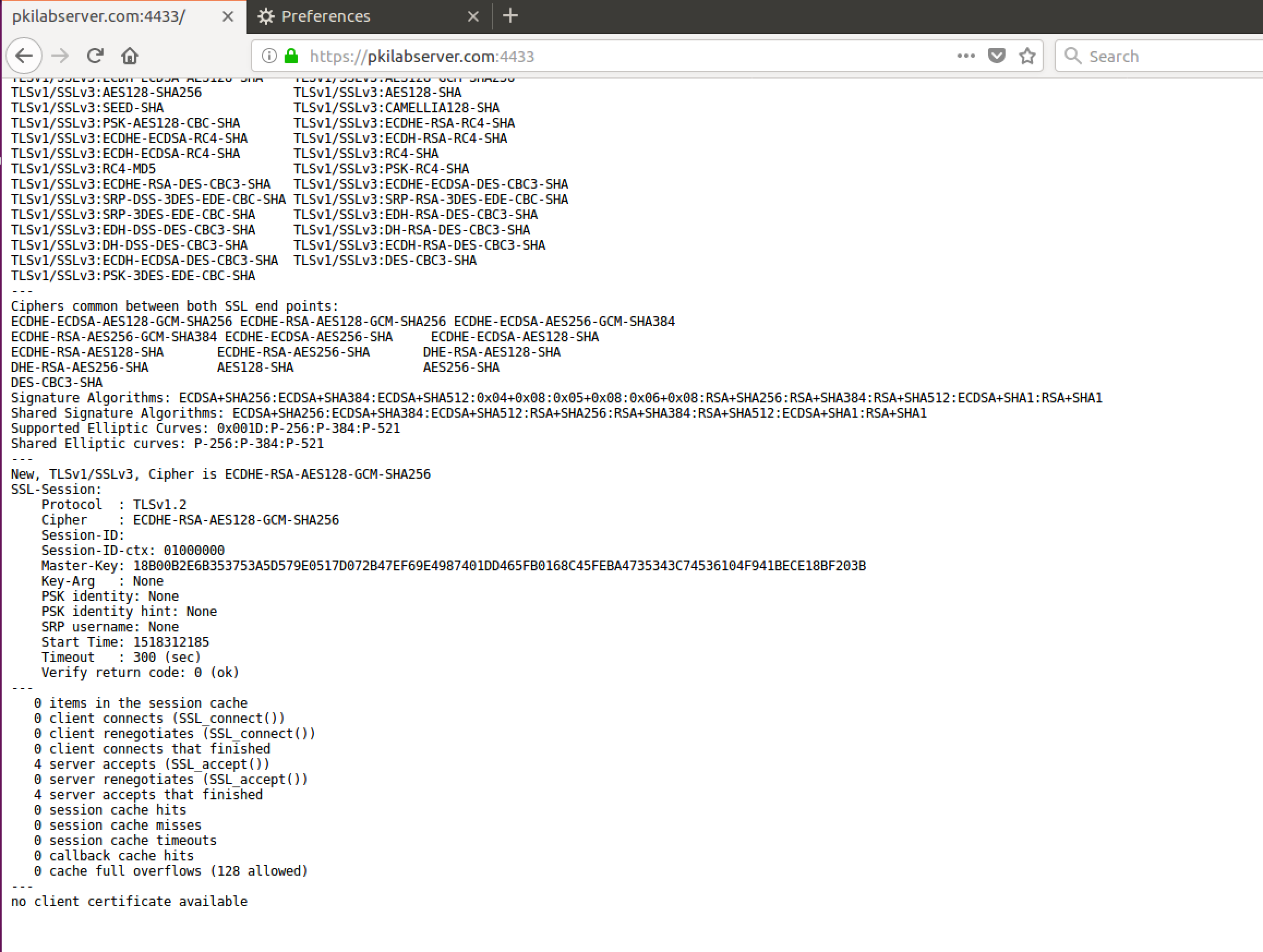
**Observation:**

After the server is mapped to local host it can be launched using server.pem which is formed by joining server.key and server.crt



