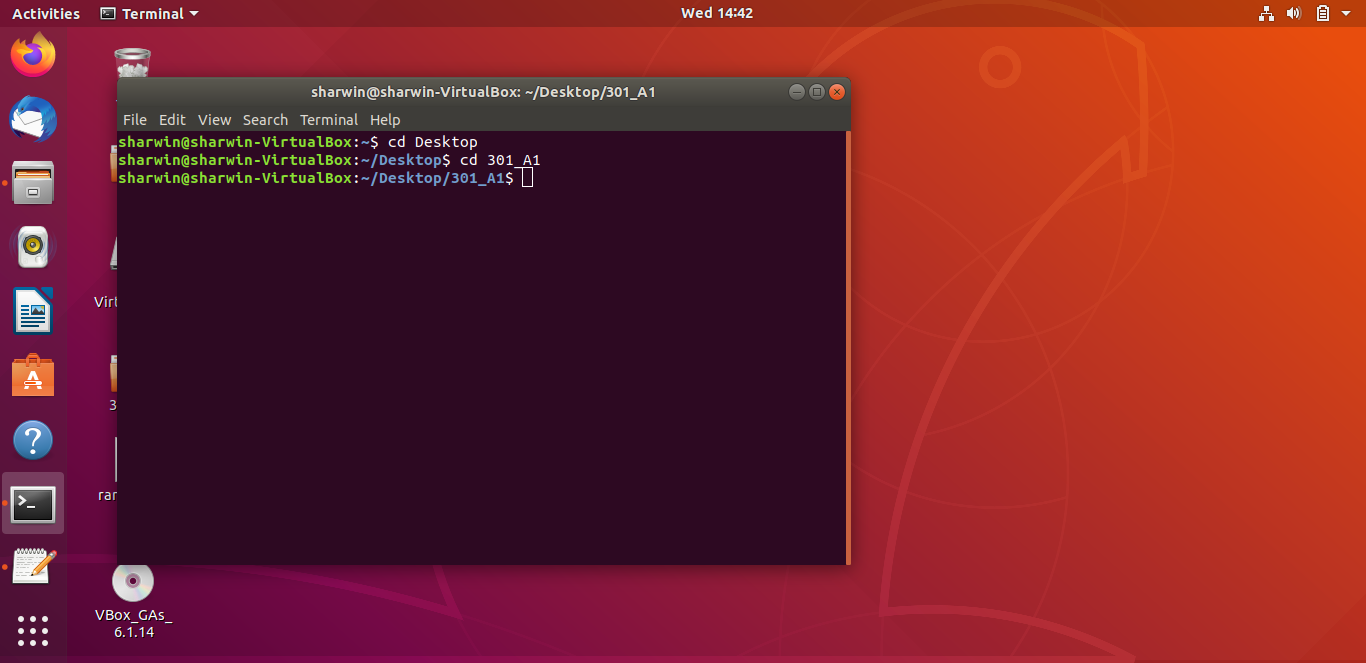
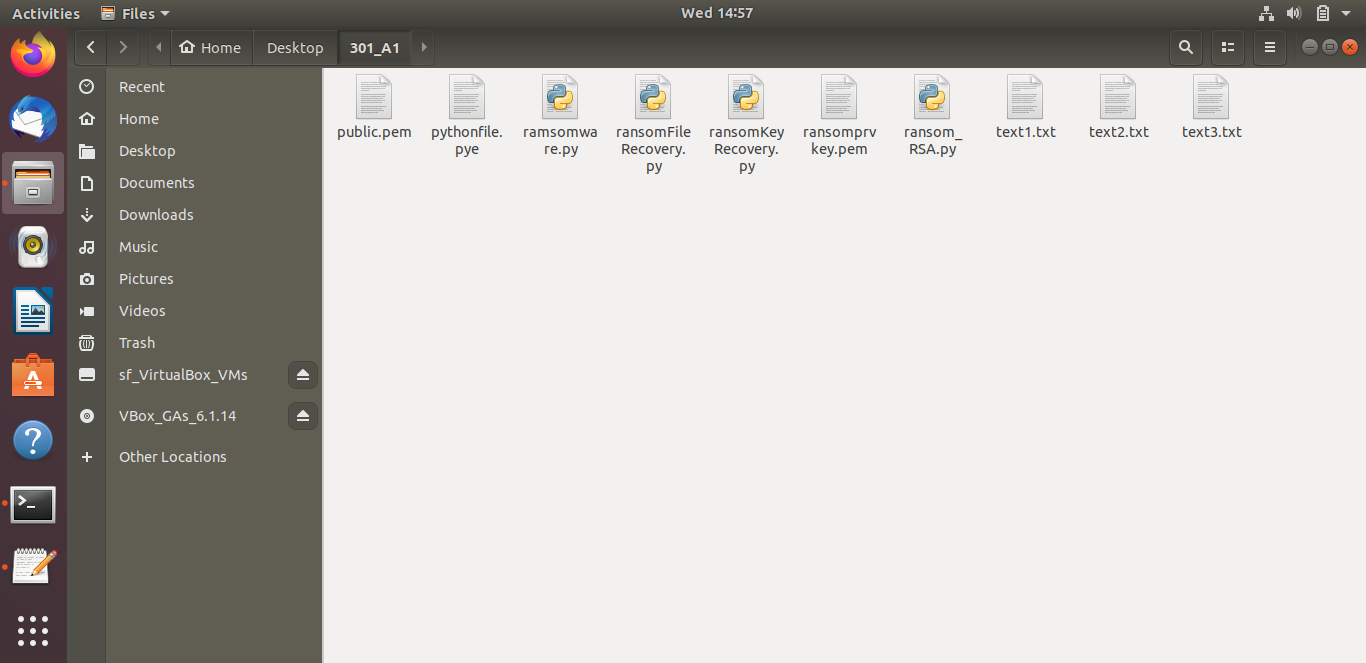
**Assignment 1 Brief:**

