

**Information Security**

**Assignment 03**

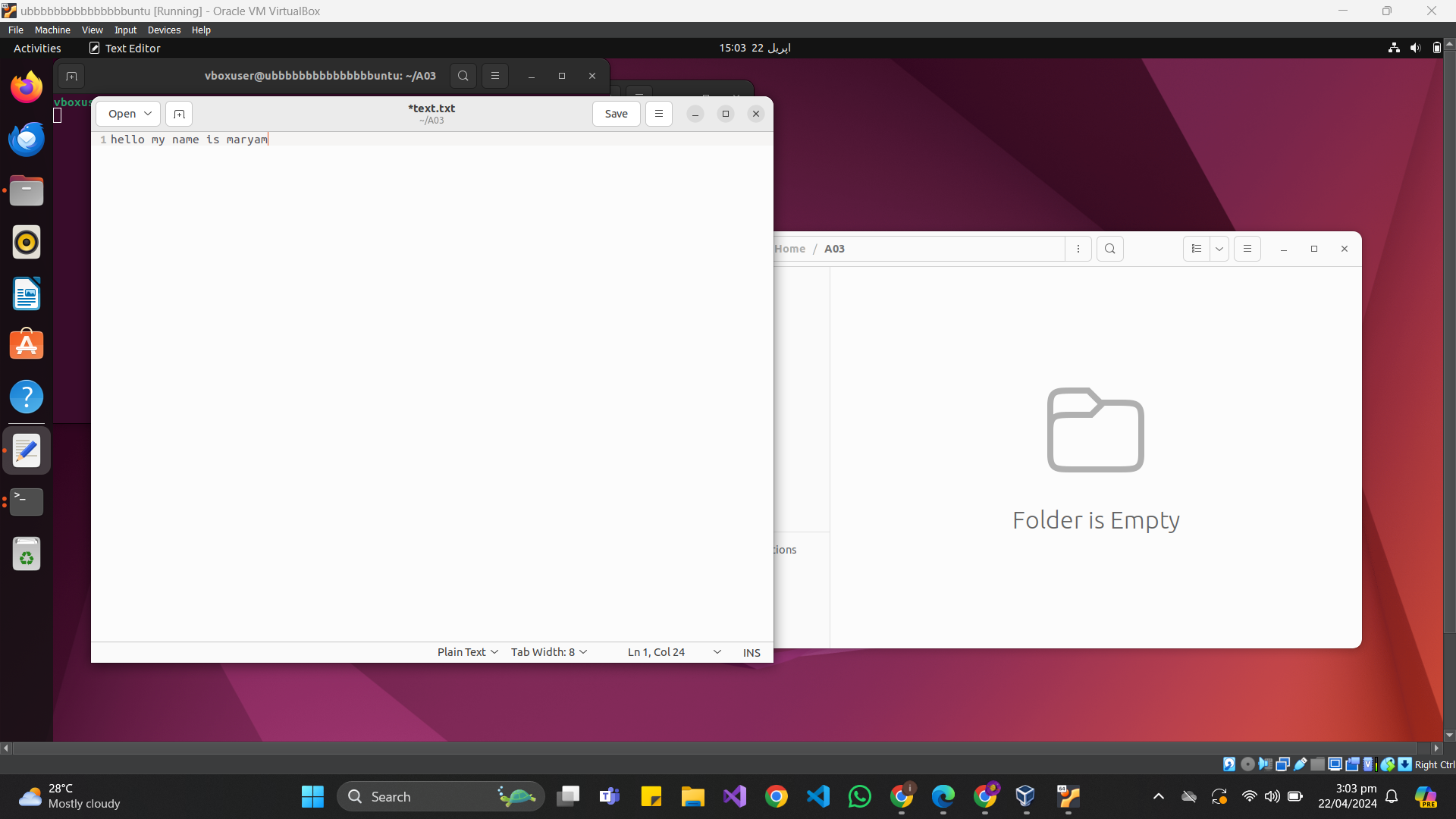
Maryam Shah (21i1570)

Hassaan Jamil (21i-2774)

Encryption and decryption using openssl 256

1.For this I used ubuntu since openssl is pre-installed in ubuntu.