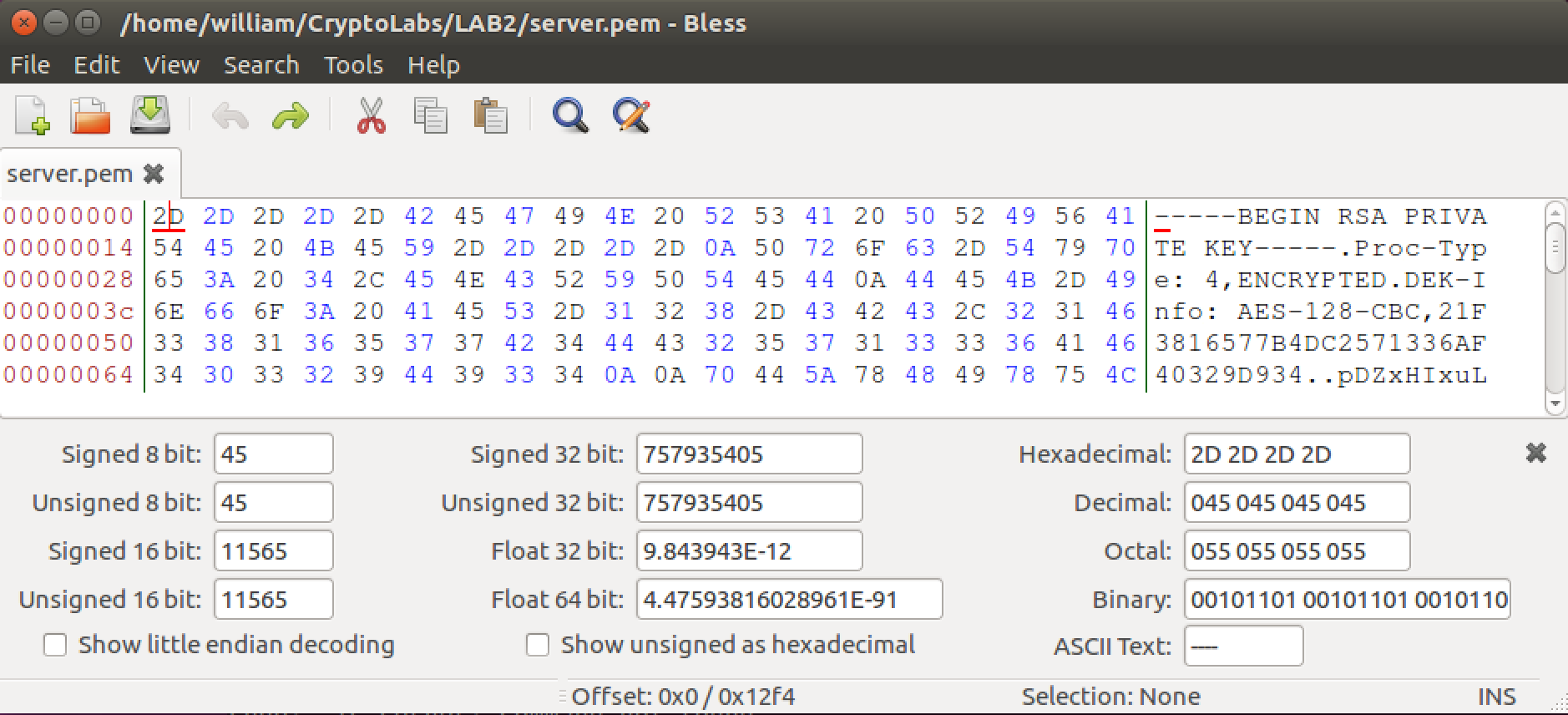
**Observation:**

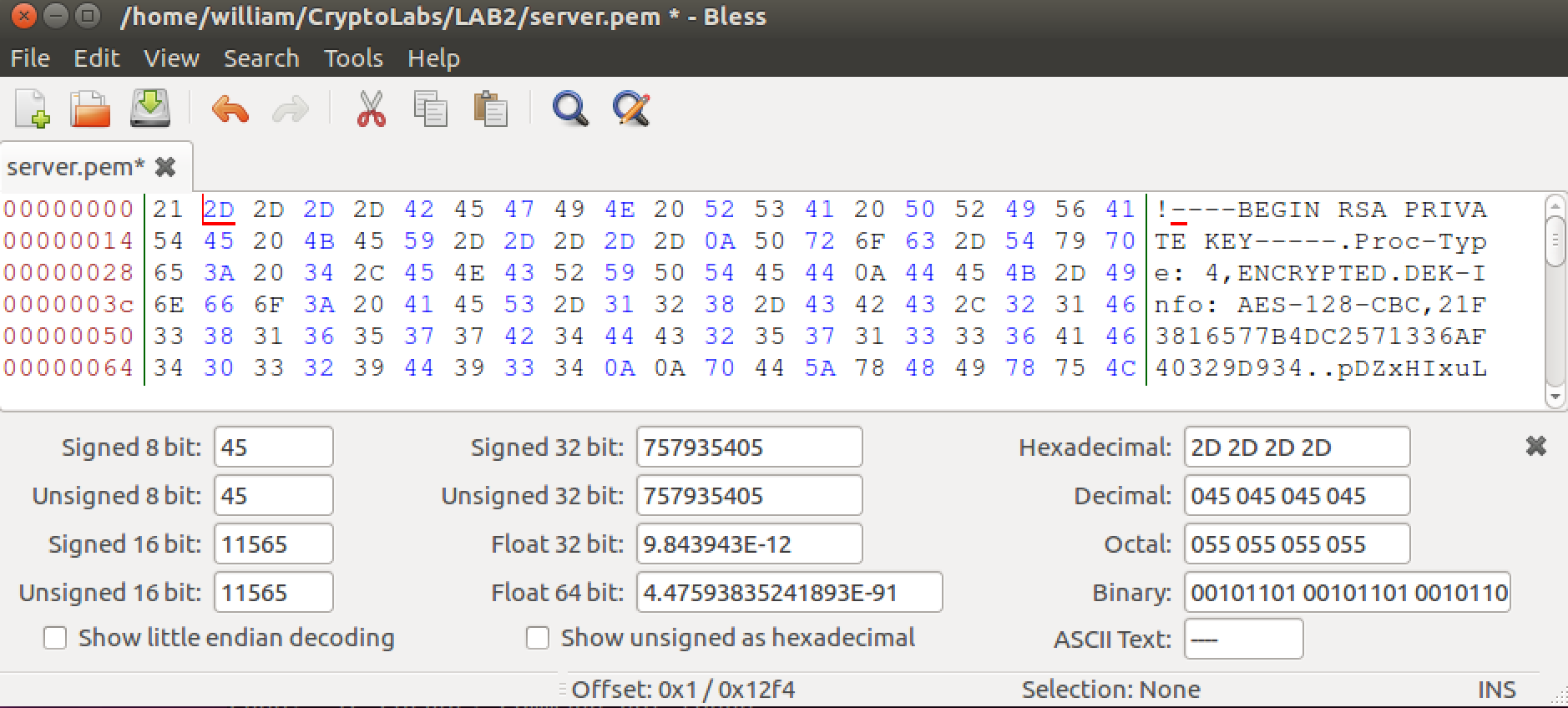
Before I imported the certificate into the browser, the access to the server using the url is not trusted by the web browser. So I manually imported the ca.crt into the web browser.



**Observation:**

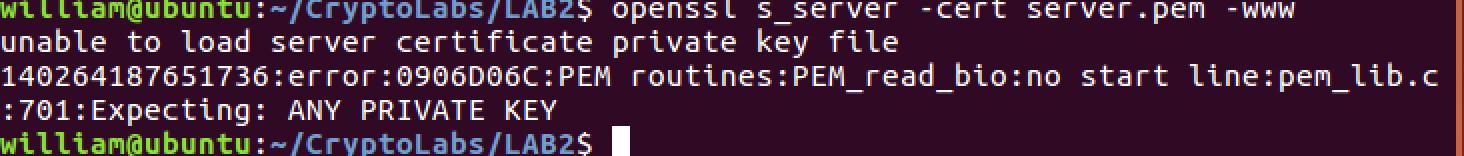
The url is agreed as trusted since it is certified by ca.crt



****

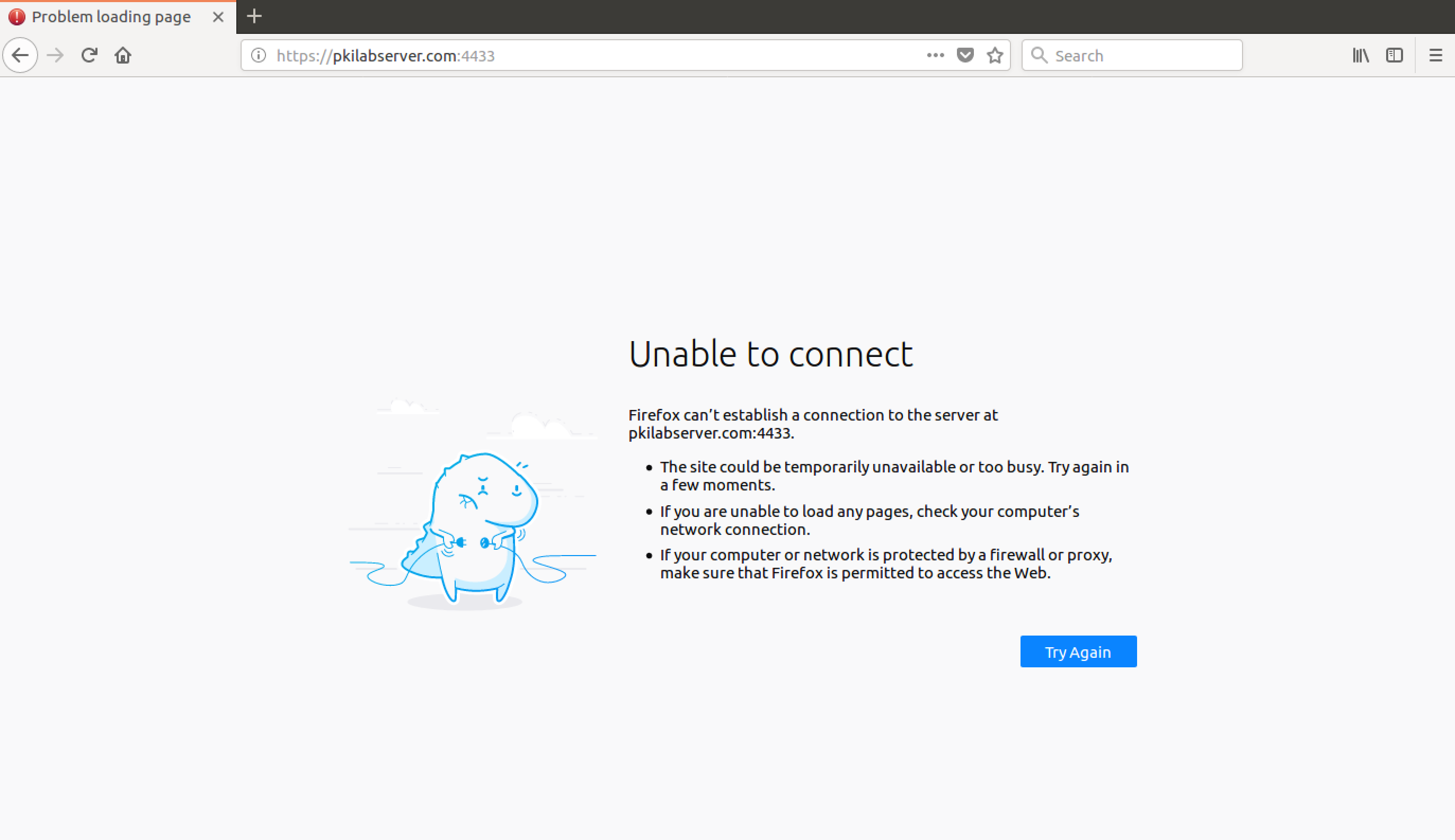
**Observation:**

As the instruction said, I changed the single byte from D to 1 in server.key.



**Observation:**

As the single byte in server.key part of the server.pem is changed, the terminal cannot load the server certificate key file.