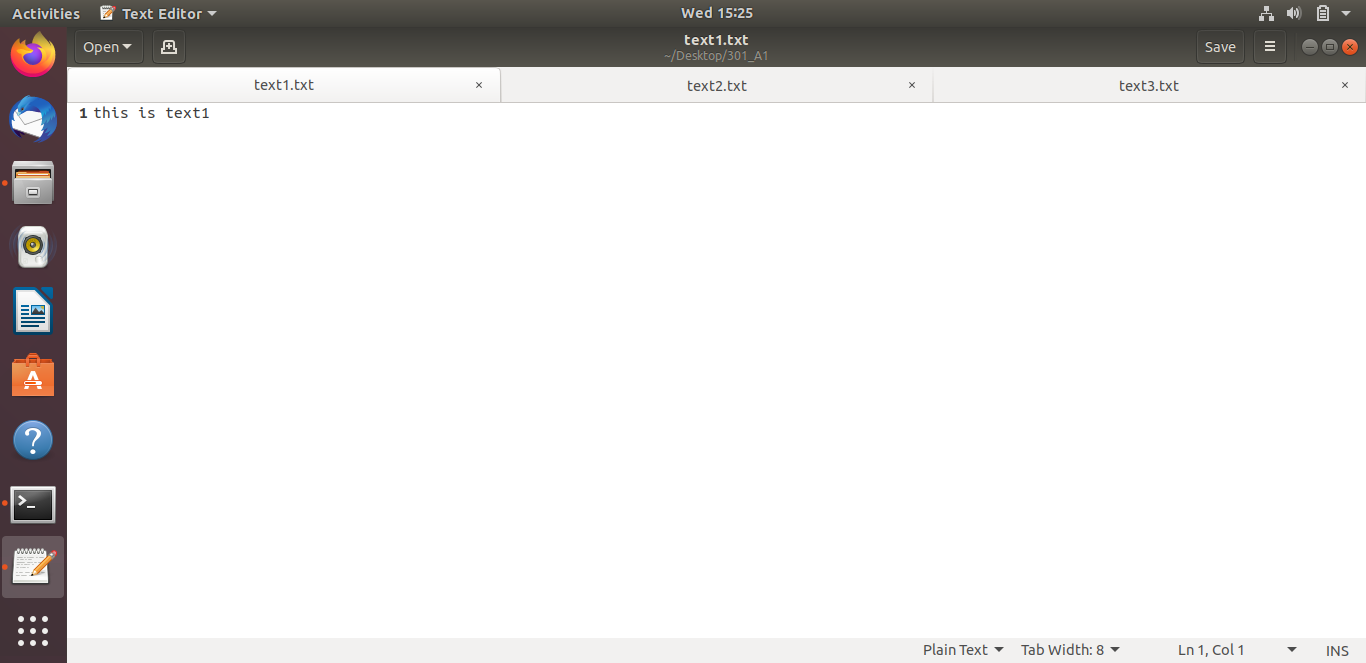
1. Copy the folder “301\_A1” into Ubuntu desktop and set current directory to cd Desktop/301\_A1

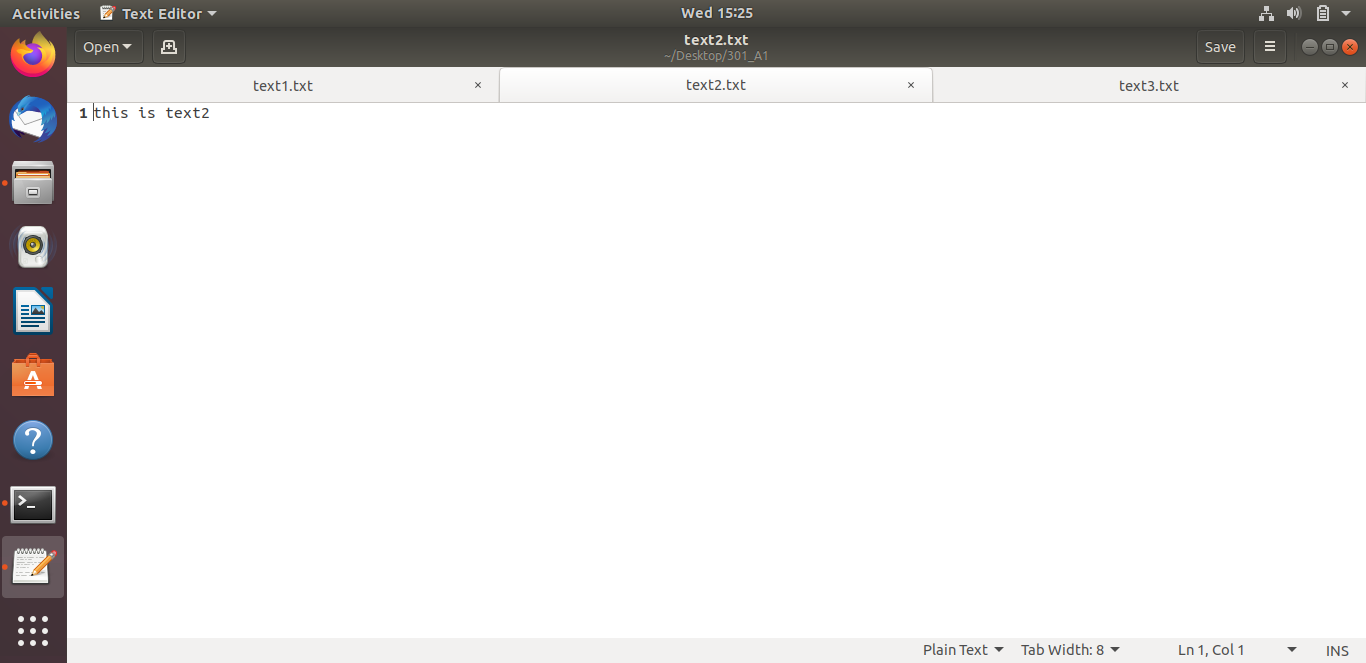


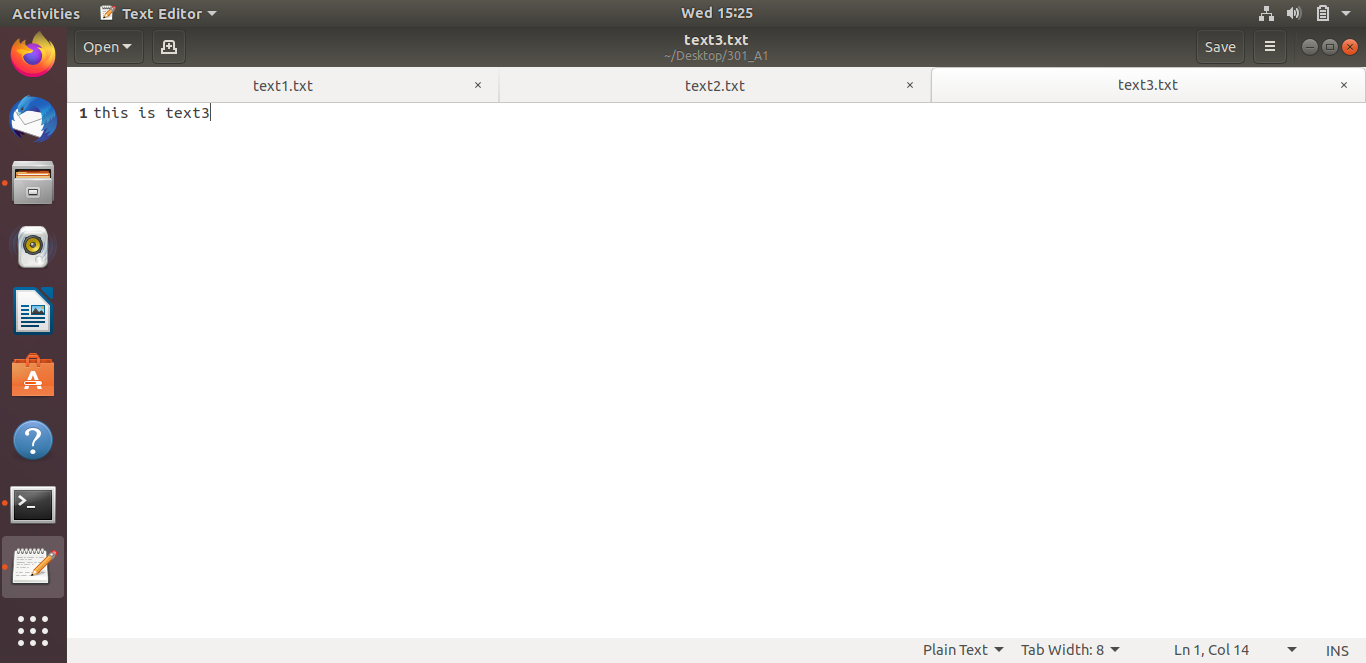
These are the files in the folder 301\_A1. It contains 2 .pem files(public and private keys) 1 pye file,4 python files and 3 txt files. “ransomKeyRecovery.py” and “ransomFileRecovery.py” are the recovery programs.