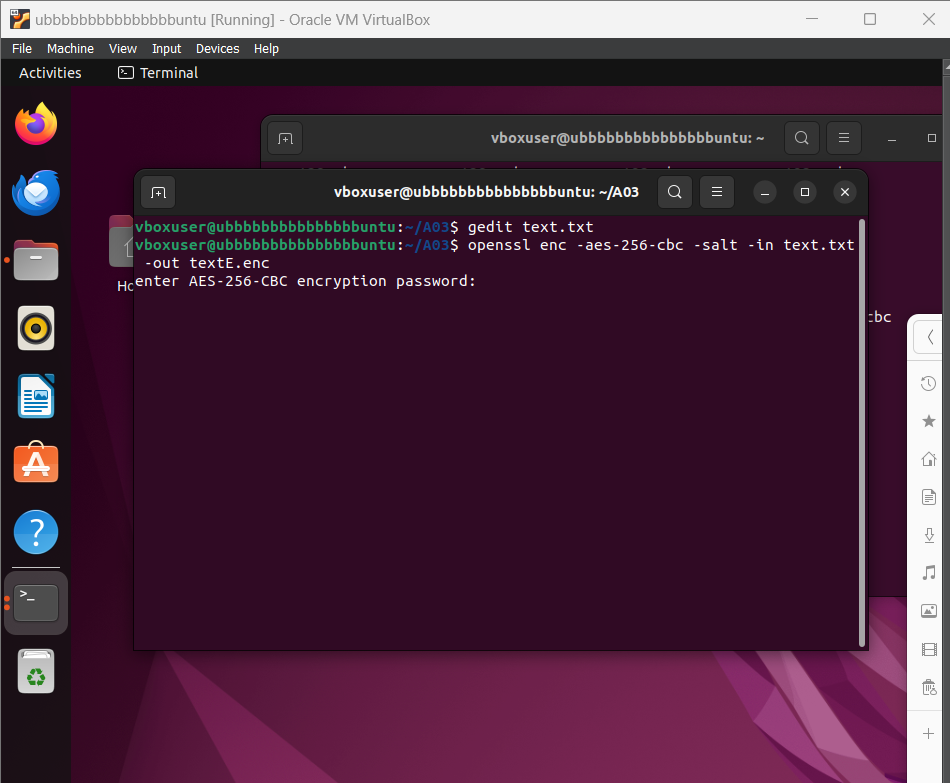
2. I created a file “text.txt” and entered random text inside it



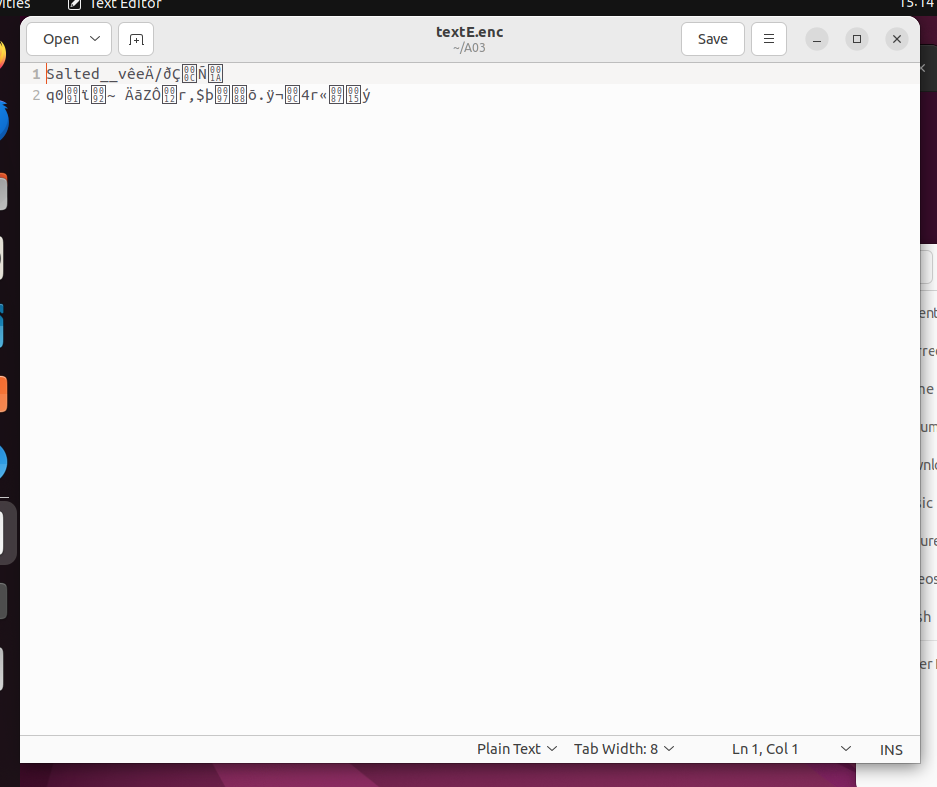
3. Then to encrypt this file I opened the terminal and used the following command;

