“ File Encryption W/ AES ” 7/26/23

This lab is powered by
Windows 10 VM

Task : Successfully Encrypt the content of any file (.txt .png .ppk , etc..)
with a script in python *(Proof of concept, not for production)*

----------2 Part Lab (Encryption/Decryption)----------

Part 1 “Encrypt the file”

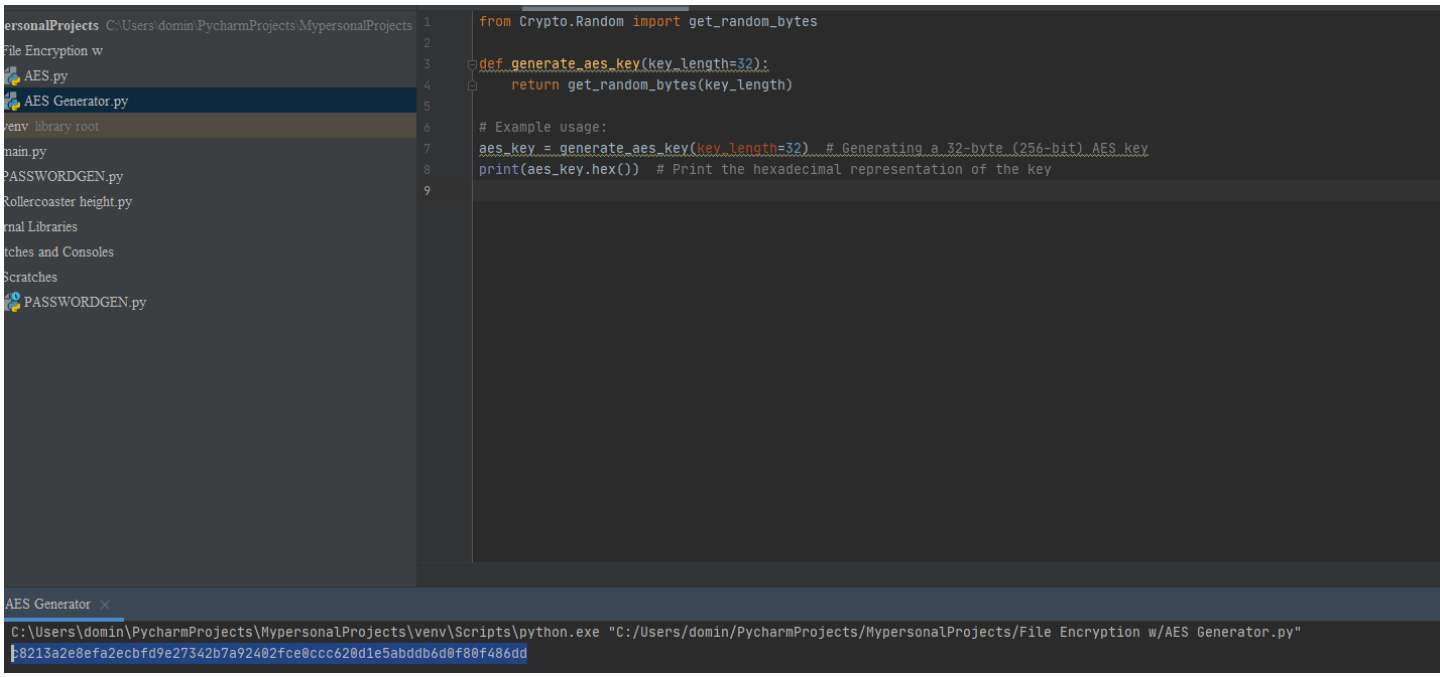
Step 1 : Install **pycryptodome** on python before beginning to write the script
You have to go into the “terminal option” on Pycharm, located on the bottom left

```
Terminal:   Local ×   +
Microsoft Windows [Version 10.0.22621.1992]
(c) Microsoft Corporation. All rights reserved.

(venv) C:\Users\domin\PycharmProjects\MypersonalProjects>pip install pycryptodome
Collecting pycryptodome
  Downloading pycryptodome-3.18.0-cp35-abi3-win_amd64.whl (1.7 MB)
     ---------------------------------------- 1.7/1.7 MB 2.0 MB/s eta 0:00:00
Installing collected packages: pycryptodome
Successfully installed pycryptodome-3.18.0

[notice] A new release of pip is available: 23.1.2 -> 23.2.1
[notice] To update, run: python.exe -m pip install --upgrade pip
```