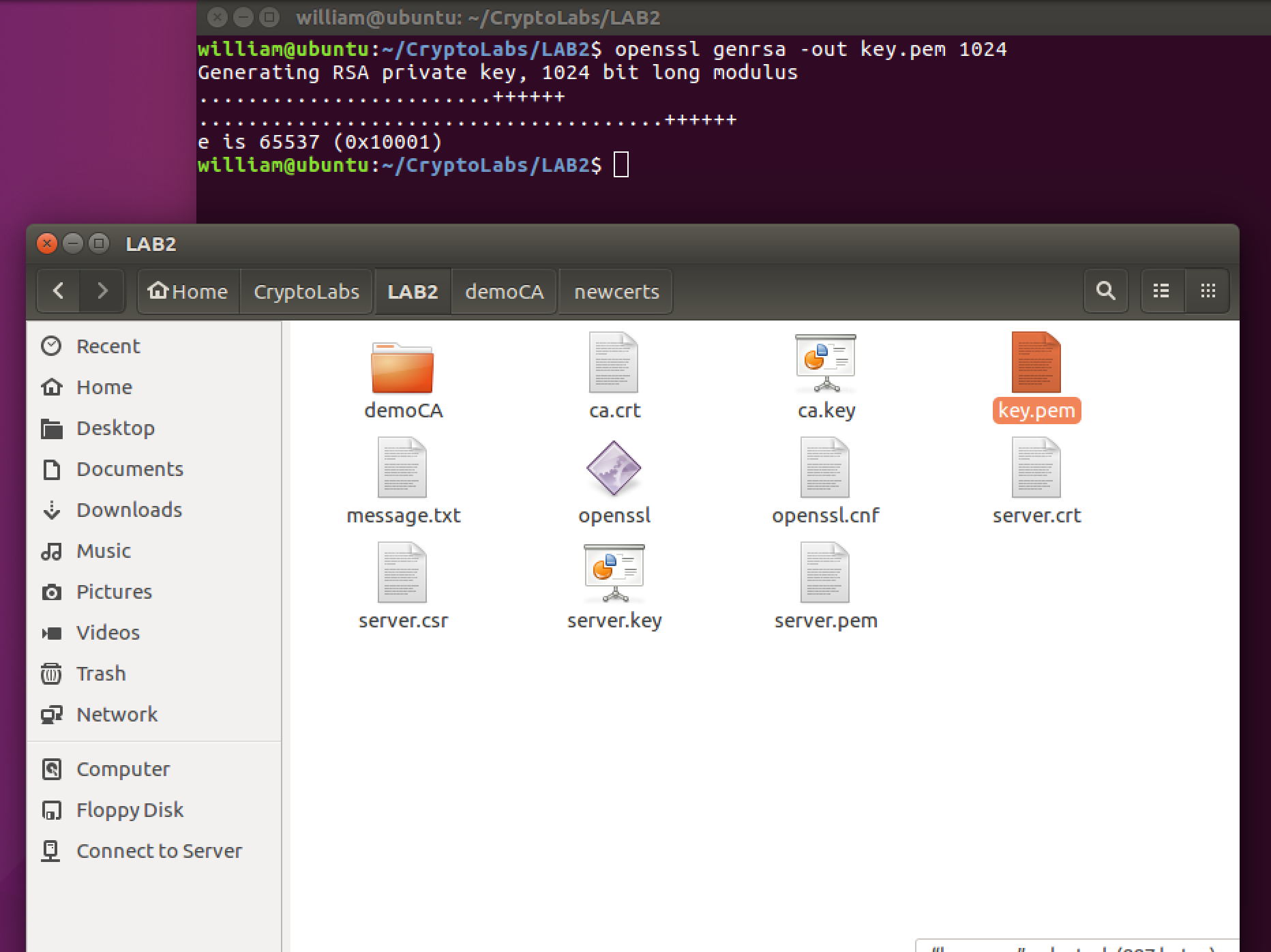


**Observation:**

The connection cannot be established to PKILabServer.com since the server certificate private key is corrupted.

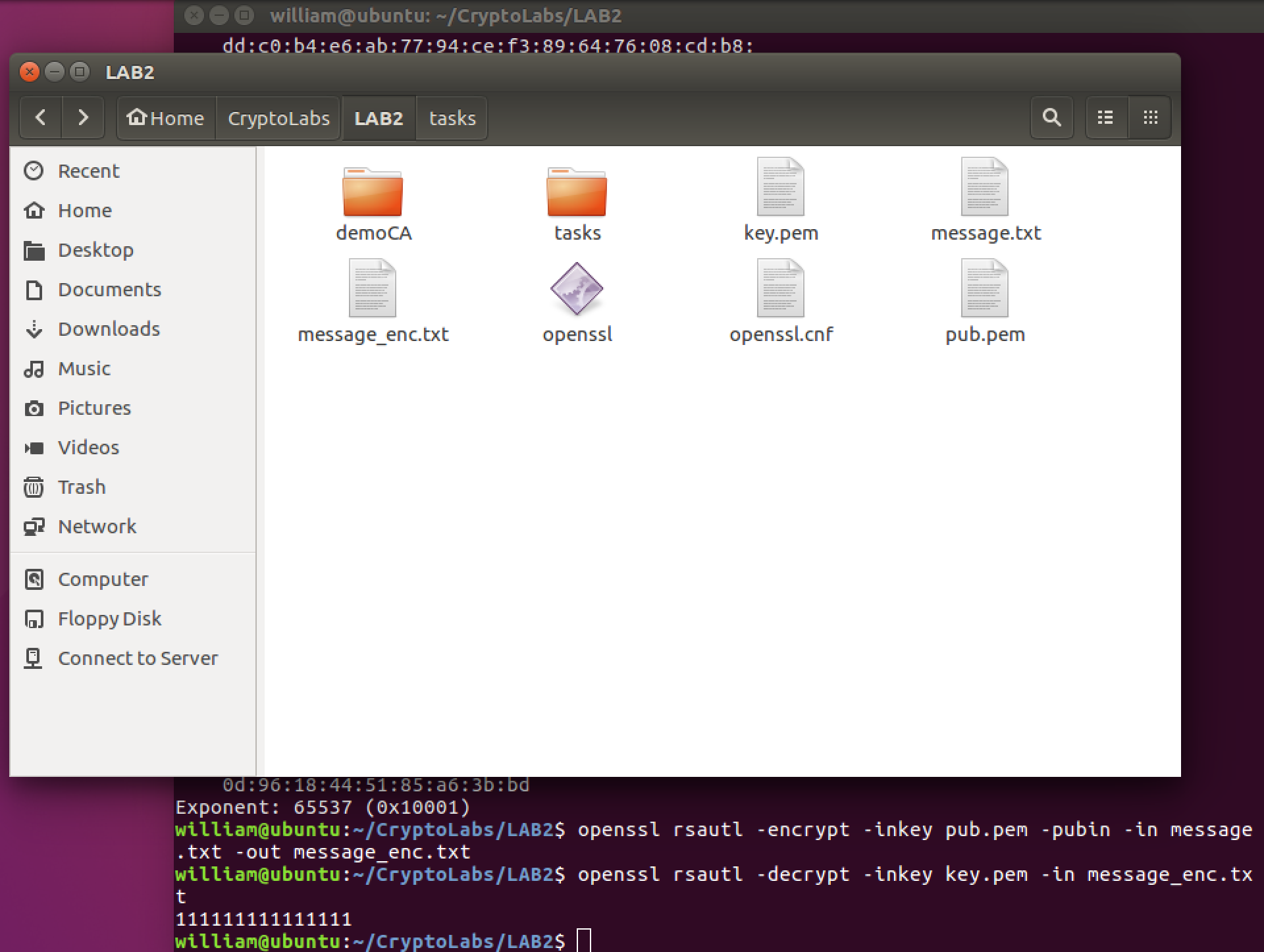
If I change the domain name to "localhost", I am blocked and warned as above. This is because i don't have a certificate for "localhost" at the local CA. I think this policy is especially important for the security of a private cluster. If you intercept the IP of a machine (hacking or whatever), you still won't be able to visit it if you don't know the certified domain name (which is often kept confidential). That's why an attempt visit simply by the IP will usually be rejected, as long as you're directing this attempt from an untrusted client.

Task 4



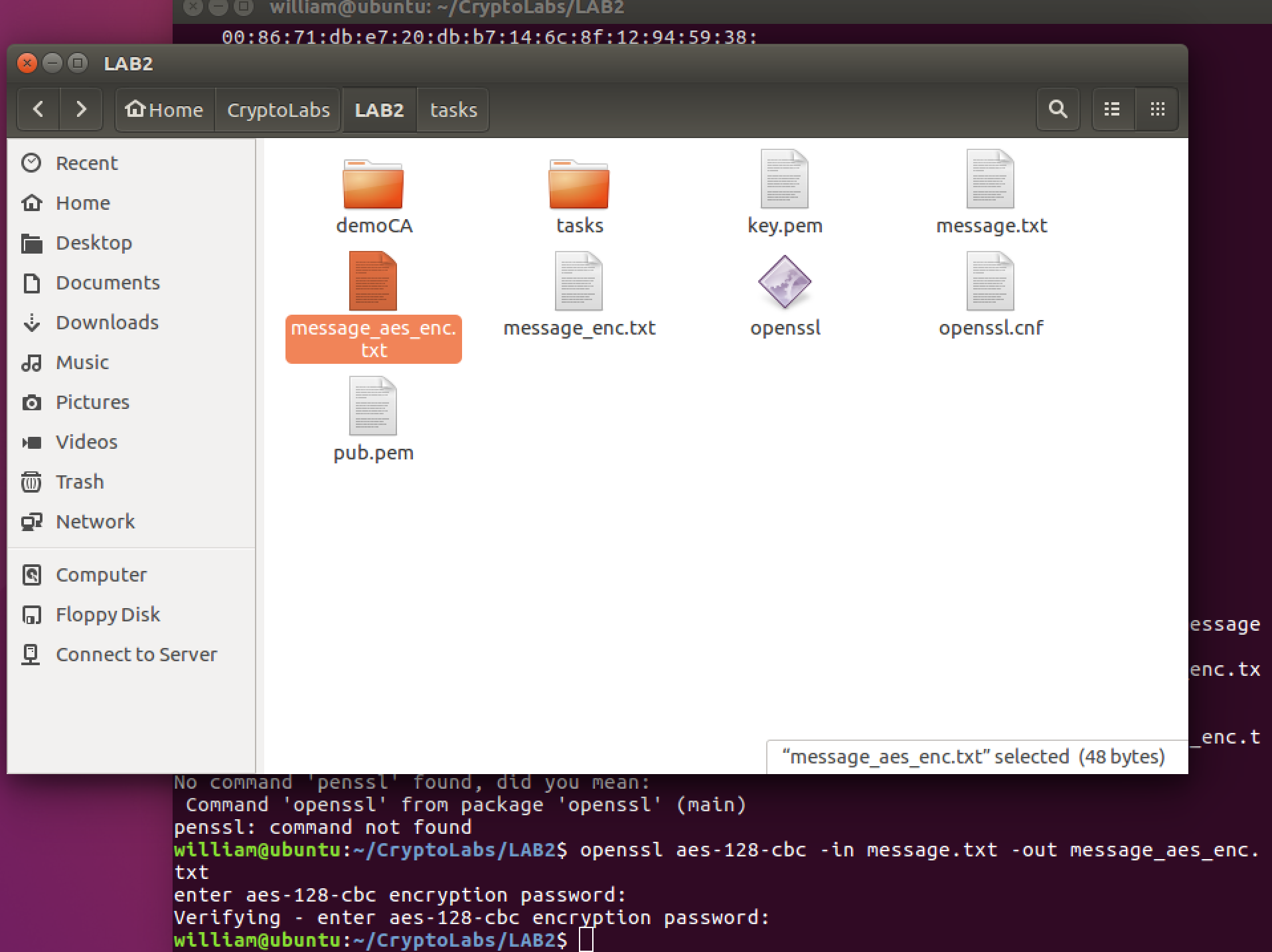
**Observation:**

Using the command as above, and I can get an key.pem file. It includes private key. And then I used the command “openssl rsa –in key.pem –pubout –out pub.pem” to save the public key in the pub.pem file. (You can see the file in the next figure)