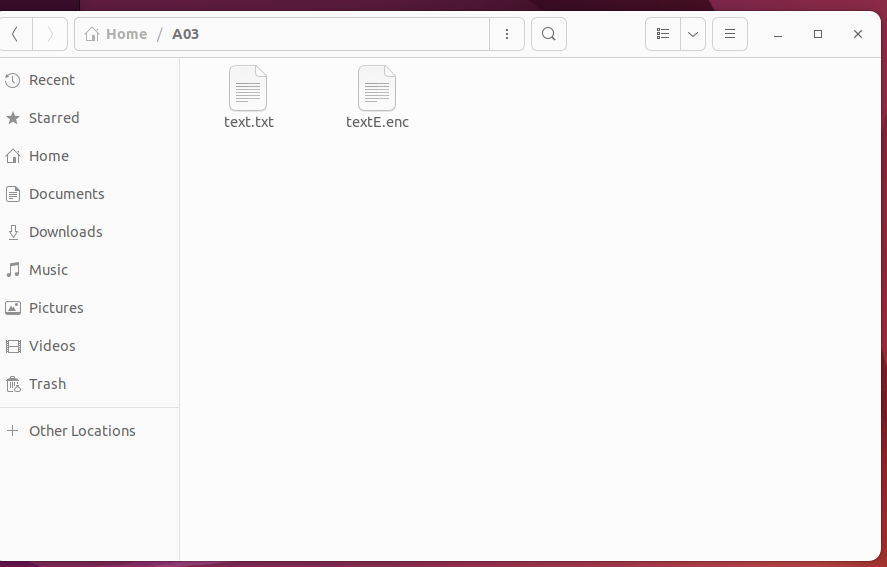
*openssl enc -aes-256-cbc -salt -in <input\_file.txt> -out <output\_file.enc>*