Step 2 : Make a second .py file to have as a separate script to generate the key

You are going to take the output of that script (Encryption Key) and feed it into line 53

(this is what will be used to decrypt the file in part 2)

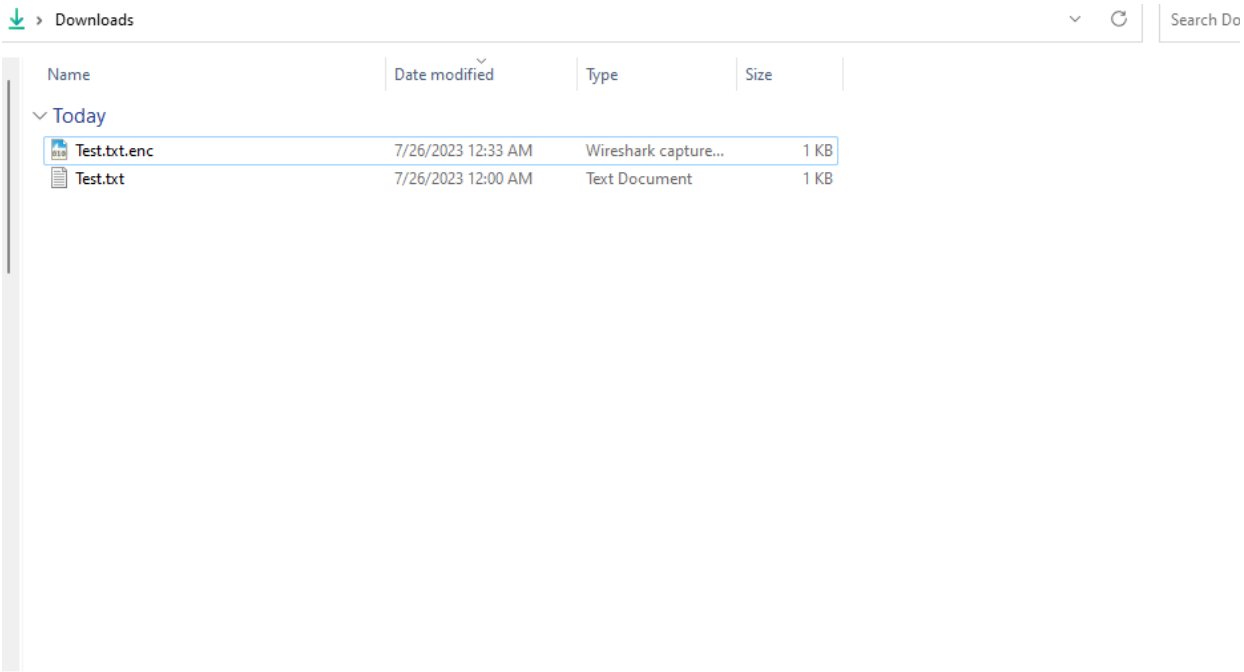


Step 3 : Take any file you want to encrypt and copy the path to it into line 56

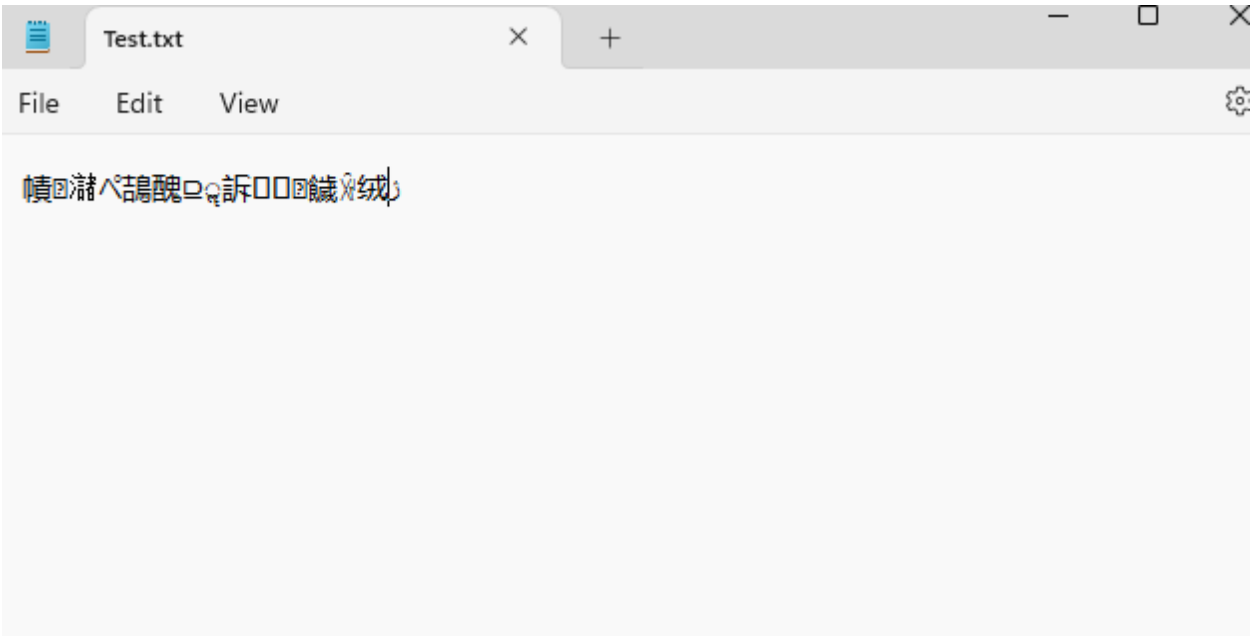
For windows, make sure you change all the backslashes “\” to forward slashes “/” or the script will fire off an error

