Hung Nguyen – Data Security Project 2

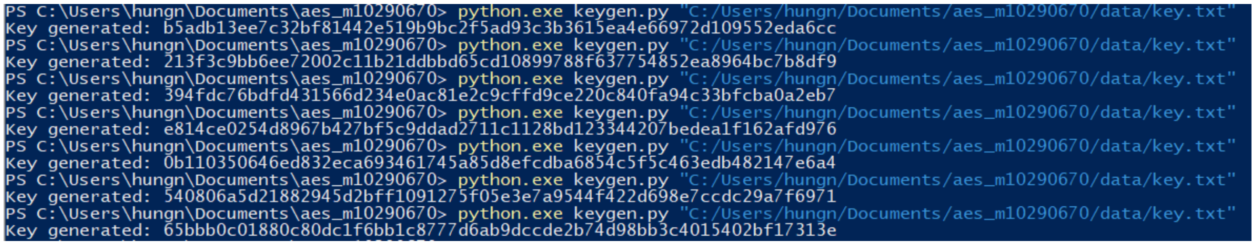
I. How to run:

1. **The following command calls and runs the key generation function:**

python.exe keygen.py "C:/Users/hungn/Documents/aes_m10290670/data/key.txt"

where the argument is the location of the key file.

Screenshot of the output of the keygen function:



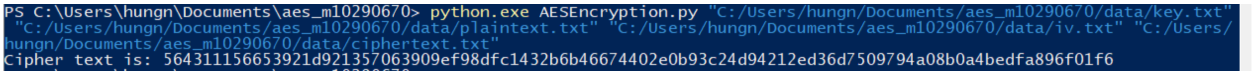
```
PS C:\Users\hungn\Documents\aes_m10290670> python.exe keygen.py "C:/Users/hungn/Documents/aes_m10290670/data/key.txt"
Key generated: b5adb13ee7c32bf81442e519b9bc2f5ad93c3b3615ea4e66972d109552eda6cc
PS C:\Users\hungn\Documents\aes_m10290670> python.exe keygen.py "C:/Users/hungn/Documents/aes_m10290670/data/key.txt"
Key generated: 213f3c9bb6ee72002c11b21ddbbd65cd10899788f637754852ea8964bc7b8df9
PS C:\Users\hungn\Documents\aes_m10290670> python.exe keygen.py "C:/Users/hungn/Documents/aes_m10290670/data/key.txt"
Key generated: 394fdc76bdfd431566d234e0ac81e2c9cffd9ce220c840fa94c33bfcba0a2eb7
PS C:\Users\hungn\Documents\aes_m10290670> python.exe keygen.py "C:/Users/hungn/Documents/aes_m10290670/data/key.txt"
Key generated: e814ce0254d8967b427bf5c9ddad2711c1128bd123344207bedea1f162afd976
PS C:\Users\hungn\Documents\aes_m10290670> python.exe keygen.py "C:/Users/hungn/Documents/aes_m10290670/data/key.txt"
Key generated: 0b110350646ed832eca693461745a85d8efcdba6854c5f5c463edb482147e6a4
PS C:\Users\hungn\Documents\aes_m10290670> python.exe keygen.py "C:/Users/hungn/Documents/aes_m10290670/data/key.txt"
Key generated: 540806a5d21882945d2bff1091275f05e3e7a9544f422d698e7ccdc29a7f6971
PS C:\Users\hungn\Documents\aes_m10290670> python.exe keygen.py "C:/Users/hungn/Documents/aes_m10290670/data/key.txt"
Key generated: 65bbb0c01880c80dc1f6bb1c8777d6ab9dccde2b74d98bb3c4015402bf17313e
```

2. **The following command calls and runs the encryption function:**

python.exe AESEncryption.py "C:/Users/hungn/Documents/aes_m10290670/data/key.txt" "C:/Users/hungn/Documents/aes_m10290670/data/plaintext.txt" "C:/Users/hungn/Documents/aes_m10290670/data/iv.txt" "C:/Users/hungn/Documents/aes_m10290670/data/ciphertext.txt"

This function takes 4 arguments: Location of the key file, location of the plaintext file, location of the IV file and location of the ciphertext file in that order.

Screenshot of the output of the encryption function:



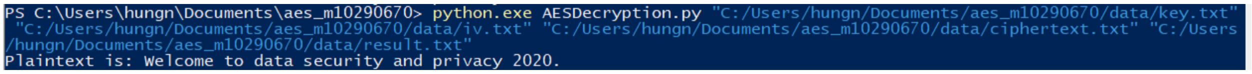
```
PS C:\Users\hungn\Documents\aes_m10290670> python.exe AESEncryption.py "C:/Users/hungn/Documents/aes_m10290670/data/key.txt"
 "C:/Users/hungn/Documents/aes_m10290670/data/plaintext.txt" "C:/Users/hungn/Documents/aes_m10290670/data/iv.txt" "C:/Users/
hungn/Documents/aes_m10290670/data/ciphertext.txt"
Cipher text is: 564311156653921d921357063909ef98dfc1432b6b46674402e0b93c24d94212ed36d7509794a08b0a4bedfa896f01f6
```

3. **The following command calls and runs the decryption function:**

python.exe AESDecryption.py "C:/Users/hungn/Documents/aes_m10290670/data/key.txt" "C:/Users/hungn/Documents/aes_m10290670/data/iv.txt" "C:/Users/hungn/Documents/aes_m10290670/data/ciphertext.txt" "C:/Users/hungn/Documents/aes_m10290670/data/result.txt"

This function takes 4 arguments: Location of the key file, location of the iv file, location of the ciphertext file and location of the result file in that order.

Screenshot of the output of the decryption function:



```
PS C:\Users\hungn\Documents\aes_m10290670> python.exe AESDecryption.py "C:/Users/hungn/Documents/aes_m10290670/data/key.txt"
 "C:/Users/hungn/Documents/aes_m10290670/data/iv.txt" "C:/Users/hungn/Documents/aes_m10290670/data/ciphertext.txt" "C:/Users
/hungn/Documents/aes_m10290670/data/result.txt"
Plaintext is: Welcome to data security and privacy 2020.
```