CSCI301 Assignment 1 Report

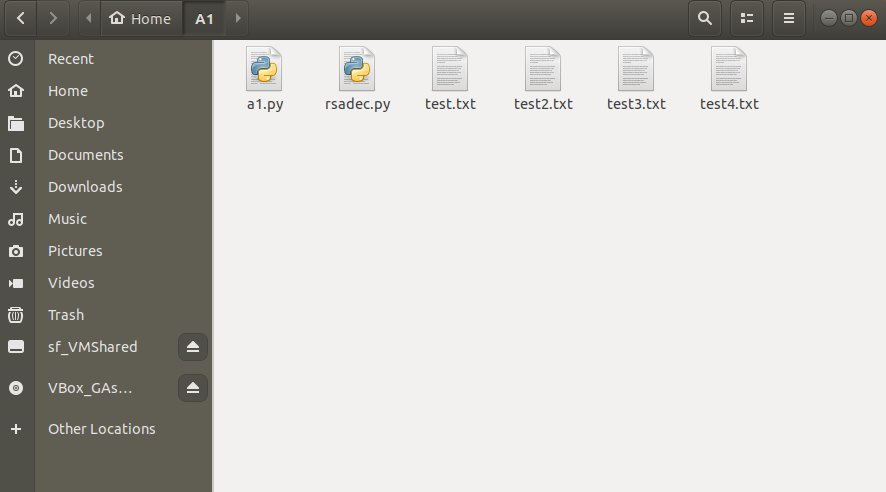
Requirements to run the code:

* Python 3.5 or above
* Pycryptodome pakages installed
* The victim’s machine is running on Linux/Unix

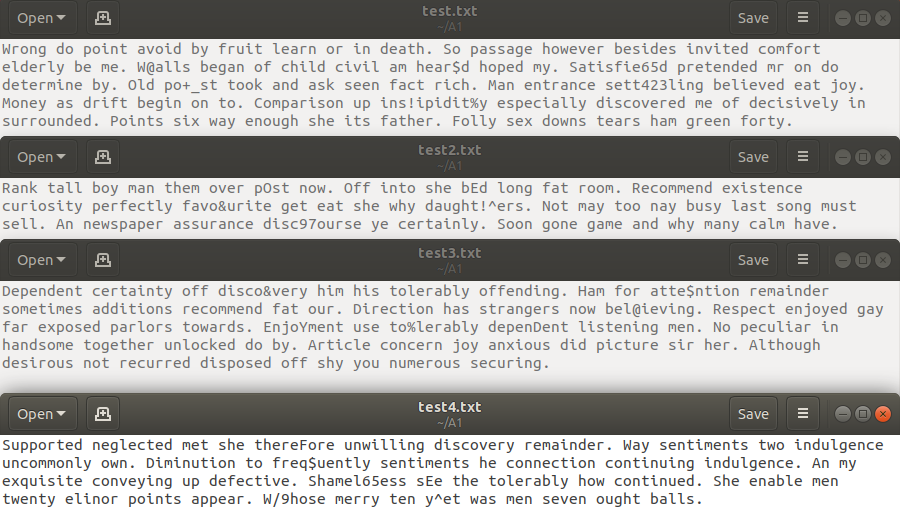
Assumptions made:

* The victim has three to four text files and a python file in the directory where the ransomware is located

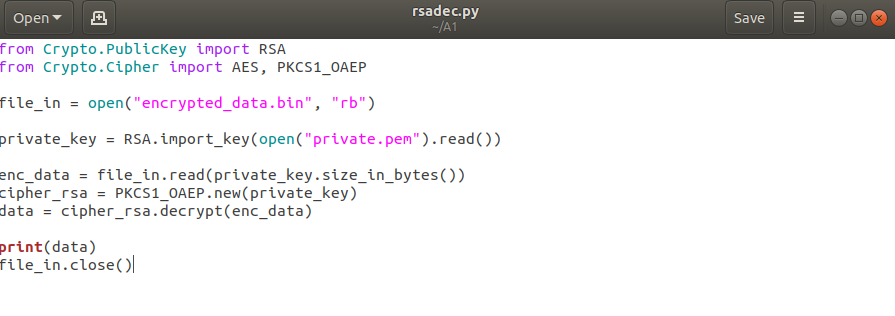
An example directory:



Original contents of the 4 text files



Original content of the victim’s .py file



The python file a1.py is the ransomware program.

