

# Report for Assignment 1 CSCI 301

Name:Jahir Hussain Mohamed Risvanudeen

Tutorial group:2

UOWID:6743511

## Pre-requisites

There is no need for additional packages or software, python3 with pycryptodome would suffice.

## Test.txt

This would be the file that we would be encrypting today.

The ransomware should perform the following:

- 1) It generates a 256 bits random key for symmetric encryption using AES\_CBC.
- 2) It encrypts all .txt files to .enc files in the current directory using the key that the attacker generated in step 1). The files in the other folders or the files in the same folder but having different file extensions must not be impacted by the ransomware.
- 3) It comments out all the content of the existing .pye file in the target folder (do not delete the content) and replicates itself to the .pye file for the further propagation.
- 4) The key in step 1) is encrypted to key.bin using public key encryption.
- 5) It will finally display a message for asking ransom "Your text files are encrypted.To decrypt them, you need to pay me \$5,000 and send key.bin in your folder to [me]." "[me]" should be your student email address.

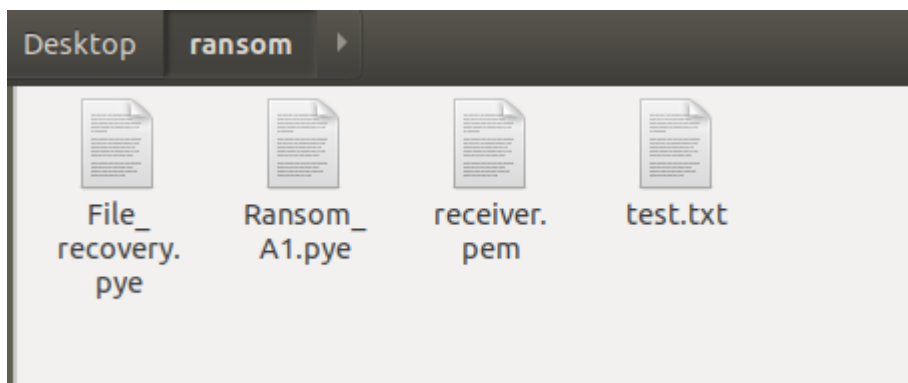
Your next task is to write programs, key-recovery and file-recovery programs that recover (decrypt) all the encrypted files if the victim pays the ransom.

- 6) The key-recovery program decrypt the encrypted key (key.bin) and encode the decrypted key to base64 and store it in key.txt.

- 7) The file-recovery program must allow a user to decrypt the encrypted files created in step 2) using the key file created in 6). You do not need to recover the infected .pye file in step 3).

## Ransomware virus and encryption of test.txt

Firstly, Run the "Ransom\_A1.pye" in the location that you desire.



For my example , I am going to run the Ransom\_A1.pye at a folder called ransom with test.txt inside , as well as the public key file called "receiver.pem" inside the same folder.The File\_recovery.pye is located there so that the victim can use it to decrypt the file in the future.

Outcome is as follows:

```
root2-VirtualBox:~/Desktop/ransom$ python3 Ransom_A1.pye
Your text files are encrypted. To decrypt them, you need to pay me $5,000 a
nd send key.bin in your folder to jahirhm001@mymail.sim.edu.sg
root2@root2-VirtualBox:~/Desktop/ransom$
```

Furthermore , the file Ransom\_A1.pye would be commented off at the top and at the bottom of the file.

Top:

```
Ransom_A1.pye
"""
```

```
from base64 import b64encode
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad
from Crypto.Random import get_random_bytes
import os
from Crypto.PublicKey import RSA
```

Bottom:

```
f.write( "\\ \\ \\ + \\ " )
f.write(sourcecode)
f.write("\\ \\ \\ \" + \\ n")
f.close()
```

```
"""
```

The following is how “test.enc” looks like. It is the encrypted version of “test.txt”:



The following is how “key.bin” looks like. Just like “test.enc” it is encrypted, but this time with RSA encryption and instead of the text file , it contains the key and iv of the encrypted “test.enc” file.