**Observation:**

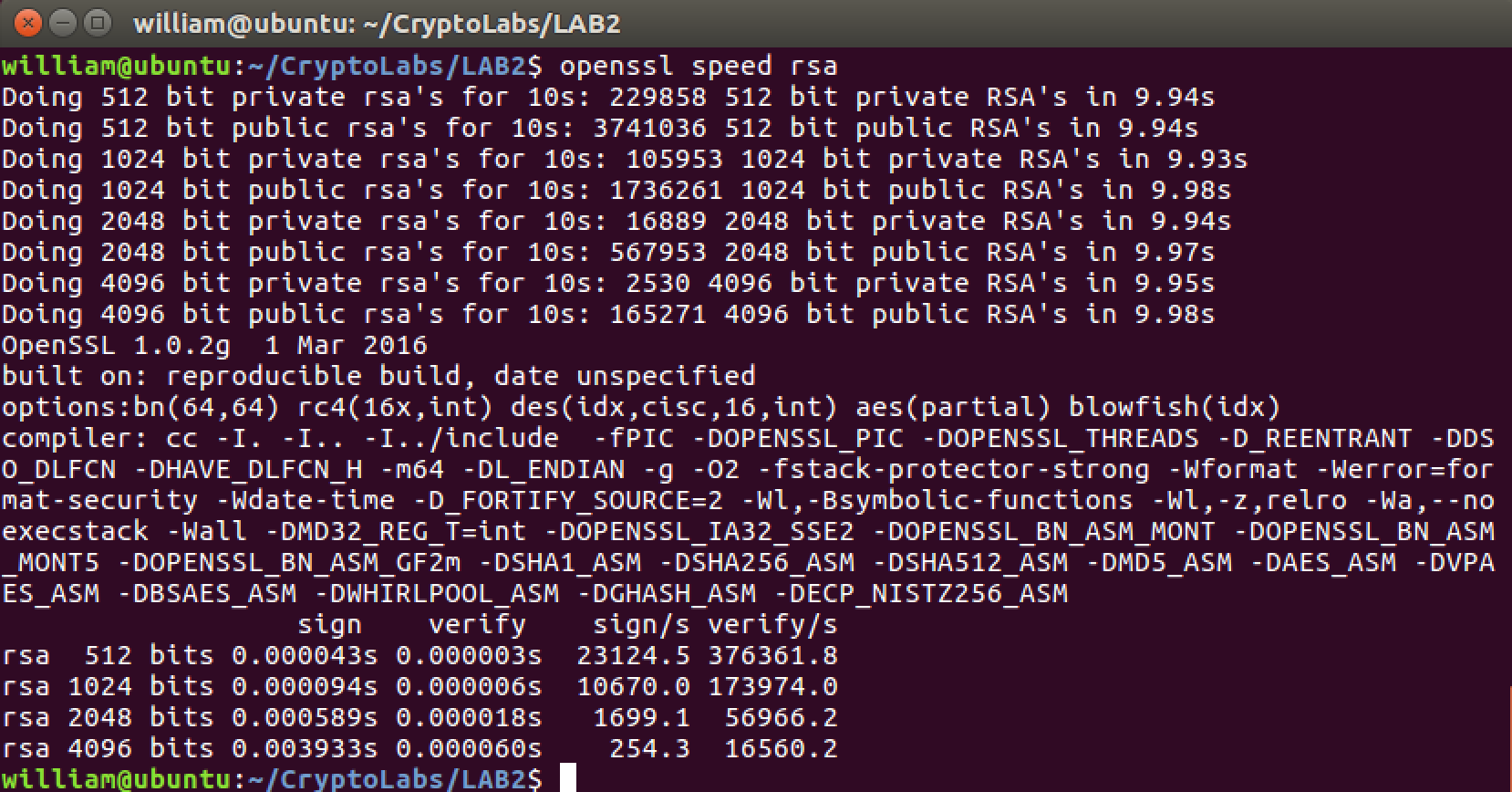
As the figure, you can see I use the two commands to encrypt the message.txt and decrypt the message\_enc.txt. I typed sixteen “1” in the plaintext file, the result is same.

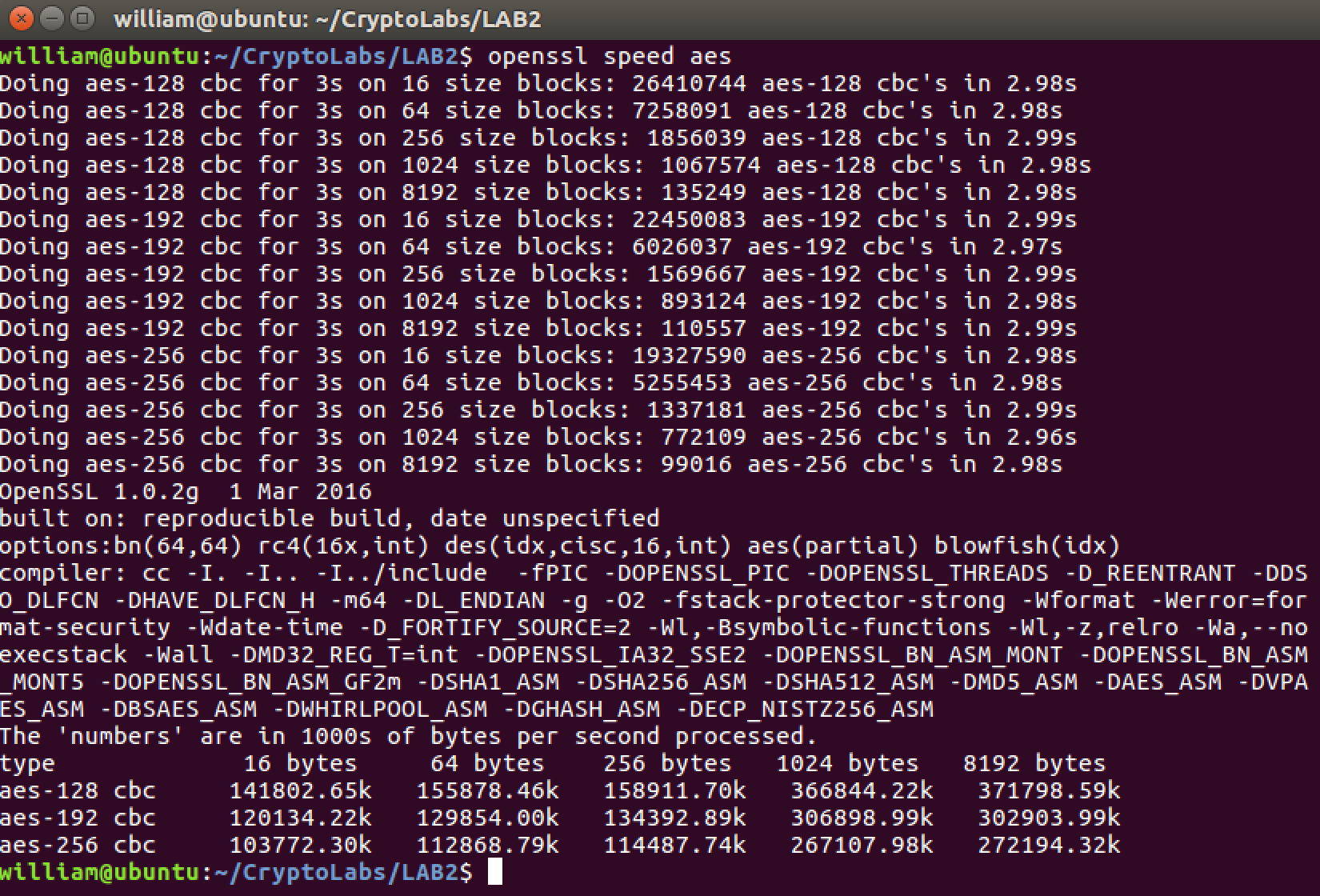


**Observation:**

And then, I used AES 128 CBC mode to encrypt the message.txt file and got the encrypted file message\_aes\_enc.txt.