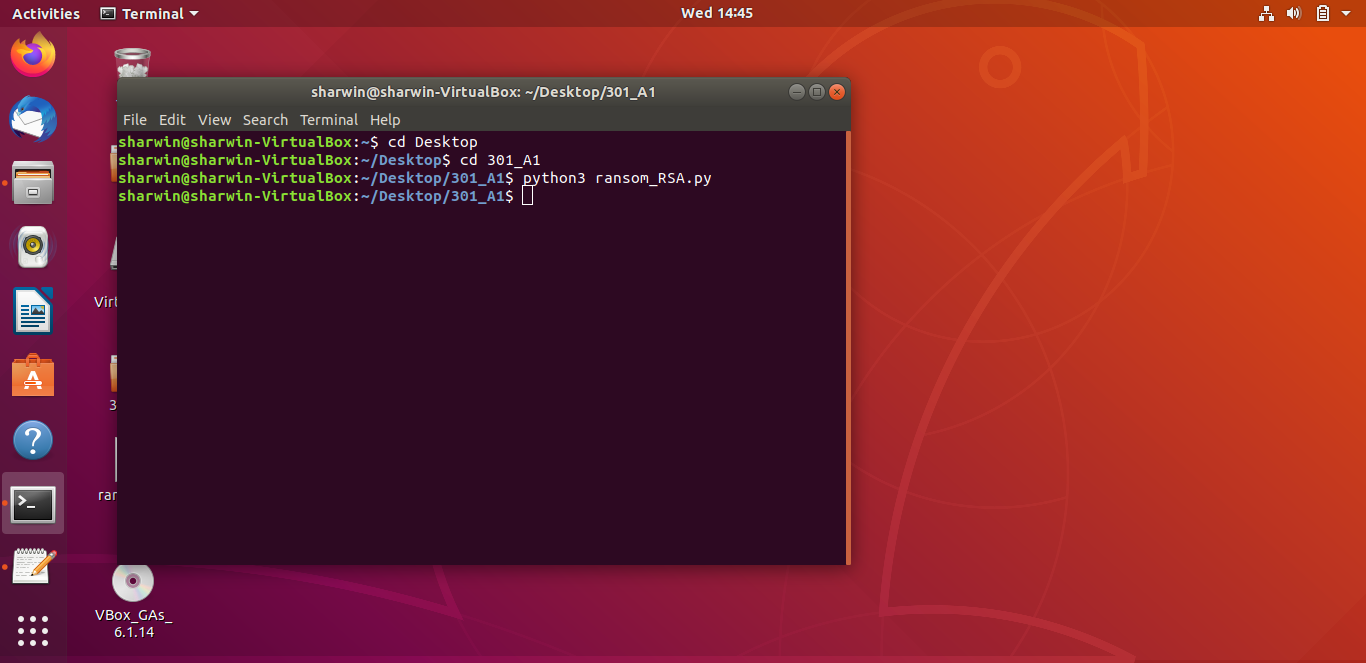
Original data in the text1.txt,text2.txt,text3.txt