4. Then I entered the password of choice “hello”

**

5. Here is the encrypted file

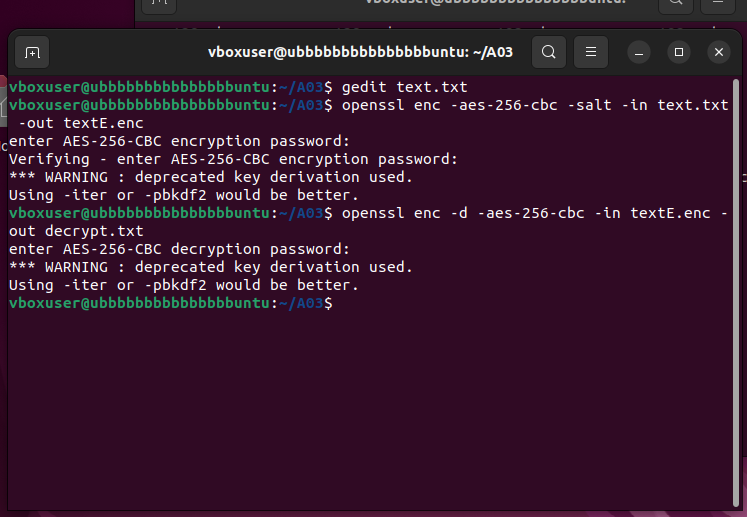




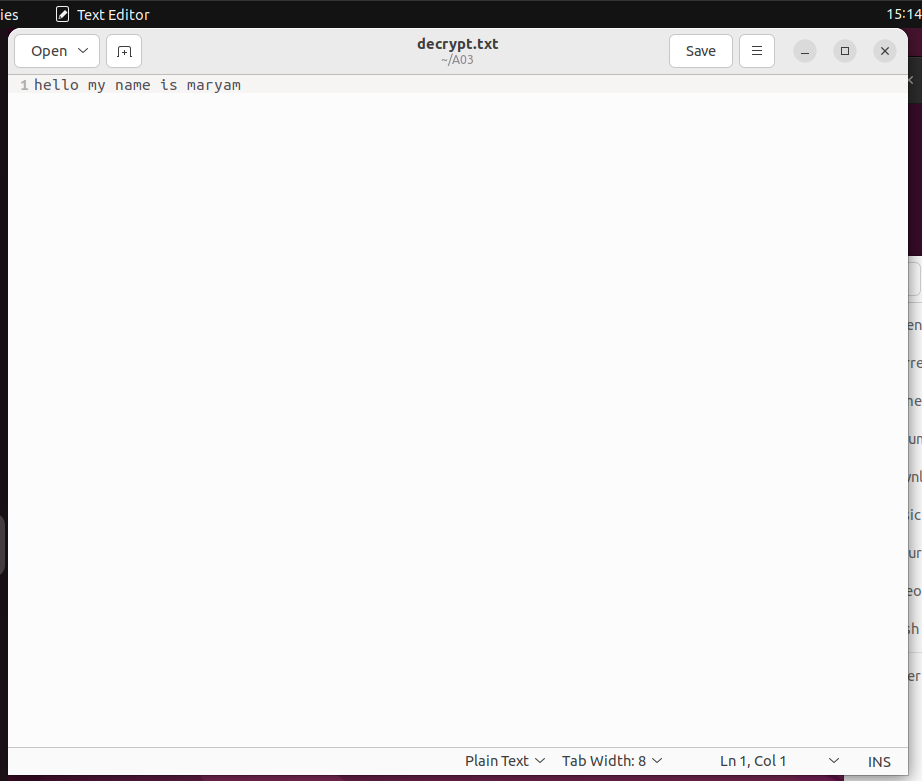
6. Then to decrypt the file I used the command

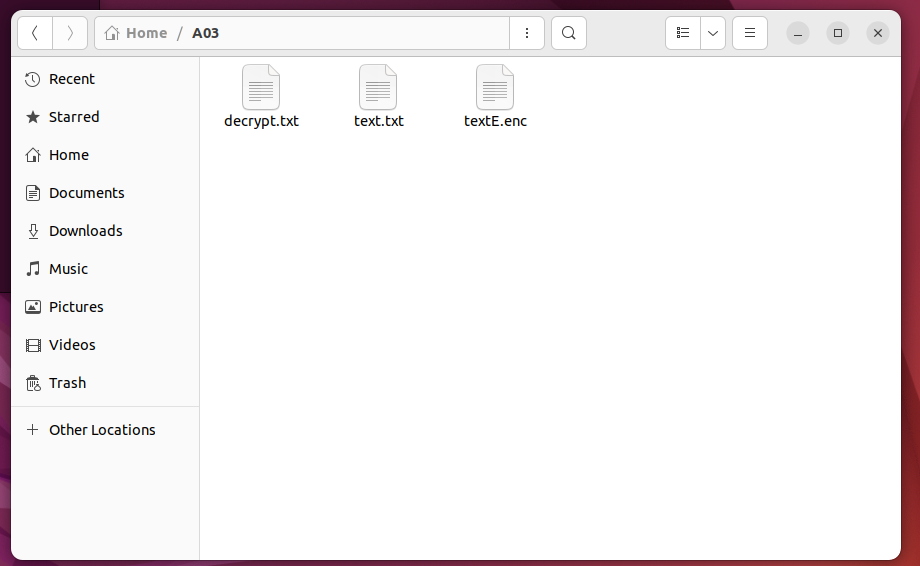
*openssl enc -d -aes-256-cbc -in <output\_file.enc> -out <decrypted\_file.txt>*