Actually, the operation is too fast, I cannot compare the time of the two algorithms. But after several times encrypted, I think the RSA is slower than AES.

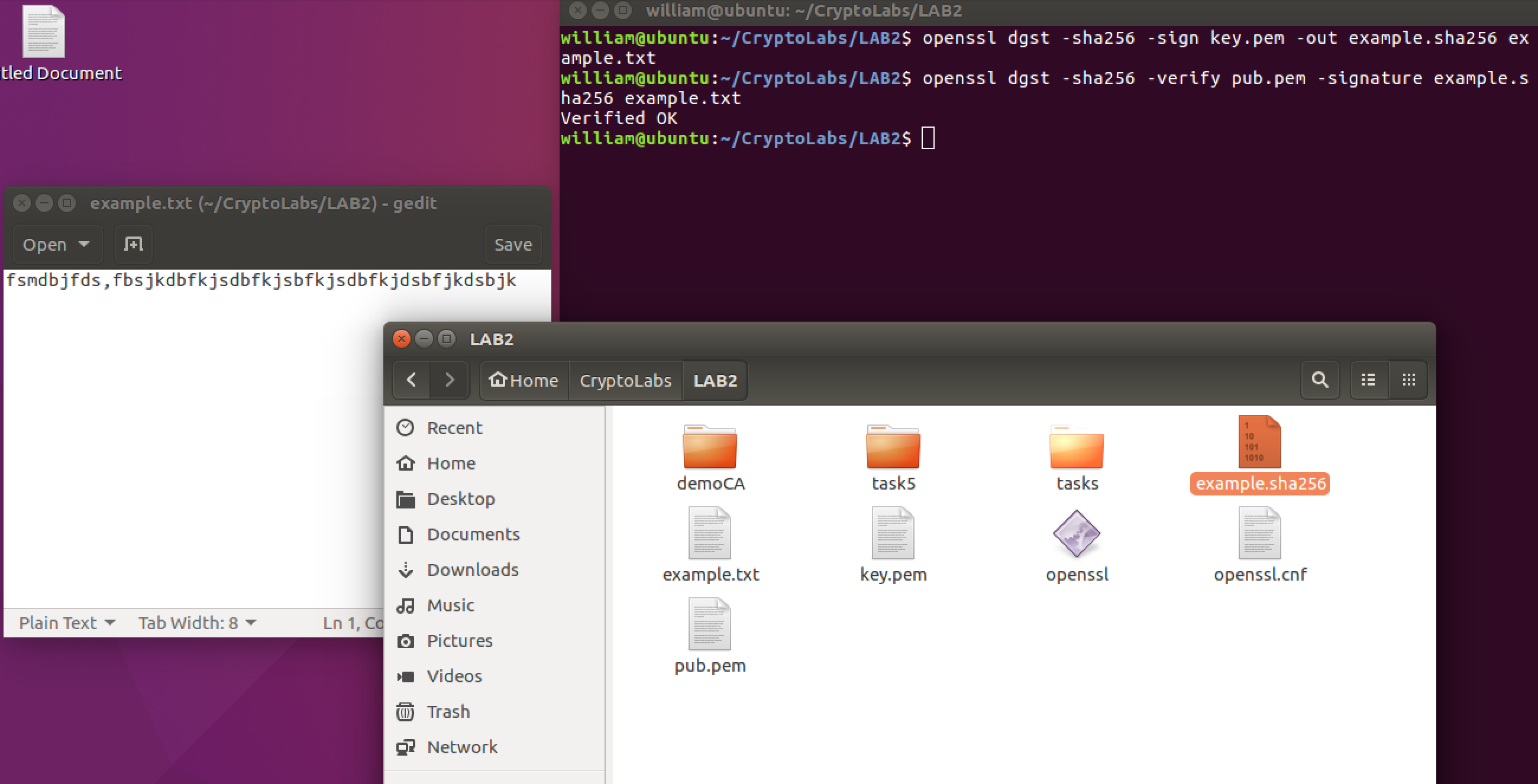




**Observation:**

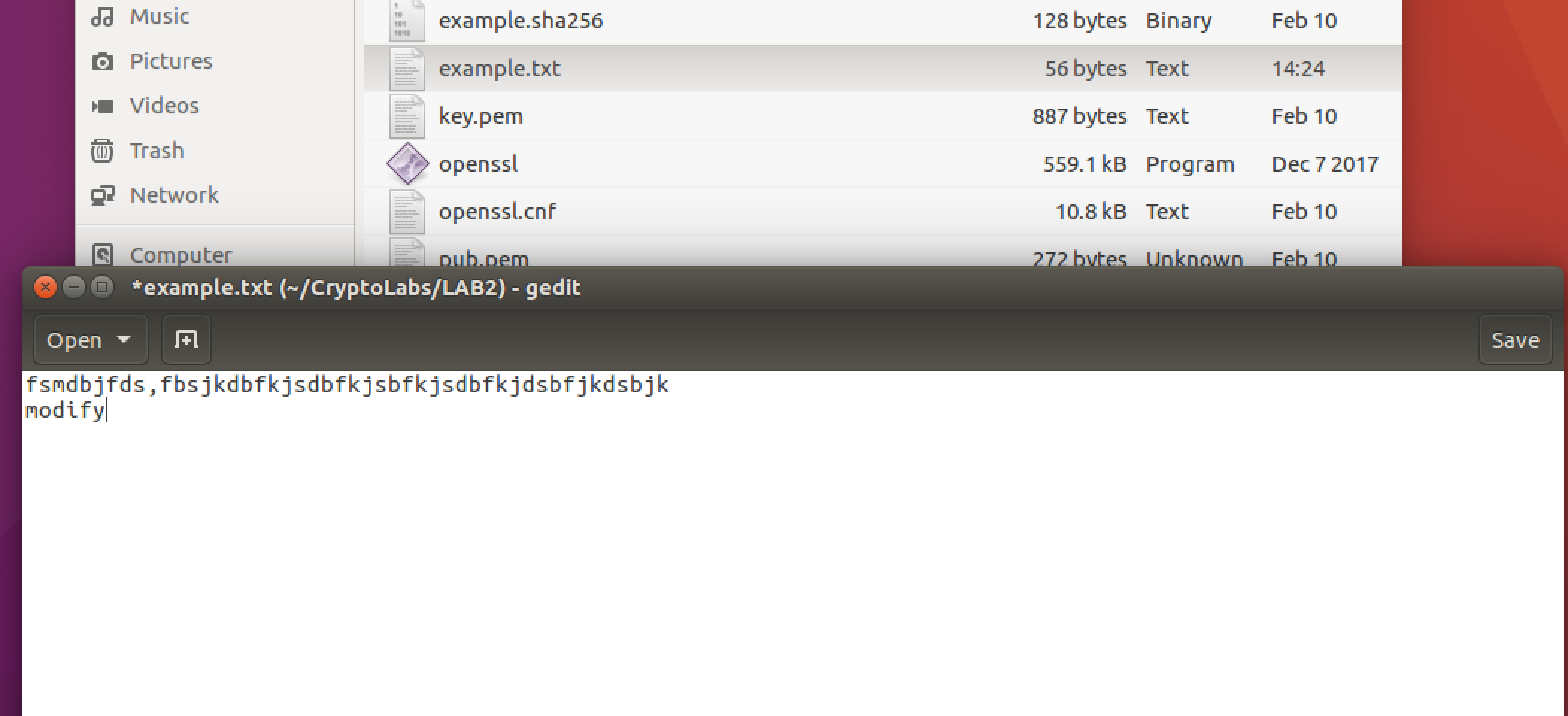
According to the two figures, we can see the RSA is slower than AES.