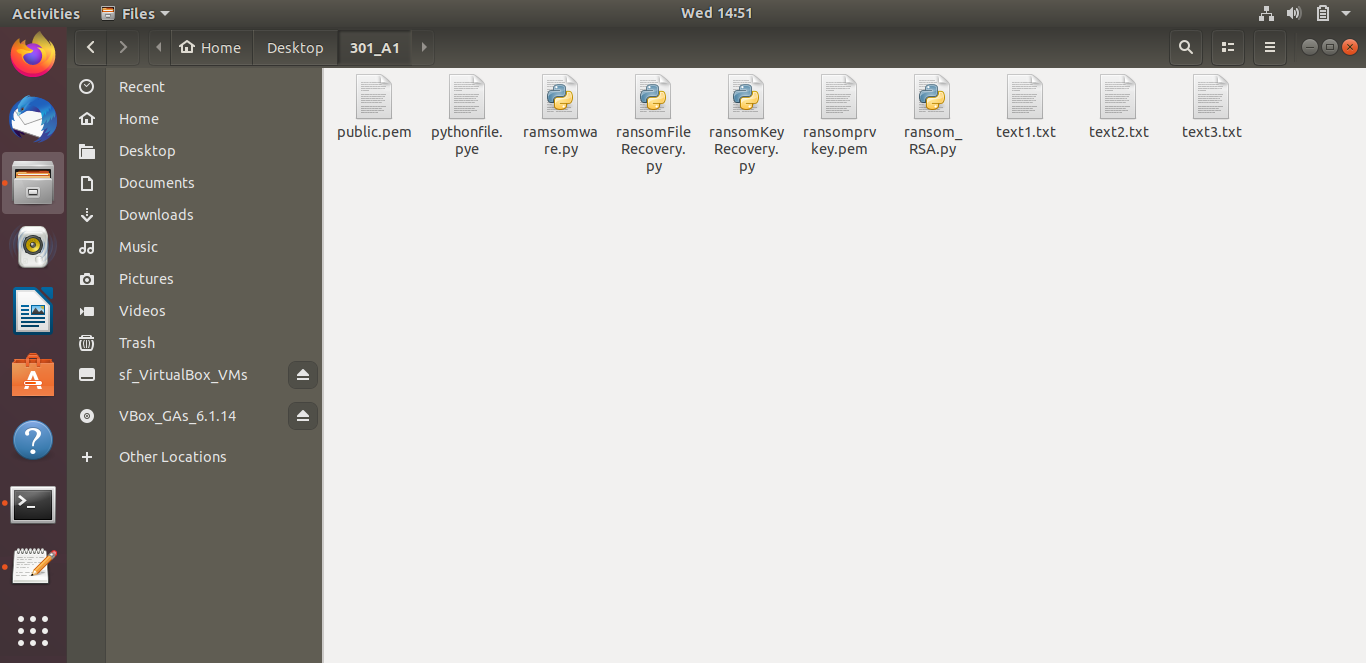






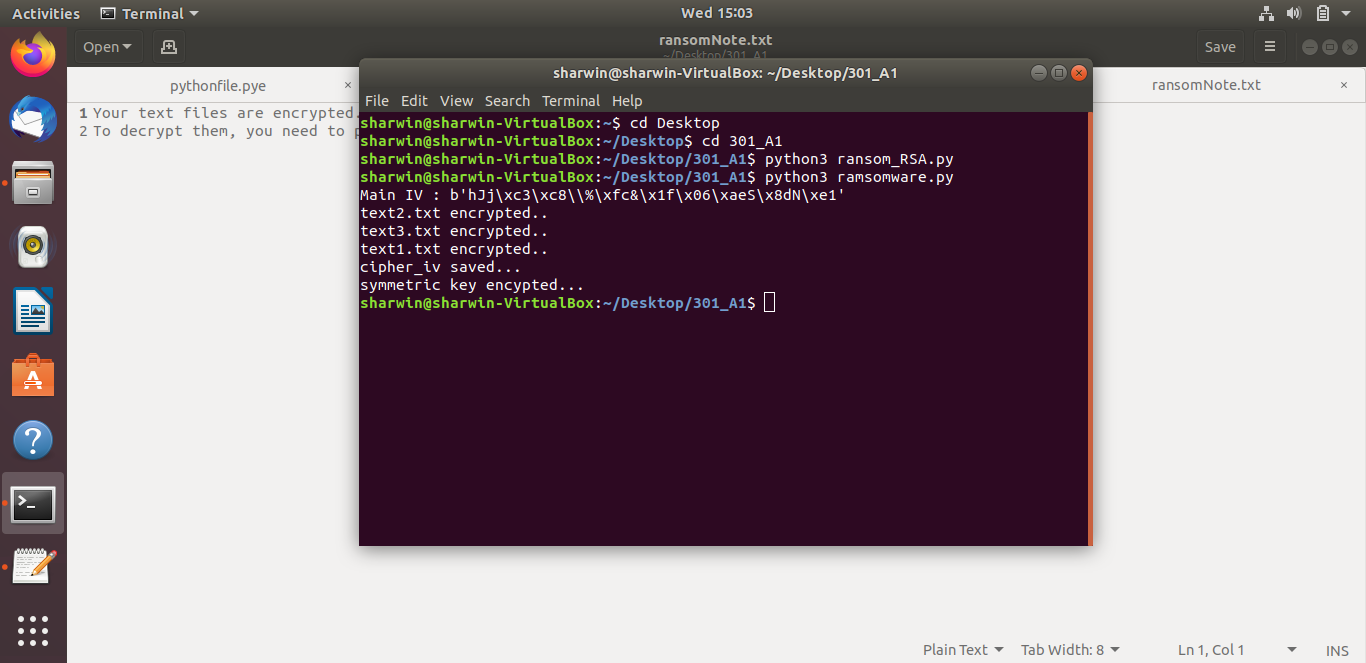
When we run the “ransom\_RSA.py” to generate the public and private keys by the command “python3 ransom\_RSA.py”. It will create 2 files, “public.pem” and”ransomprvkey.pem”.