And entered the password that was set before

**

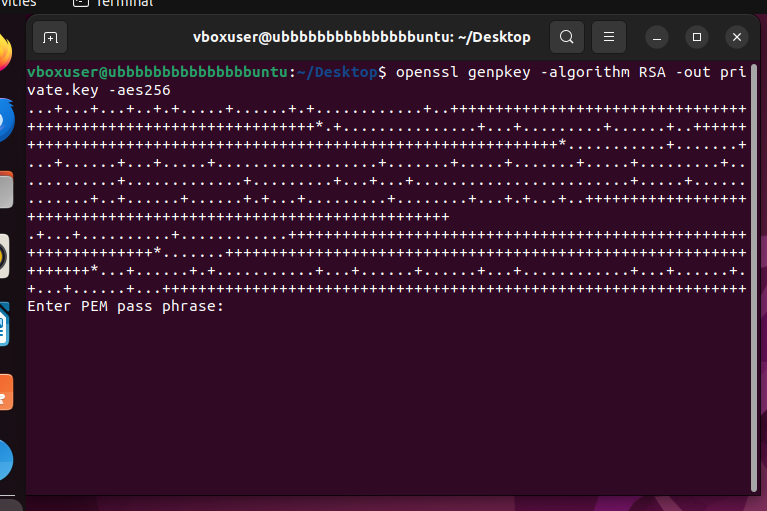
7. Here are the decrypted files



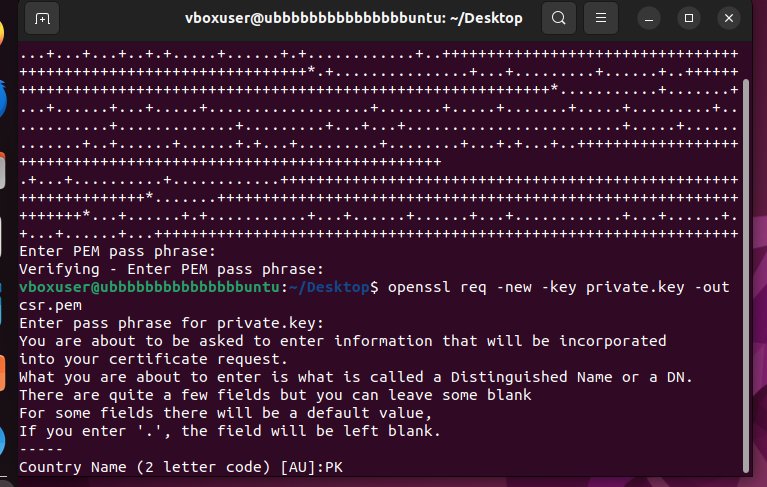


Manage certificates

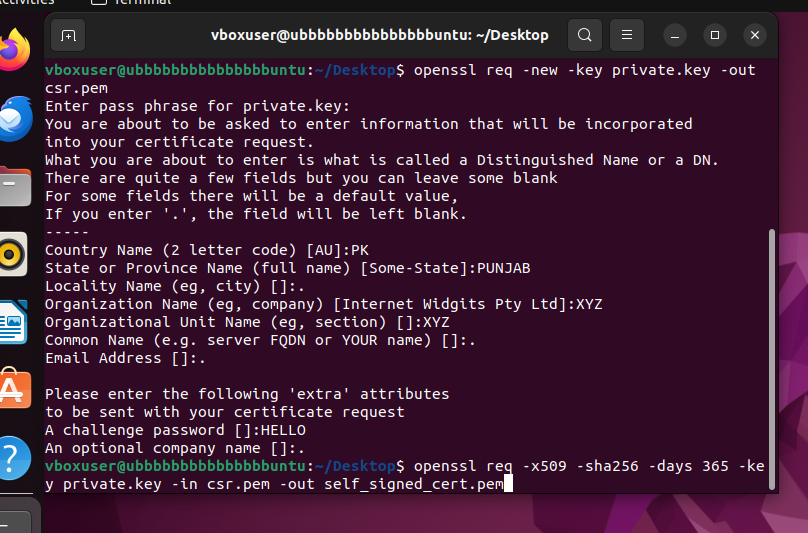
1. I again used ubuntu for this
2. I used the command *openssl genpkey -algorithm RSA -out private.key -aes256* to generate a private key. The following command generates a 2048 bit private key and entered a PEM pass “hello”

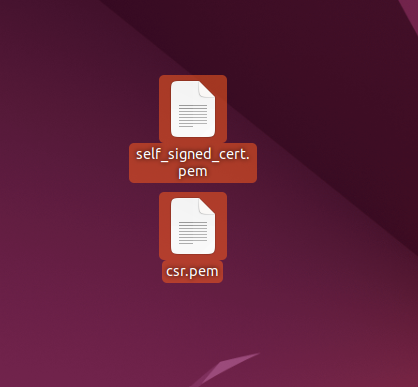


1. Then to generate the CSR I used my private key and the following command *openssl req -new -key private.key -out csr.pem.* During this I was asked to provide some information regarding my organization



1. Finally, I generated the self signed certificate using my private key. I used the following command for this *openssl req -x509 -sha256 -days 365 -key private.key -in csr.pem -out self\_signed\_certificate.pem*