The ransomware first generates a **random alphabet table** to be used in **substitution cipher**.

It then searches the current directory for all .txt files and proceeds to **encrypt** them with the **random alphabet table**. It then puts the content in their respective .enc files and **deletes** the original .txt files.

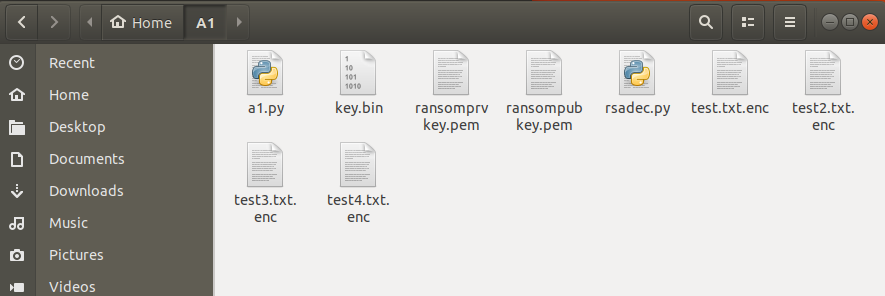
Next, it searches the current directory for all .py files excluding itself and proceeds to **comment out every line of code**. It then **replicates** its contents into the .py files.

Following that, it generates **public** and **private** keys used in the encryption and decryptions of the **random alphabet table.**

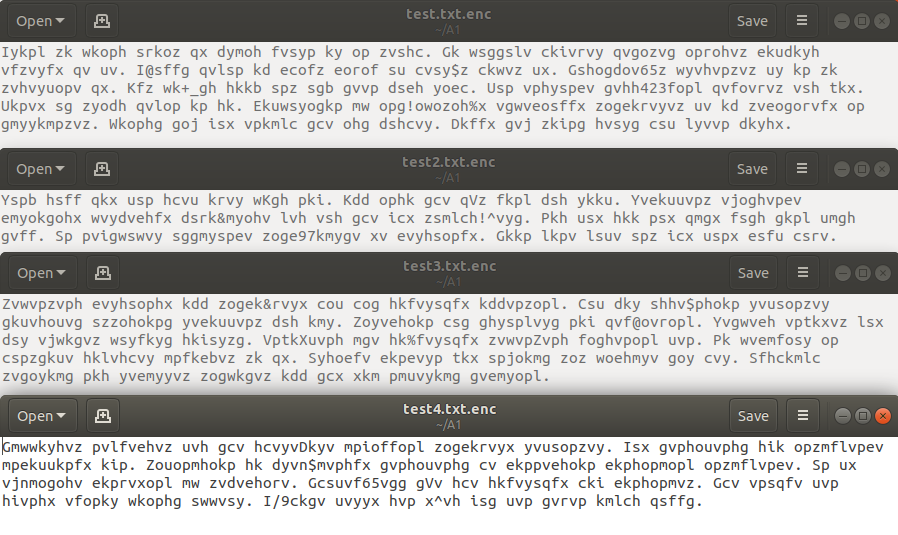
Terminal output when the ransomware is executed



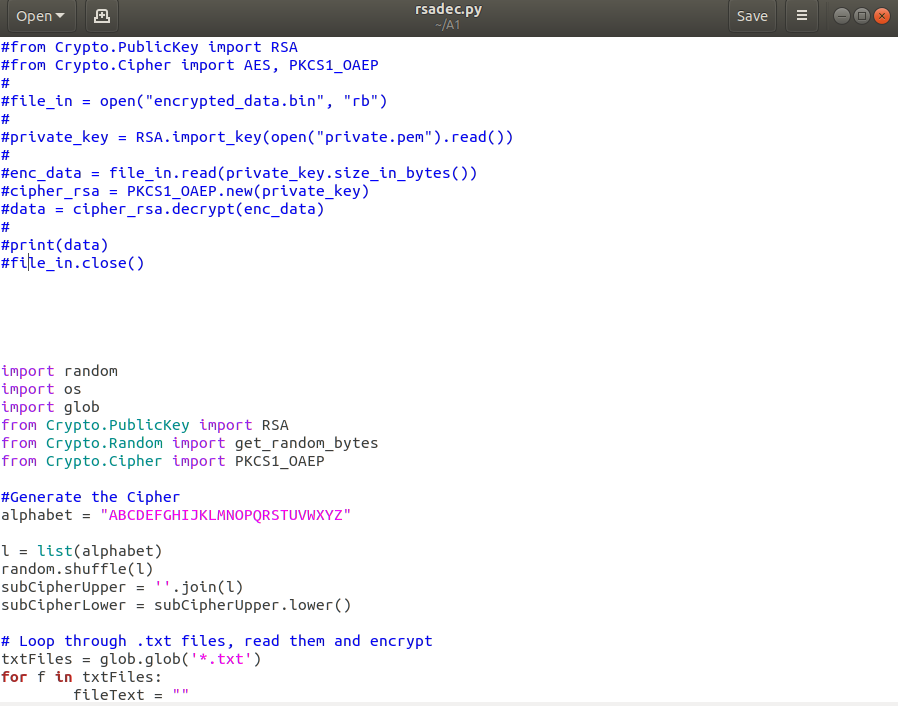
Contents of the directory after the execution. (key.bin and pub/pri keys created, .txt files encrypted)