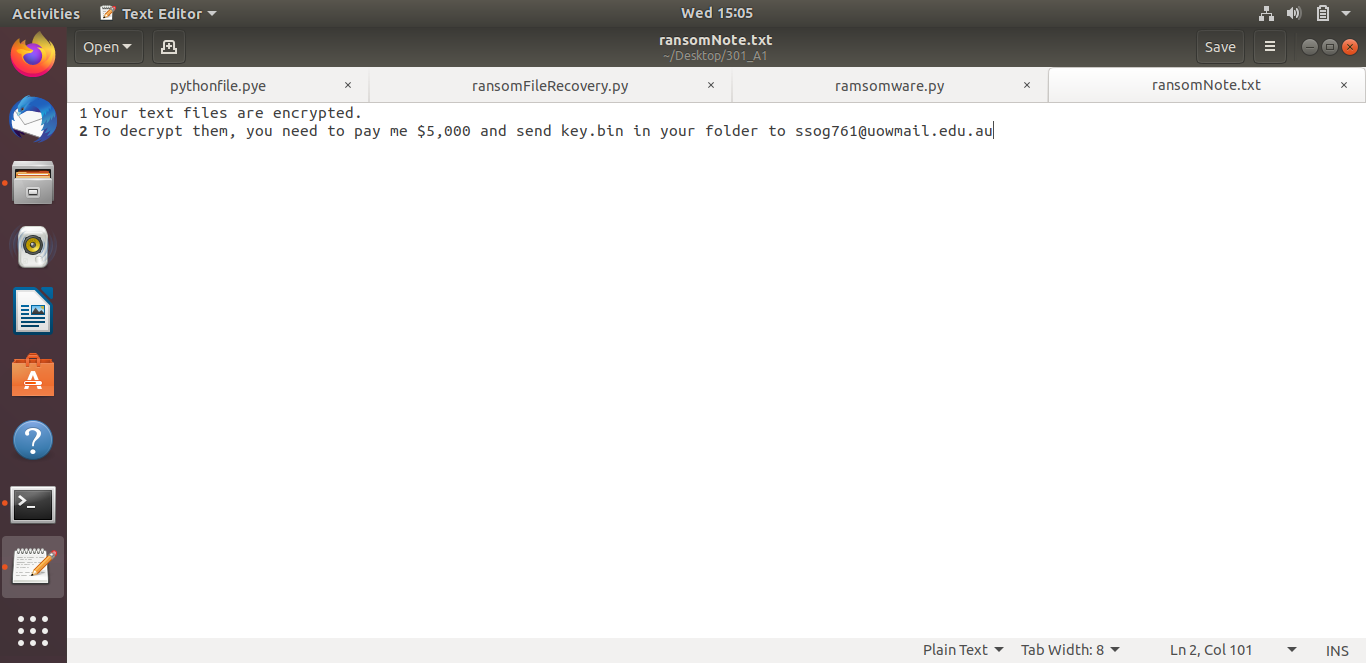


**Running the ransomware program(ENCRYPTION)**

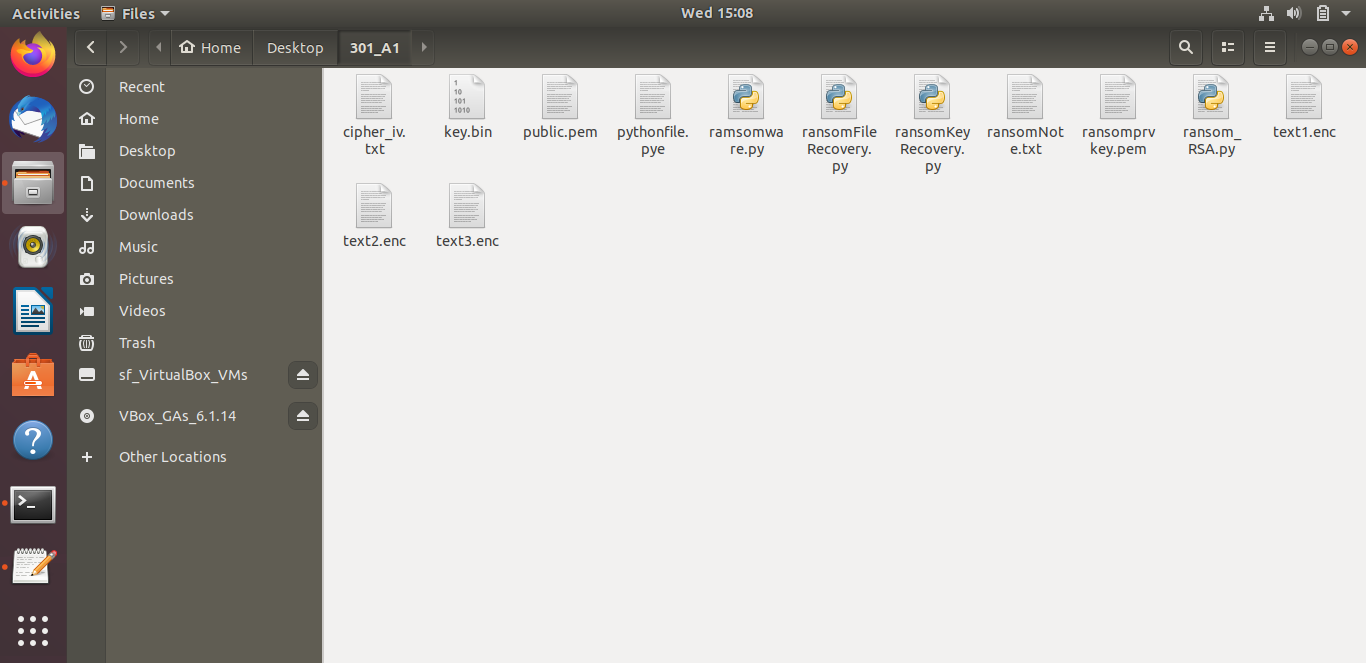
1)First, we run “ramsomware.py”(cd python3 ramsomeware.py) to encrypt the 3 .txt files, replicate the ransomware program to the “pythonfile.pye” with its contents commented. It will also generate a “key.bin” containing the encrypted AES key as well as “cipher\_iv.txt” containing the IV.



A text editor will be generated containing the ransom note

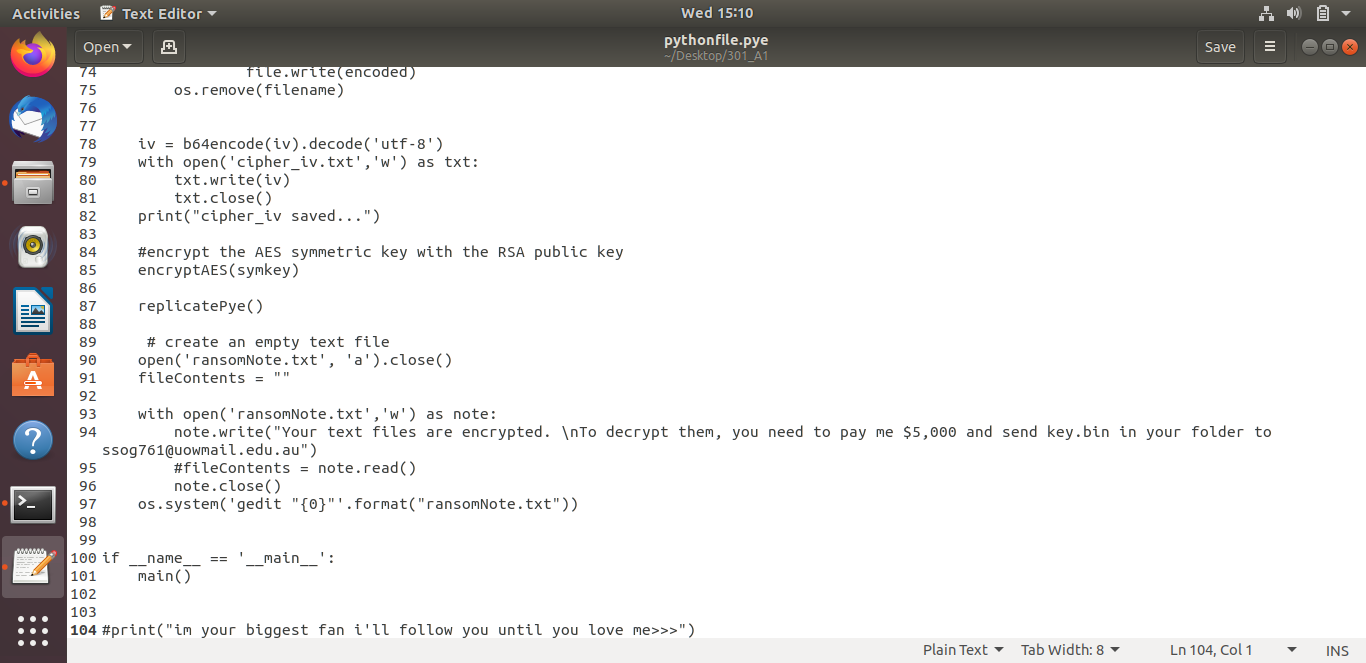


These are the files in the “301\_A1”folder upon running “ransomware.py”.Note that the .txt files have been changed to .enc and its data encrypted. “pythonfile.pye” has also been modified.