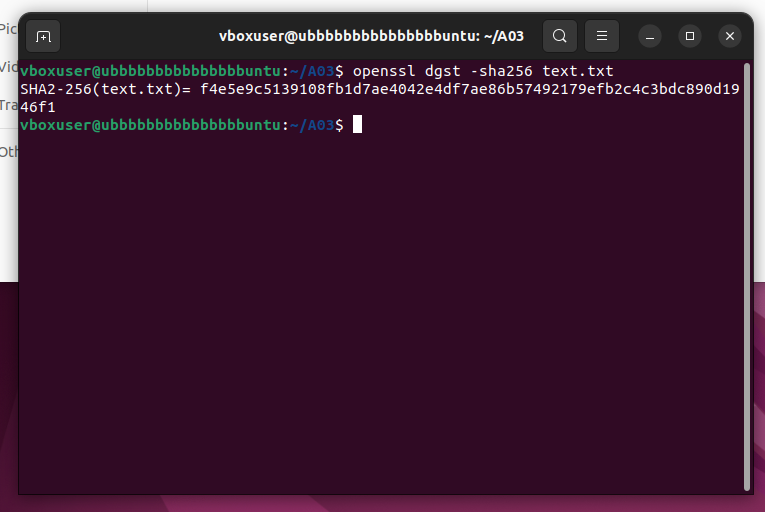




Generate Hashes

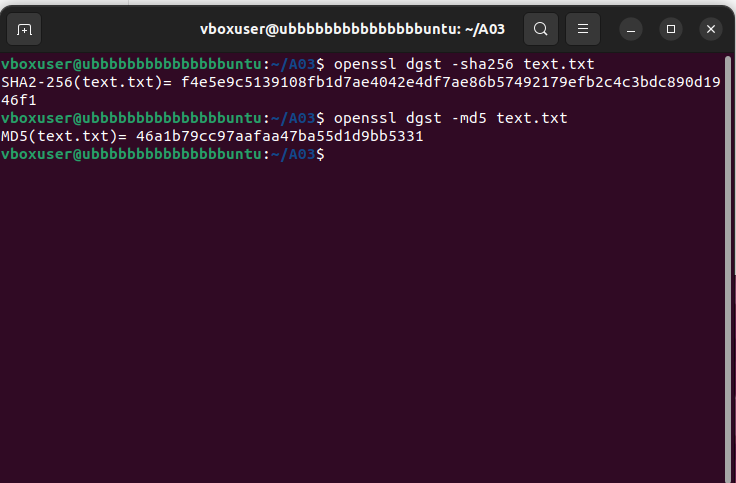
SHA-256

Using the command *openssl dgst -sha256 <file\_name>*

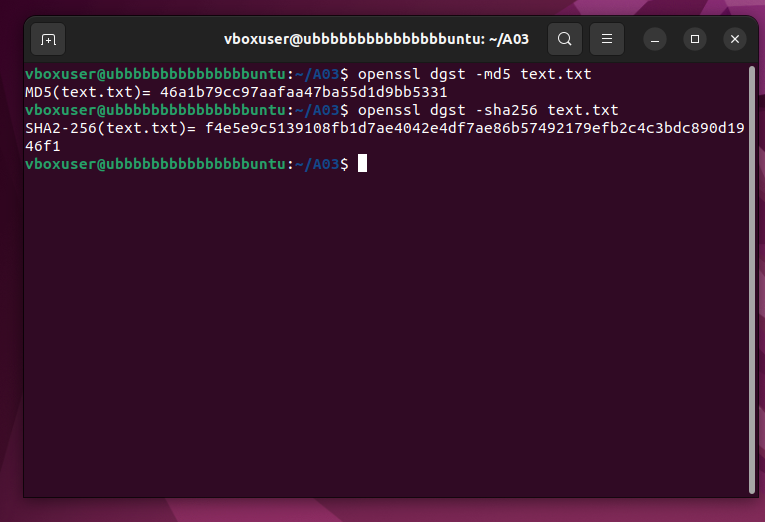
**

MD-5 using the command

*openssl dgst -md5 <file\_name>*

**

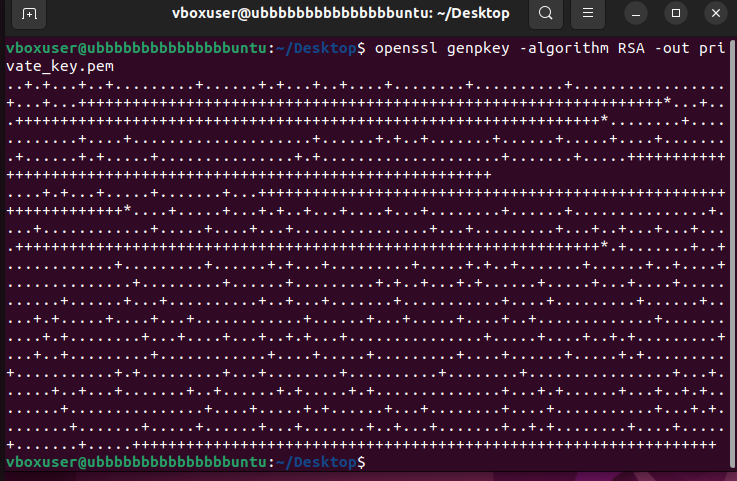
Verifying by generating the hashes again



Digital signature and verification

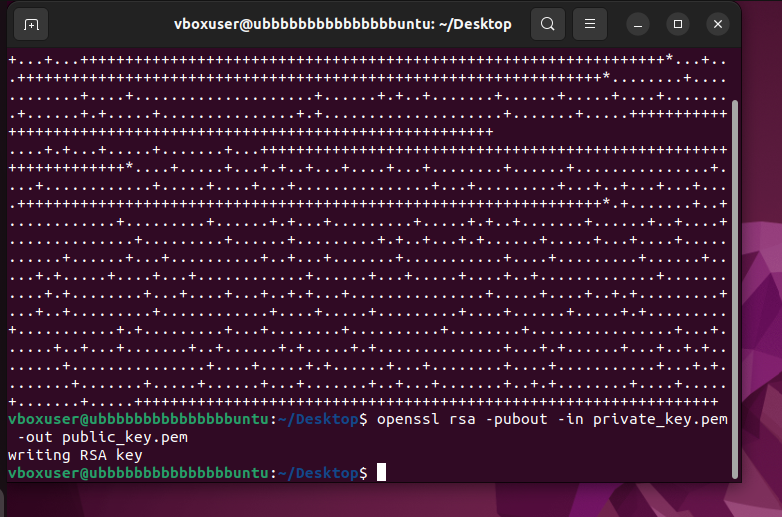
1. I generated a private key *openssl genpkey -algorithm RSA -out private\_key.pem*

RSA algorithm is being used and it saves it in the file “private\_key.pem”