## Key recovery program

Next, we would want to recover our key and iv from “key.bin” , and to do that , we use “Key\_recovery.pye”.

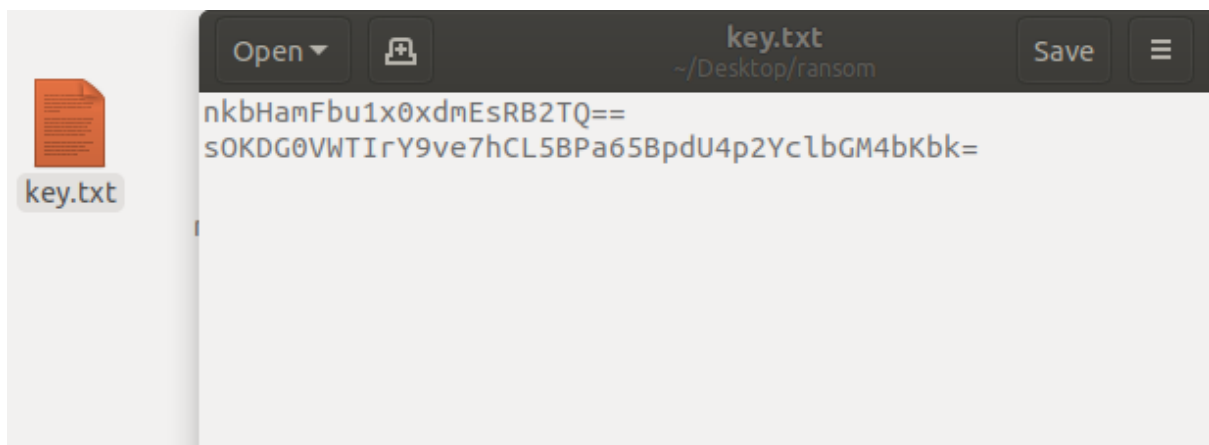
Following is the outcome:

```
root2@root2-VirtualBox:~/Desktop/ransom$ python3 Key_recovery.pye
Locate "key.bin":
key.bin
Locate "ransomprvkey.pem":
ransomprvkey.pem
"key.bin" is recovered and it is now called "key.txt"
root2@root2-VirtualBox:~/Desktop/ransom$
```

First of all ,we locate the “key.bin” and the “ransomprvkey.pem”. For convenience sake , I have placed the “key.bin” and the “ransomprvkey.pem” in the same folder as “Key\_recover.pye” , but if the location were different , do type out its exact location so that the program could capture. Incorrect location would result in the prompting of location of the files once again with an error message. Incorrect or corrupted file however , would result in termination of the program with an error message as well.

Secondly , we see that our “key.bin” has been recovered and it would now be called “key.txt” as we have transferred the data over to that file.

Following is how it would look like:



Now , we give this “key.txt” to the victim to retrieve his or her “test.txt”.

## File recovery program

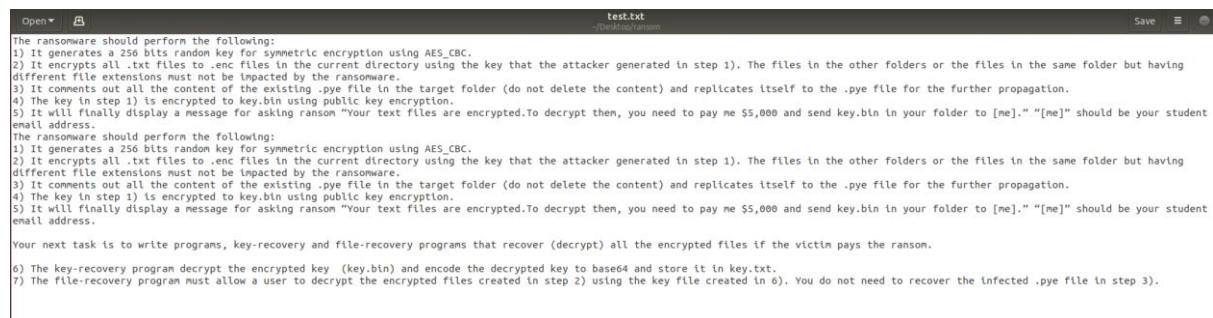
Next , with the “key.txt” we decrypt our file , so we run the “File\_recovery.pye”.