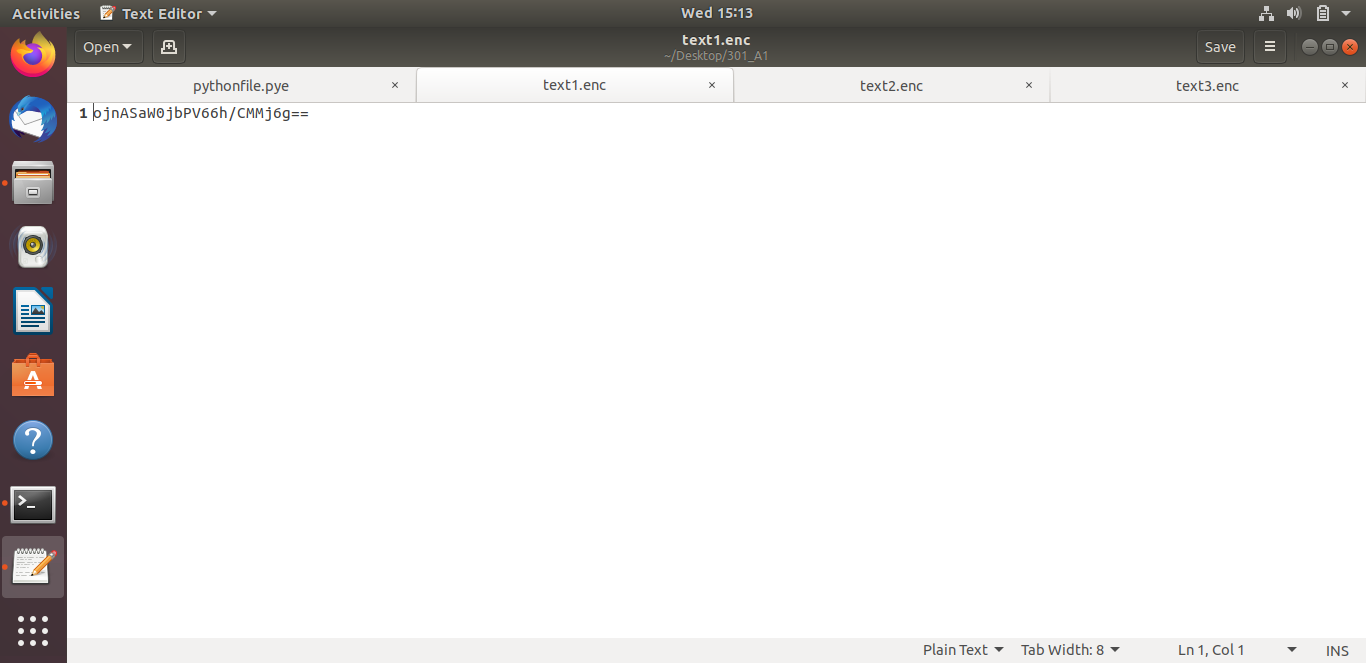


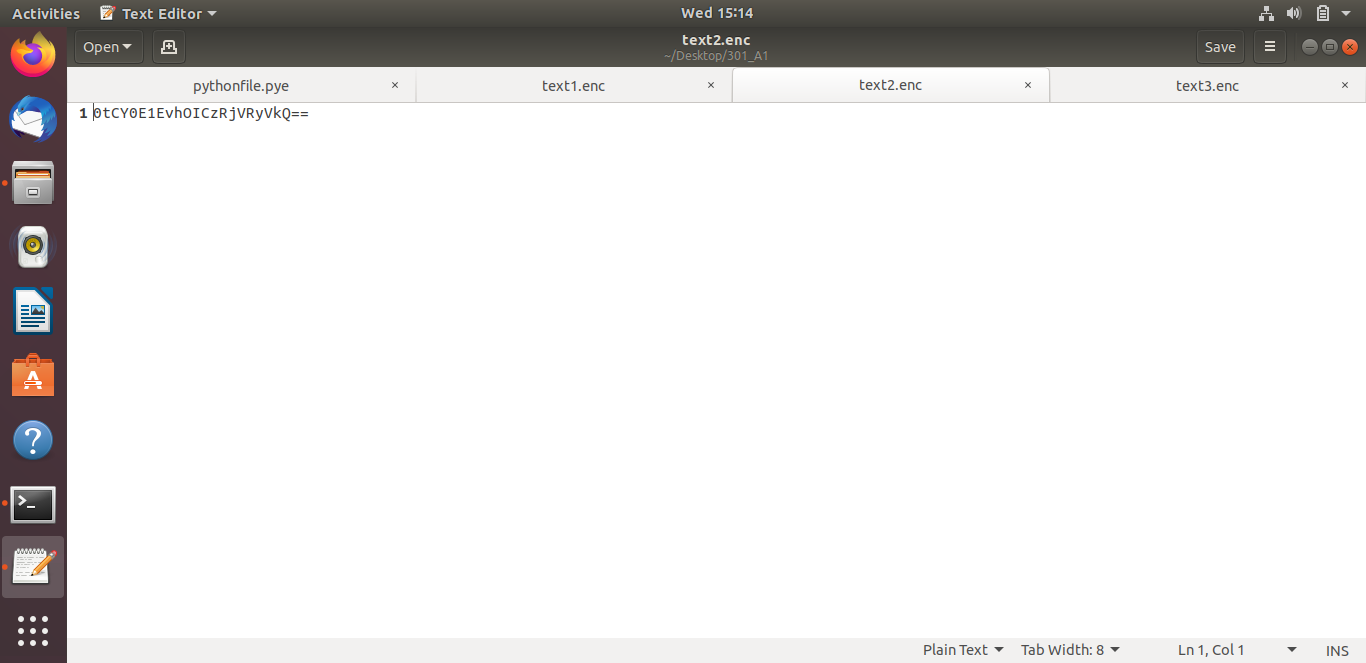
pythonfile.pye

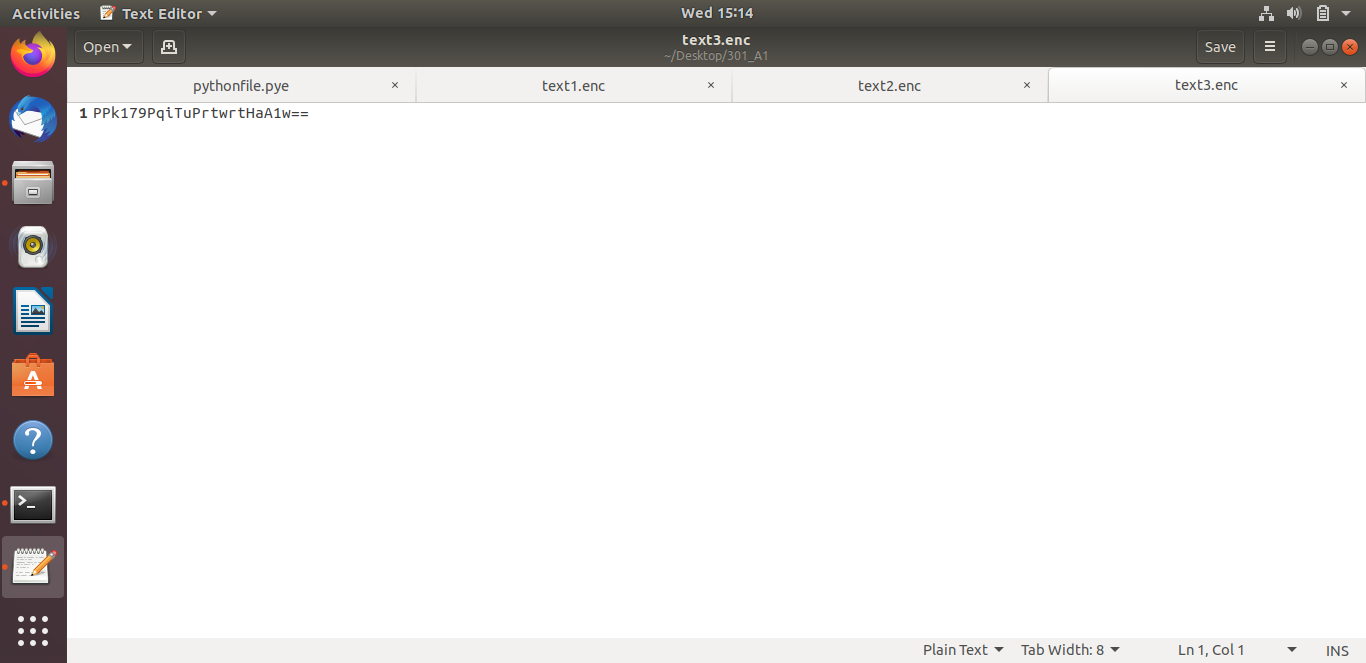




encrypted text file

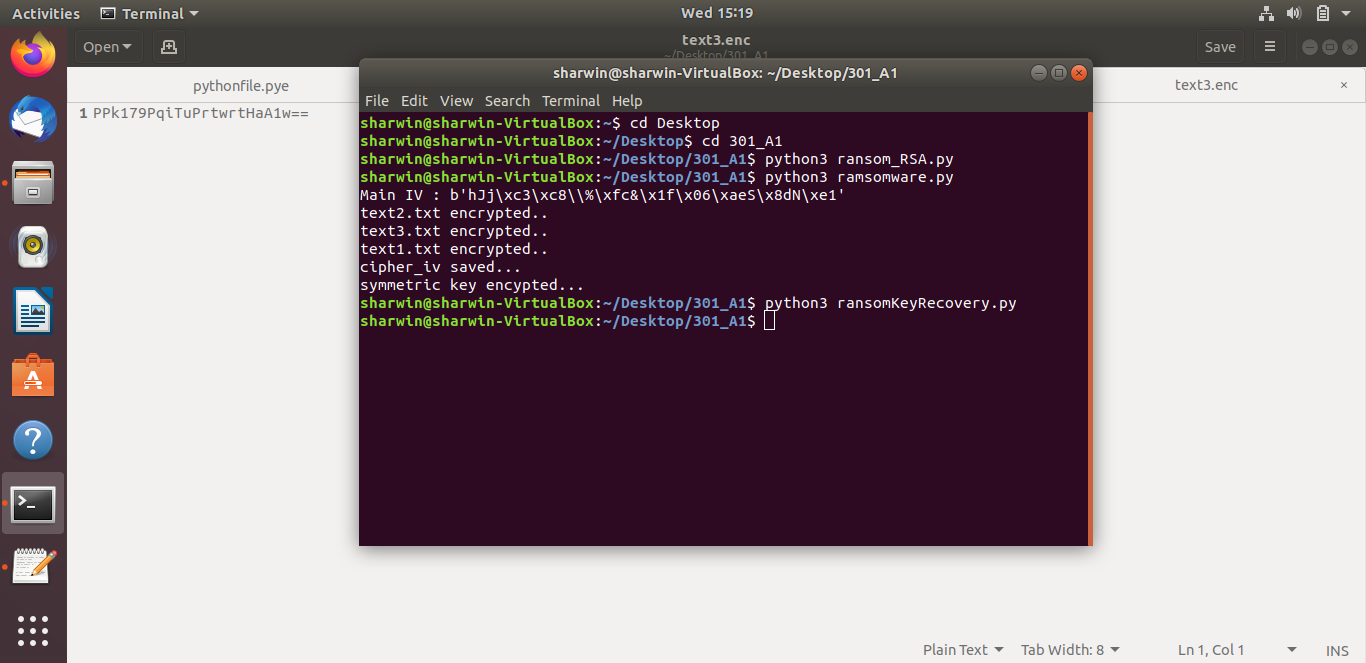




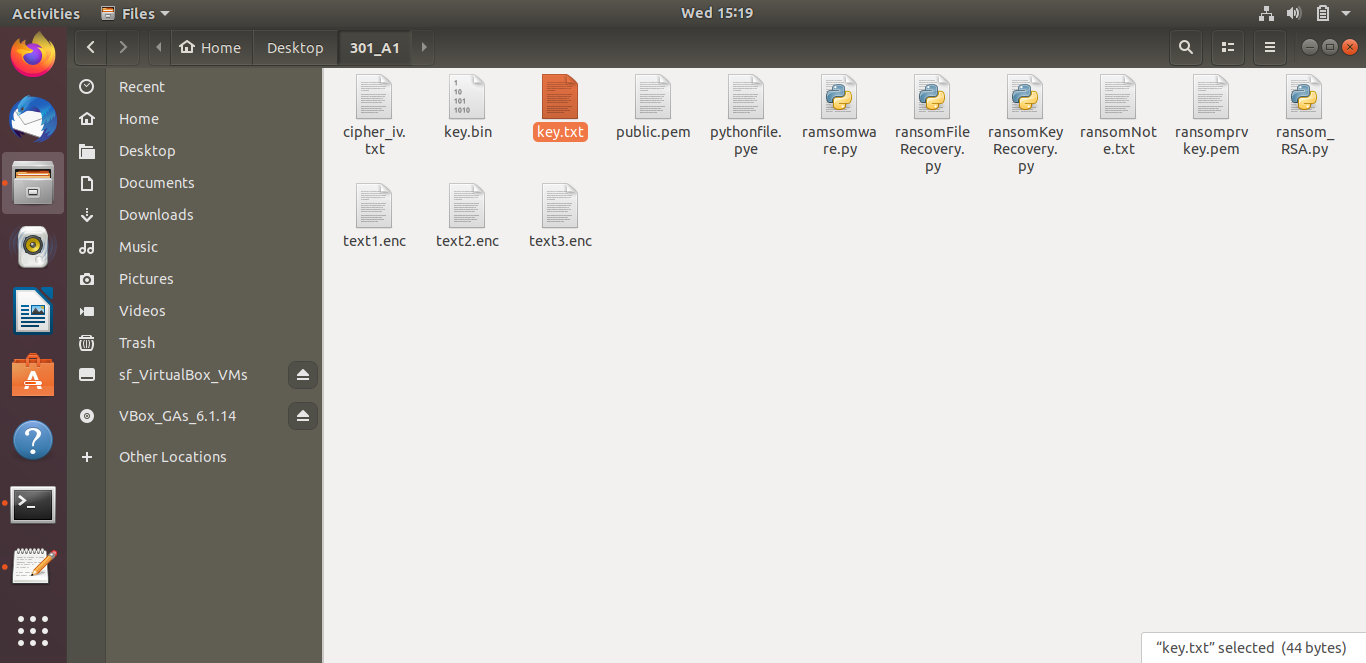