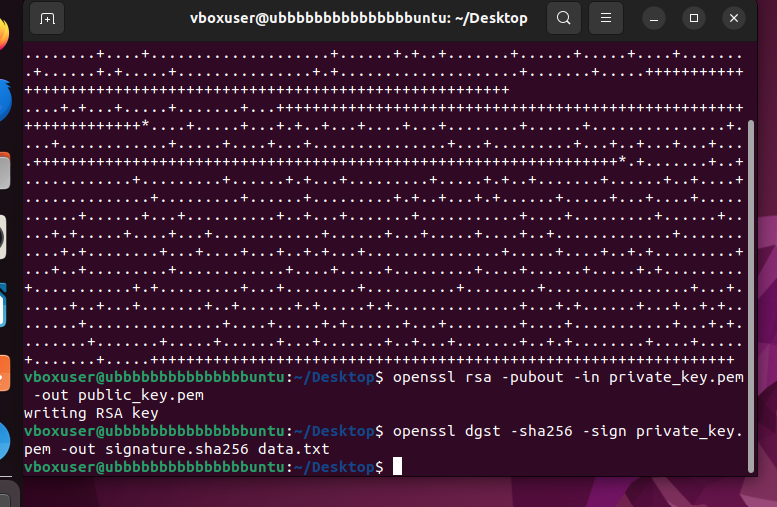


1. Then I generated a public key using the command *openssl rsa -pubout -in private\_key.pem -out public\_key.pem*

It gets saved in “public\_key.pem”



1. Then to sign the data that was present in the “data.txt” file I used the following command *openssl dgst -sha256 -sign private\_key.pem -out signature.sha256 data.txt*



1. Finally, to verify the signature I used the command *openssl dgst -sha256 -verify public\_key.pem -signature signature.sha256 data.txt*

Verified ok: signature is valid

Verification failure: not valid signature