Task 5



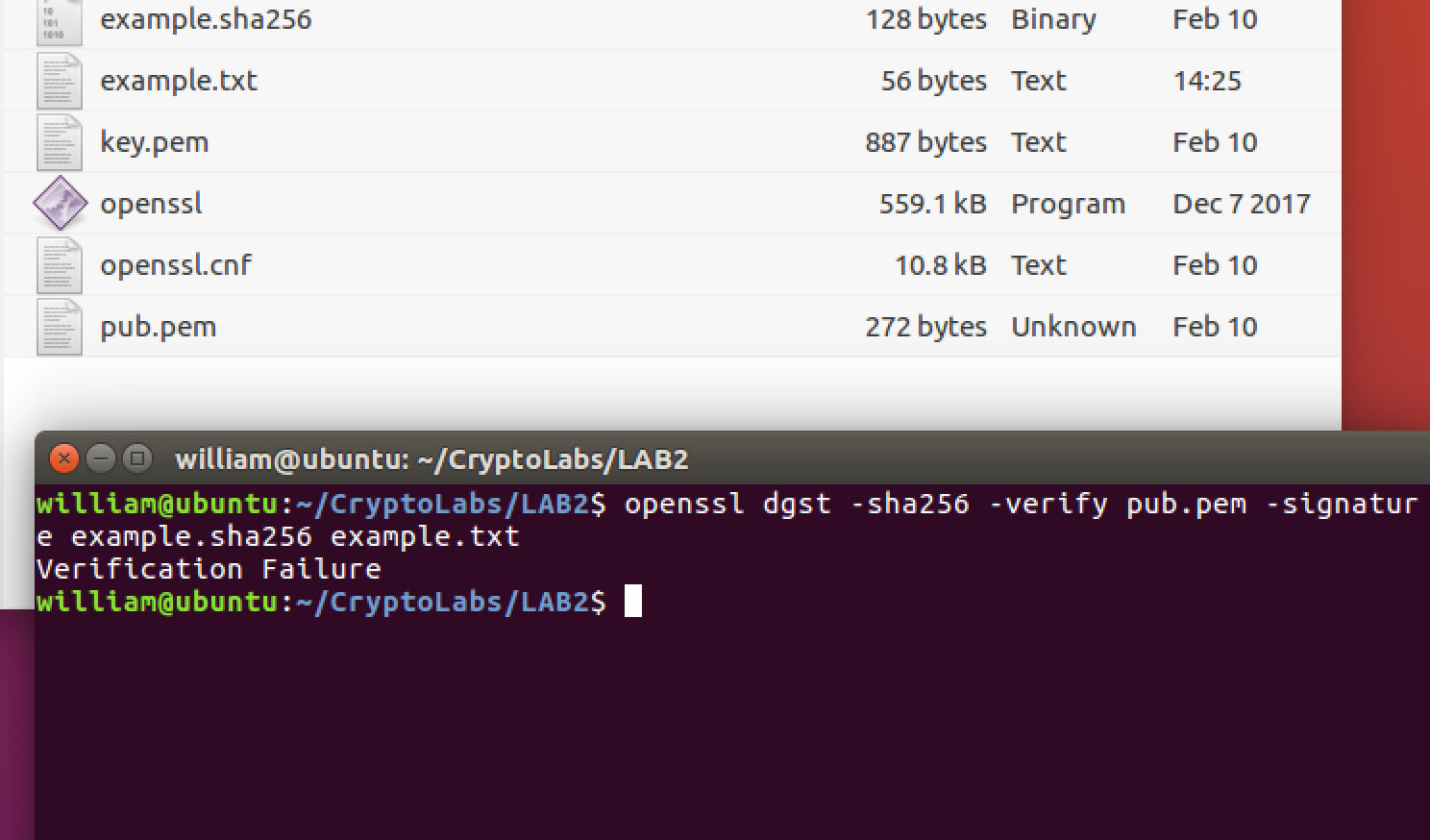
**Observation:**

In this figure, we can see that I used the RSA private key and SHA256 made a signature, and the output file is example.sha256. And then I verify the it by the public key and SHA256. The result is verified ok. (In this task, I used the key pair in task 4)



**Observation:**

I modified the example.txt file by adding a word “modify”.



**Observation:**

We can see the result is verification is failure.

Why digital signatures are useful?

Answer:

During the information transmission process, simply using encryption to ensure data confidentiality, there are still flaws. If the sender after sending a message suddenly back, declare that this information is not sent, although the data transmission process is confidential, it cannot prove the identity of the sender of this information. This is not conducive to the management of communications.

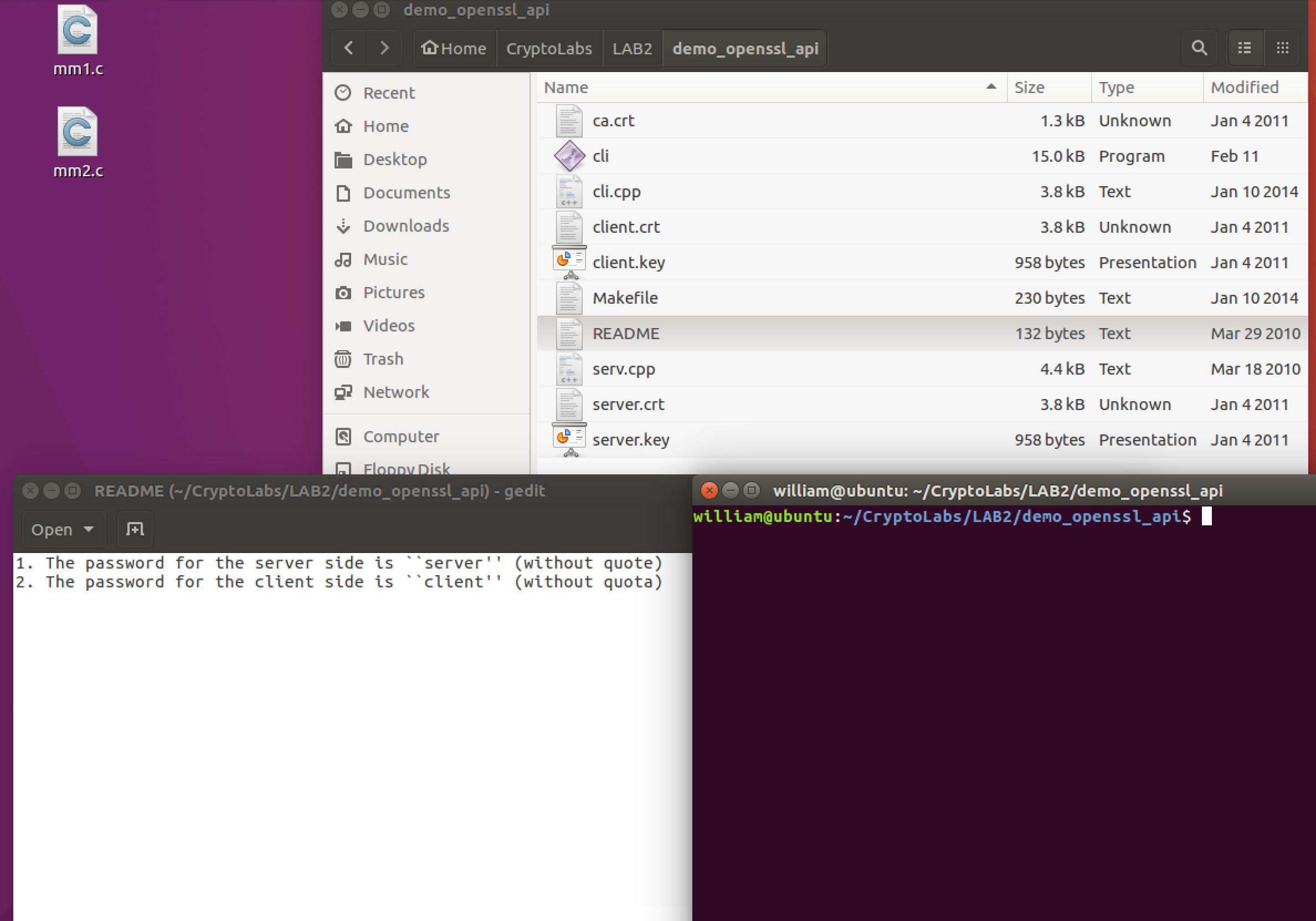
In reality, the way of signing is generally used to make the information undeniable. For example, contract negotiation and bank withdrawals all take the form of user signatures to prove that this information really happened.

In the digital signature process, the sender is based on the information to be sent and its own private key encrypted digital digest combined into a digital signature. Users use their own private key to handle the information, because the key is only for this, so the file is unique. It formed a digital signature. The digital signature has the following two advantages:

1. Guarantee information is signed by the signer to send, the signer cannot deny or hard to deny.

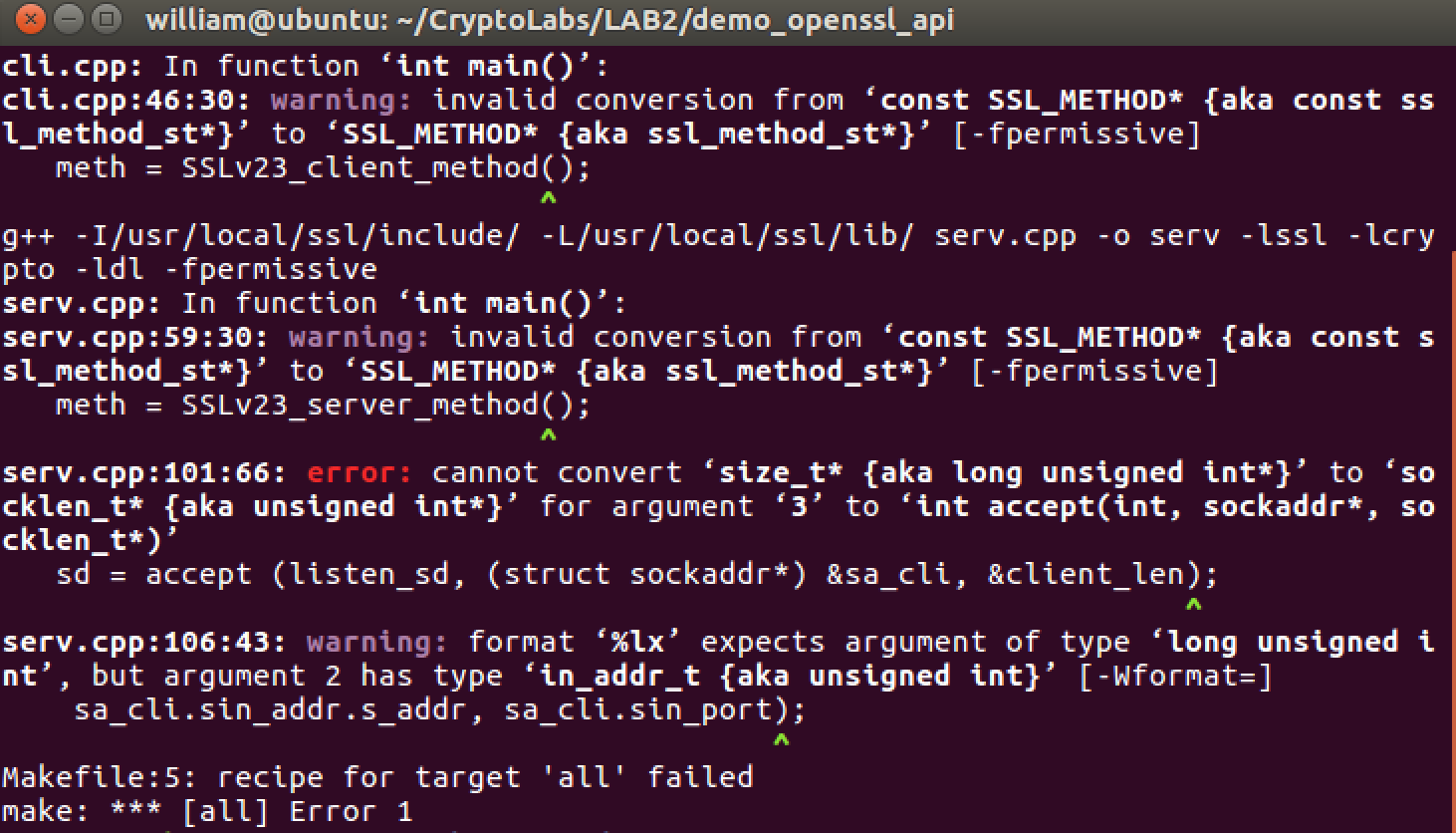
2. The receiving people can verify that the information has not been modified from sender to receiver, and the file issued is a true one.

Task 6



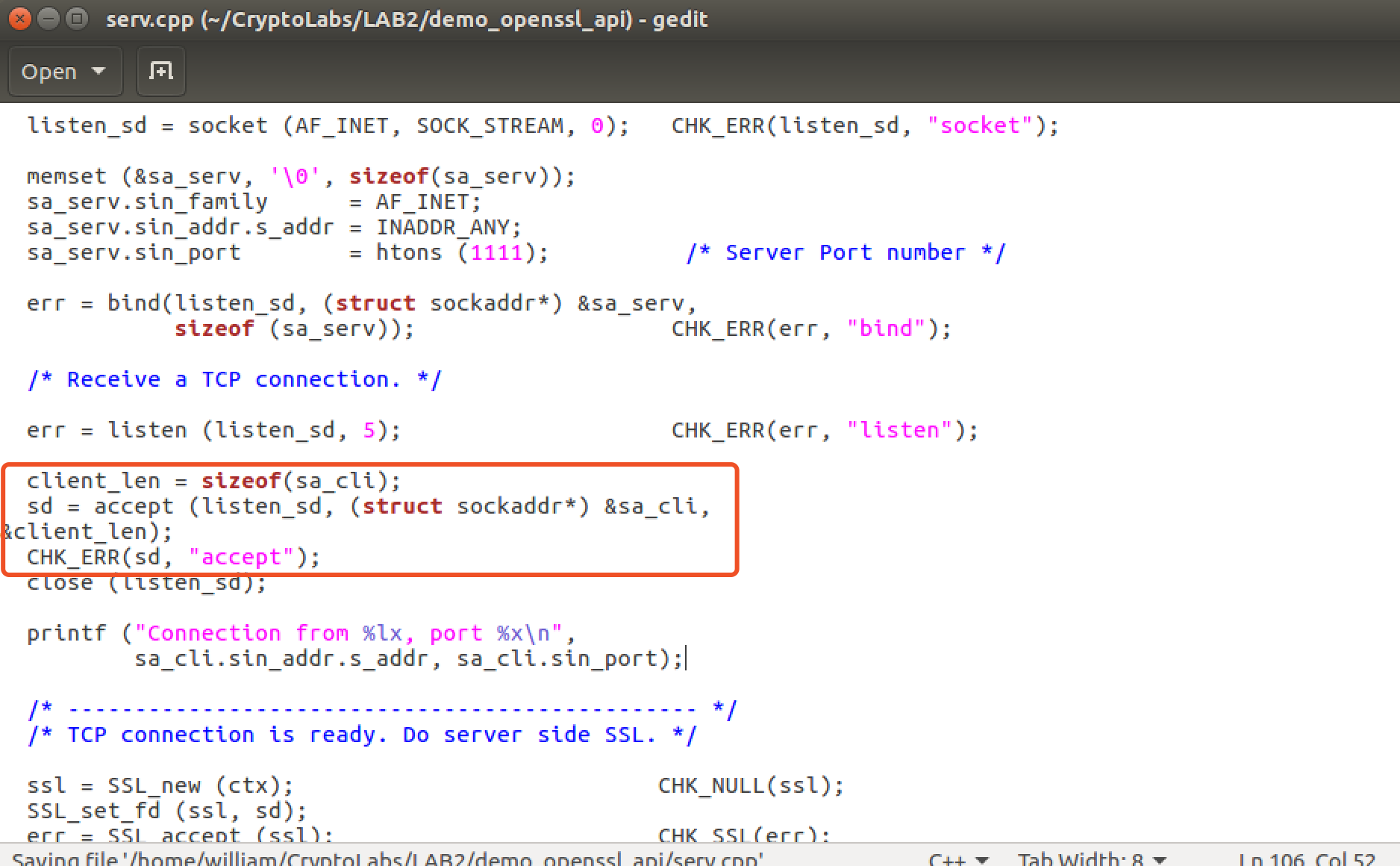
**Observation:**

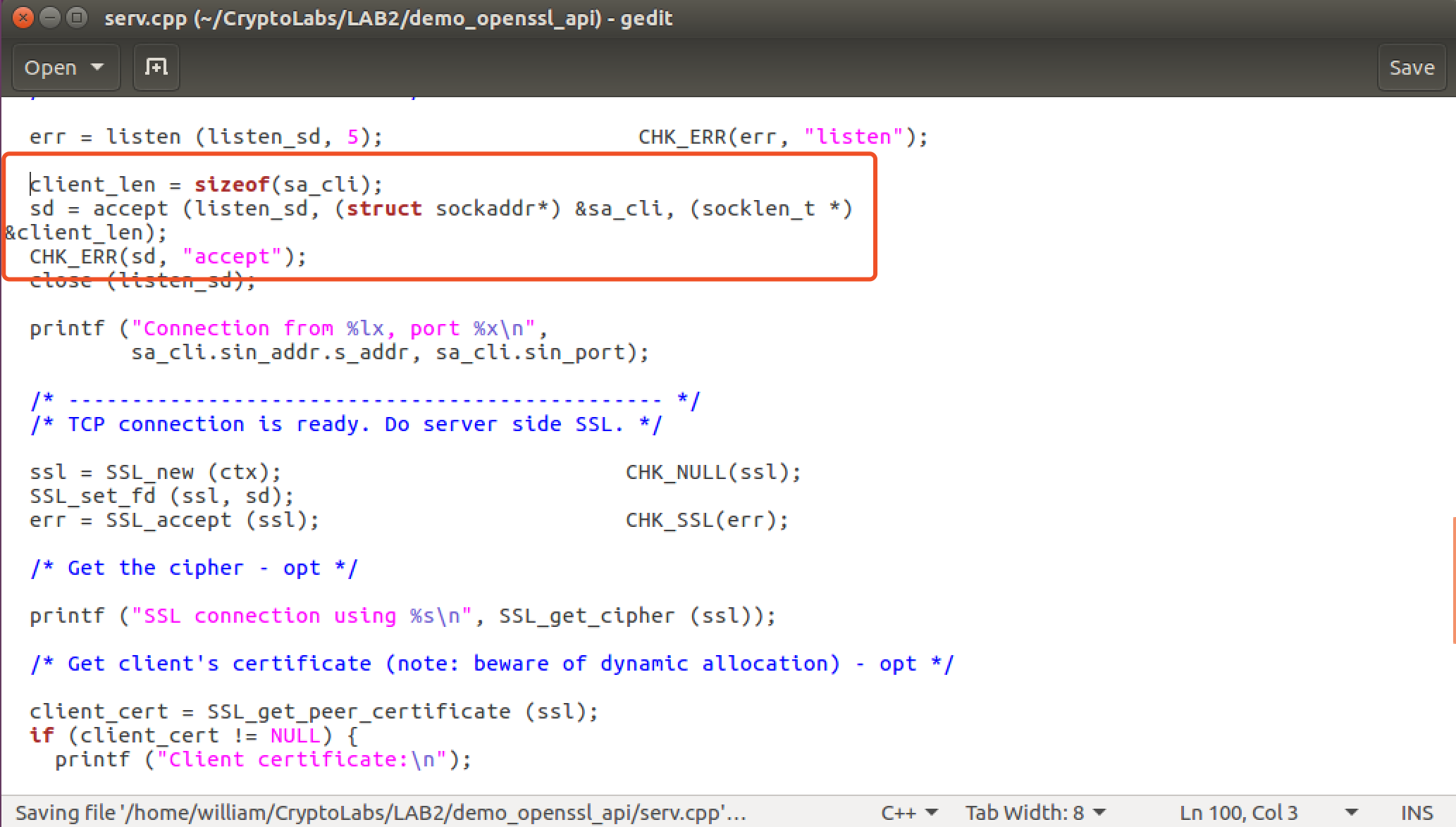
Download the client-server demo program from the given URL and try it.