**Runnning the recovery programs(DECRYPTION)**

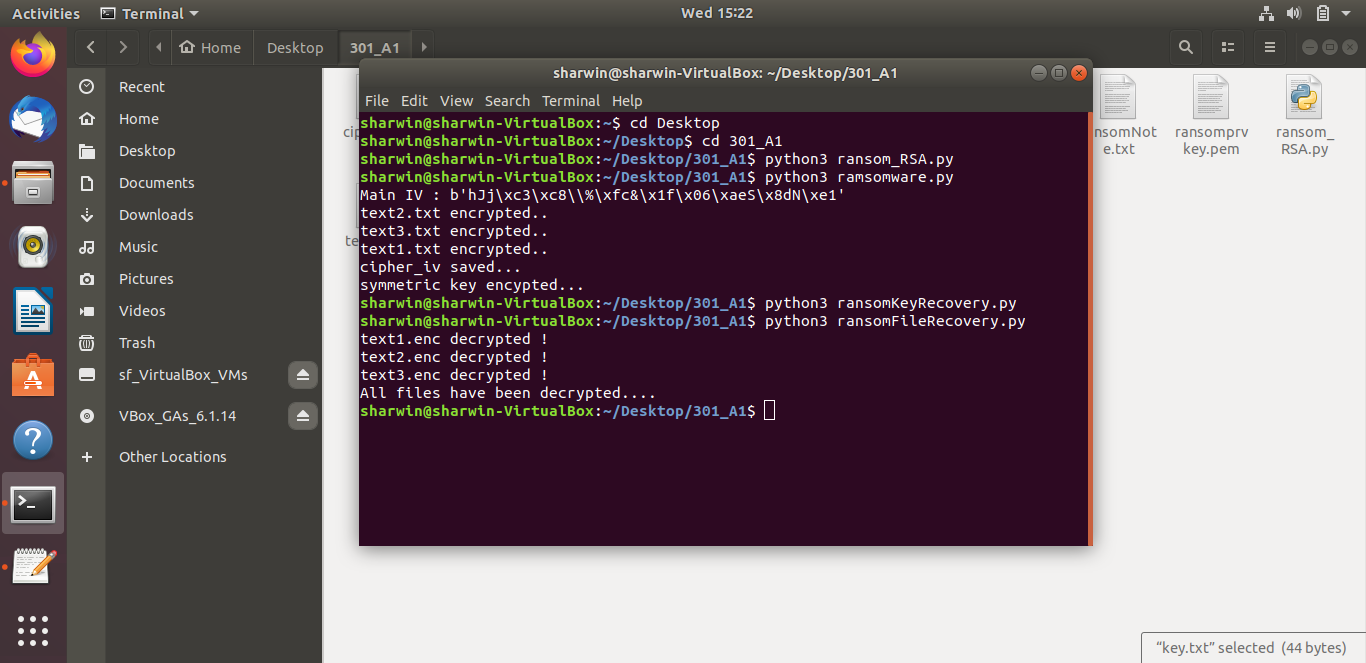
First run “ransomKeyRecovery.py”.This file will decrypt the AES key from “key.bin” and saves the key into a file called “key.txt”