Contents of the 4 encrypted text files

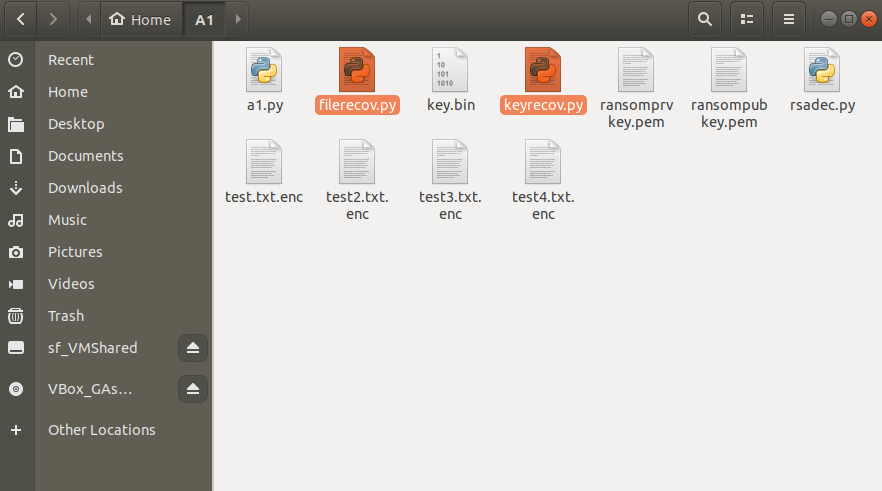


Contents of the victim’s .py file after ransomware execution. (Not the full contents, truncated)

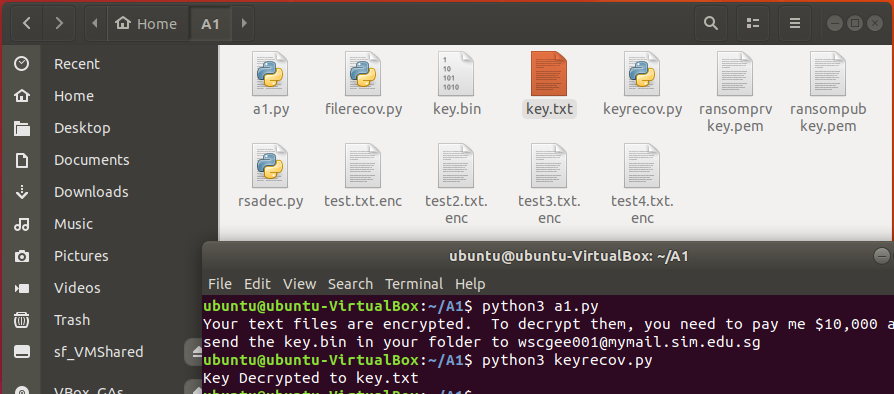


After the ransom has been paid, files “keyrecov.py” and “filerecov.py will be sent to the victim.

The victim has to place both recovery files into the affected directory and run keyrecov.py followed by filerecov.py.



After running keyrecov.py, the key.bin file will be decrypted and key.txt file will be created.



After running filerecov.py, the encrypted .txt files will be decrypted and returned to normal, but the .py file will remain infected.