Example : `C:/Users/domin/Downloads/Test.txt`

Step 4 : After the script was run successfully, it will make a new copy of the file with an added **.enc** to it, rename the file and take out that extension, then remove the original.



Step 5 : View the contents of the encrypted file



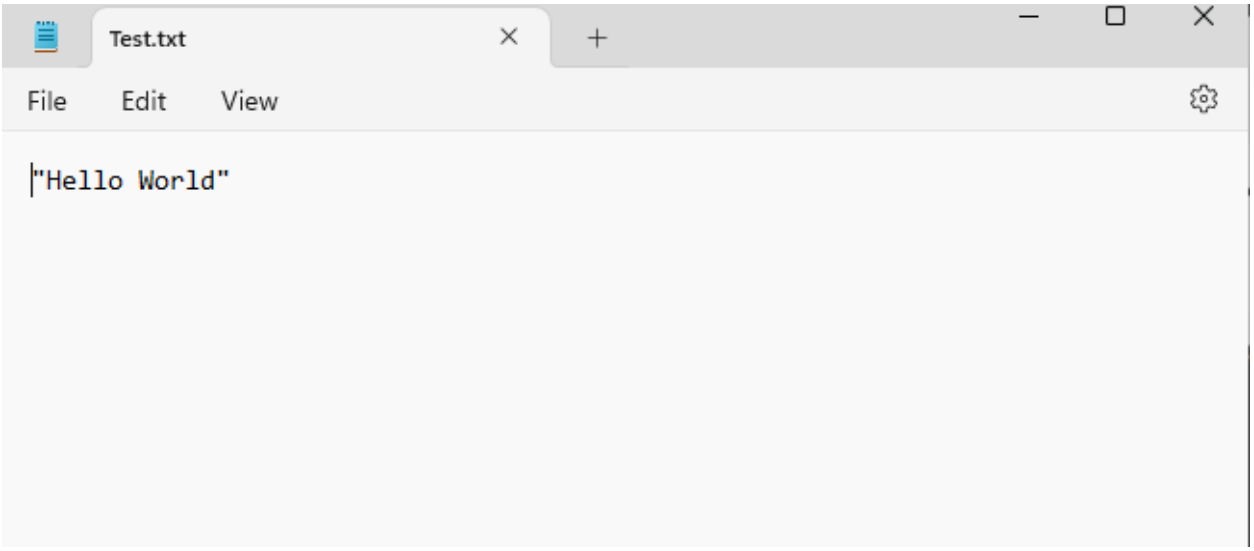
Part 2 “File Decryption”

Step 1 : Go back to the python script and uncomment lines 63-64, this will allow us to decrypt the file (You can also make the decryption script separate for ease of use)

```
61
62  # Decryption example
63  decrypt_file(encryption_key, 'C:/Users/domin/Downloads/Test.txt')
64  print("File decrypted.")
65
```

Run the script and view that the file is now back to it’s unencrypted form

```
C:\Users\domin\PycharmProjects\MypersonalProjects\venv\Scripts\python.exe "C:/Users/domin/PycharmProjects/Mype
File encrypted.
File decrypted.

Process finished with exit code 0
```



Optional : Ways the script can improve is by modifying the script to produce the encryption key with the file when you run it, and also to make a search for the user to input the directory of the file they want to encrypt