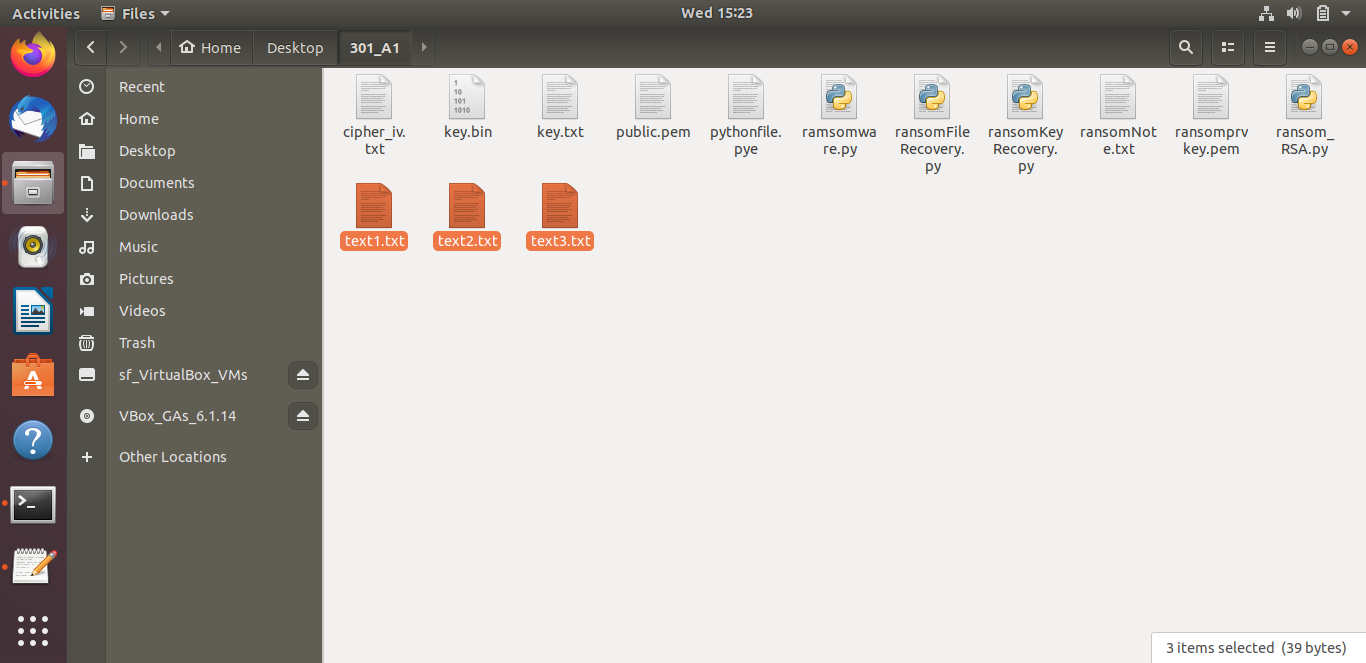


“key.txt” is in the 301\_A1 folder



Next we run “ransomFIleRecovery.py” to decrypt the encrypted text files. The .enc files will be changed to its original data





File data have be decrypted