Following is the outcome:

```
root2@root2-VirtualBox:~/Desktop/ransom$ python3 File_recovery.pye
Locate "key.txt":
key.txt
Your files are decrypted! Good luck and good bye!
```

Firstly , we locate the “key.txt” and similar to the “Key\_recovery.pye”, incorrect location would result in an error message and prompting of the location of the file once again with an error message, and incorrect file would lead to termination of program with an error message.

And finally ,we are able to decrypt our encrypted file from “test.enc” to “test.txt” , results are as follows:



The screenshot shows a text editor window titled 'test.txt'. The content is a ransomware script. It starts with a list of steps: 1) It generates a 256 bits random key for symmetric encryption using AES\_CBC. 2) It encrypts all .txt files to .enc files in the current directory using the key that the attacker generated in step 1). The files in the other folders or the files in the same folder but having different file extensions must not be impacted by the ransomware. 3) It comments out all the content of the existing .pye file in the target folder (do not delete the content) and replicates itself to the .pye file for the further propagation. 4) The key in step 1) is encrypted to key.bin using public key encryption. 5) It will finally display a message for asking ransom "Your text files are encrypted.To decrypt then, you need to pay me \$5,000 and send key.bin in your folder to [me]." "[me]" should be your student email address. The script then repeats these steps. Below the steps, it says: "Your next task is to write programs, key-recovery and file-recovery programs that recover (decrypt) all the encrypted files if the victim pays the ransom." At the bottom, it says: "6) The key-recovery program decrypt the encrypted key (key.bin) and encode the decrypted key to base64 and store it in key.txt. 7) The file-recovery program must allow a user to decrypt the encrypted files created in step 2) using the key file created in 6). You do not need to recover the infected .pye file in step 3)." The text editor has a menu bar with 'Open', 'Save', and a search icon.

## Error handling

```
root2@root2-VirtualBox:~/Desktop/ransom$ python3 Key_recovery.pye
Locate "key.bin":
asda
Incorrect location of key.bin,renter location or press ctrl z to quit
Locate "key.bin":
key.bin
Locate "ransomprvkey.pem":
a
Incorrect location of ransomprvkey.pem,renter location or press ctrl z to quit
Locate "ransomprvkey.pem":
ransomprbkey.pem
Incorrect location of ransomprvkey.pem,renter location or press ctrl z to quit
Locate "ransomprvkey.pem":
ransomprvkey.pem
Files given are incorrect , please restart this program and provide the correct files
```

As stated earlier , in both files , users are prompted to give the correct location of the files once again upon entry of incorrect location of the files , and the program would result in termination if the user give incorrect files.

```
root2@root2-VirtualBox:~/Desktop/ransom$ python3 Ransom_A1.pye
reciver.pem was not found , please try again with receiver.pem in the same folder as Ransom_A1.pye
```

Likewise for missing “receiver.pem” file.

### **Summary of steps**

Step 1:

Run "python3 Ransom\_A1.pye" in the same folder as "receiver.pem".

Step 2:

Run "python3 Key\_recovery.pye"

Step 3:

Give location of "key.bin" and "ransomprvkey.pem"

Step 4:

Run "python3 File\_recovery.pye"

Step 5:

Give location of "key.txt" and make sure the encrypted files are within the same folder.

**Thank you**