**Observation:**

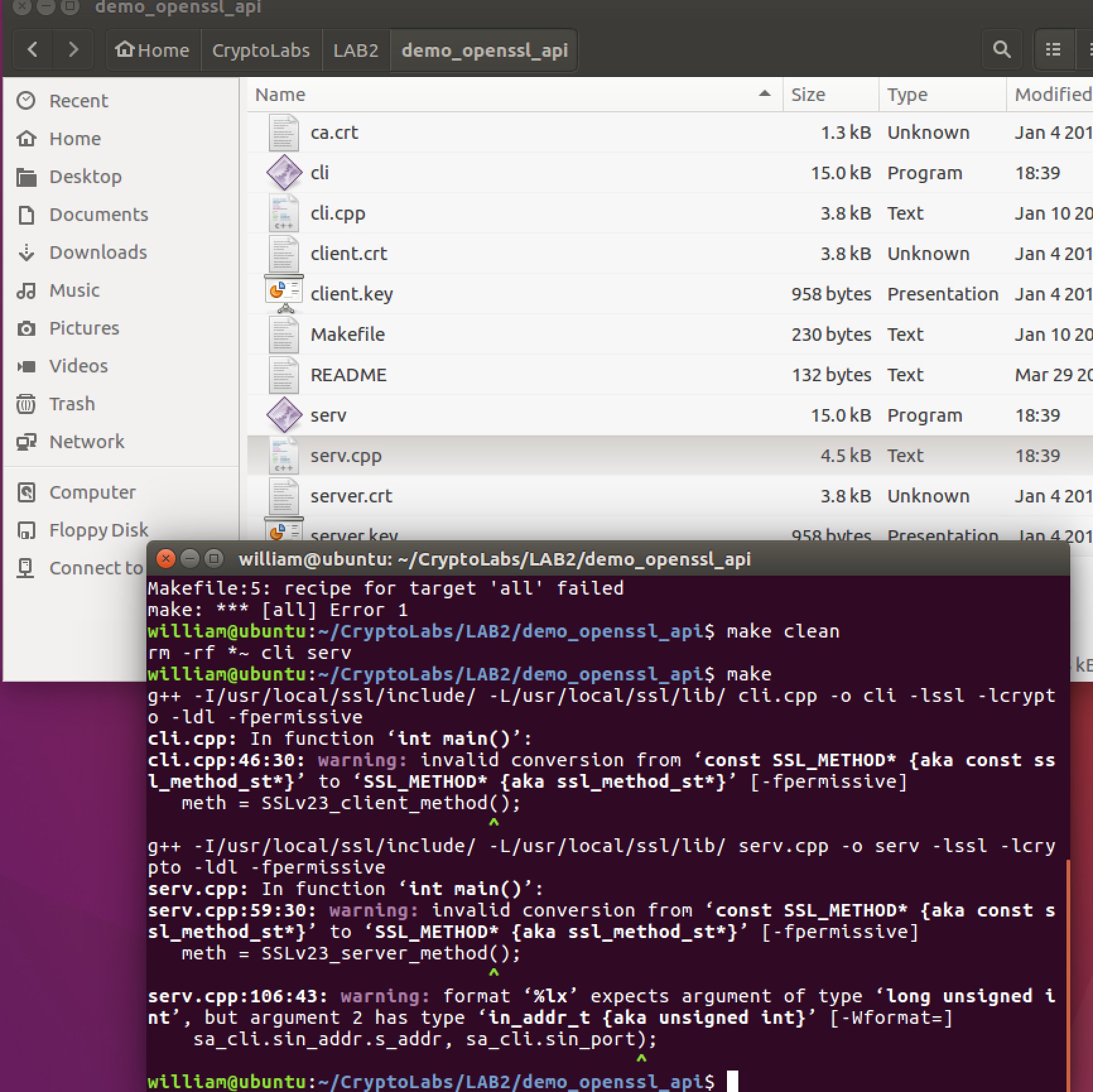
Then I run the client and server demo. The order should be server first and client second. After make, there are some errors.





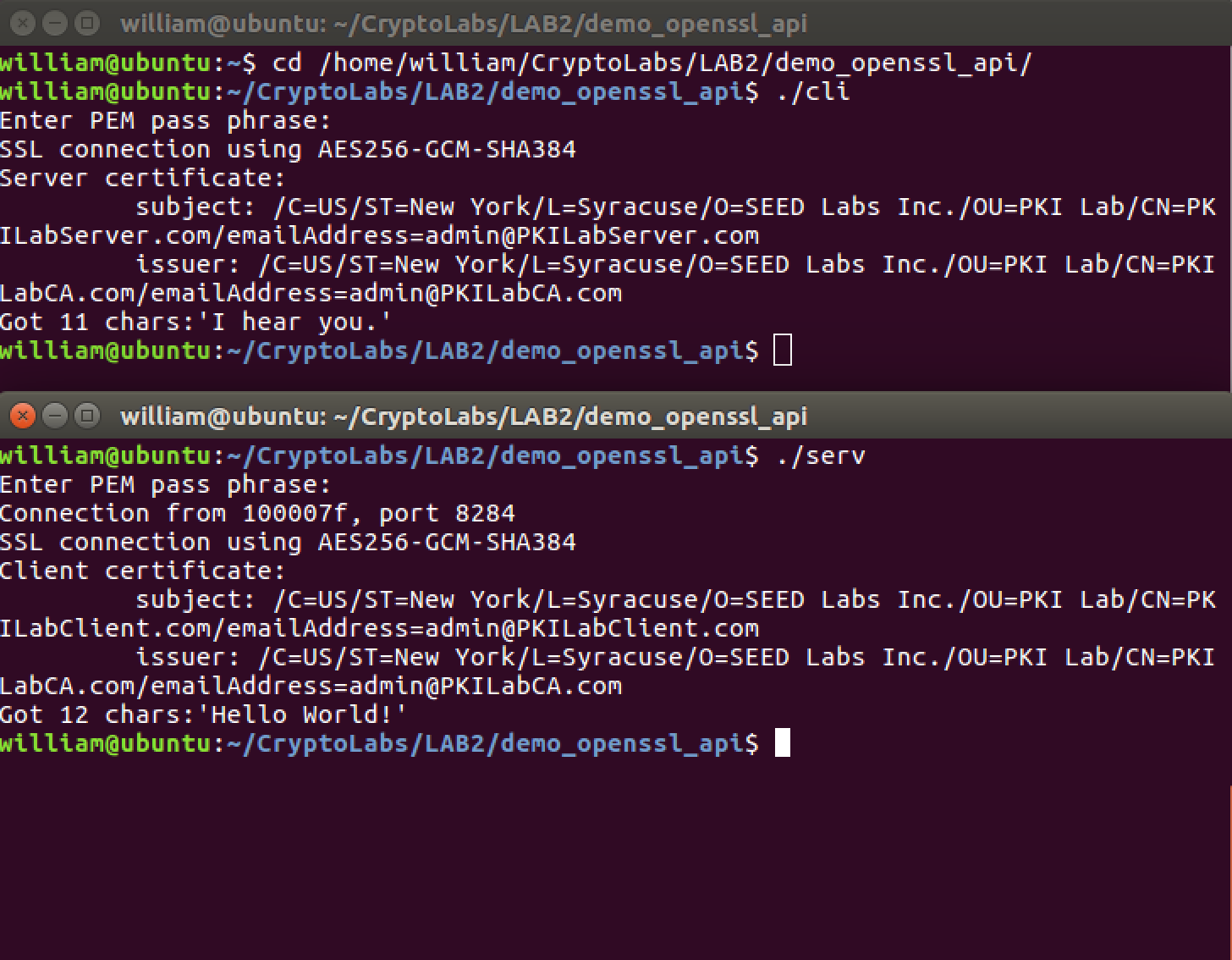
**Observation:**

Let correct the code from the first figure to the second one.



**Observation:**

Make again, and we can see the serv and cli files.



**Observation:**

Run the server and the client, the server program was hanged up at startup. When the client program started, both programs exited successfully with a message.

Server got greeted by the client: Hello World! Client got responded by the server: I hear you.