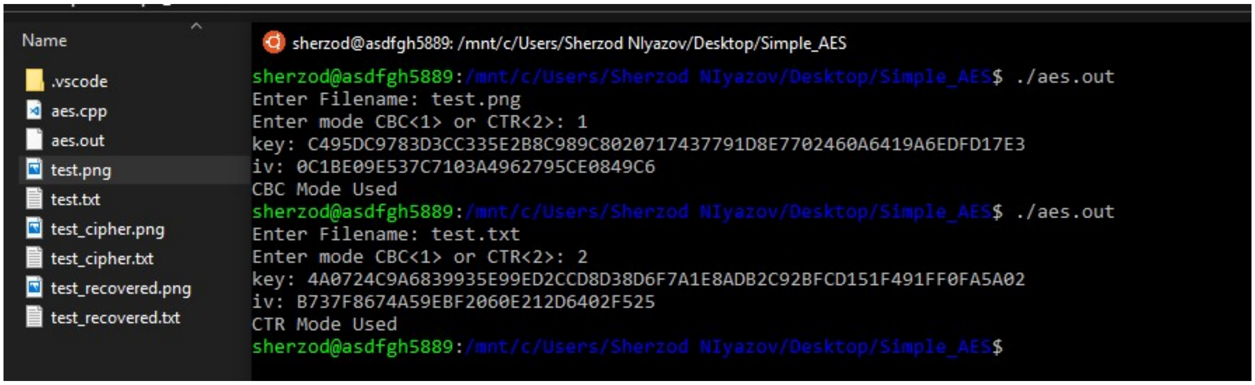
CS HW2. SIMPLE AES-256

U1510349
SHERZOD NIYAZOV

aes.out is Linux OS executable which is implemented with Crypto++ library for C++.

Usage: When your run aes.out you will be asked to enter file location to be encrypted. Then you have to enter AES encryption mode either CBC or CTR (enter 1 for CBC, 2 for CTR mode). After inputs are taken program encrypts file that was given and creates "<filename>_cipher" file in directory where application was run, which is encryption of file using AES-256 printed {key, iv}. Then it decrypts "<filename>_cipher" to "<filename>_recovered" file which will be stored in directory where program was run.

Here is snapshot from program:



```
sherzod@asdfgh5889:/mnt/c/Users/Sherzod NIyazov/Desktop/Simple_AES$ ./aes.out
Enter Filename: test.png
Enter mode CBC<1> or CTR<2>: 1
key: C495DC9783D3CC335E2B8C989C8020717437791D8E7702460A6419A6EDFD17E3
iv: 0C1BE09E537C7103A4962795CE0849C6
CBC Mode Used
sherzod@asdfgh5889:/mnt/c/Users/Sherzod NIyazov/Desktop/Simple_AES$ ./aes.out
Enter Filename: test.txt
Enter mode CBC<1> or CTR<2>: 2
key: 4A0724C9A6839935E99ED2CCD8D38D6F7A1E8ADB2C92BFCD151F491FF0FA5A02
iv: B737F8674A59EBF2060E212D6402F525
CTR Mode Used
sherzod@asdfgh5889:/mnt/c/Users/Sherzod NIyazov/Desktop/Simple_AES$
```

From snapshot, you can see that sample file "test.png" was used and CBC mode encryption was used. Then program created "test_cipher.png" which is encrypted file and "test_recovered.png" which is decrypted file.

From snapshot, you can see that sample file "test.txt" was used and CTR mode encryption was used. Then program created "test_cipher.txt" which is encrypted file and "test_recovered.txt" which is decrypted file.

If you want to build source code, you have to install crypto++ library to your system. For simple build you can use command:

```
g++ -g3 -ggdb -O0 -DDEBUG -I/usr/include/cryptopp aes.cpp -o aes.out -lcryptopp -lpthread
```