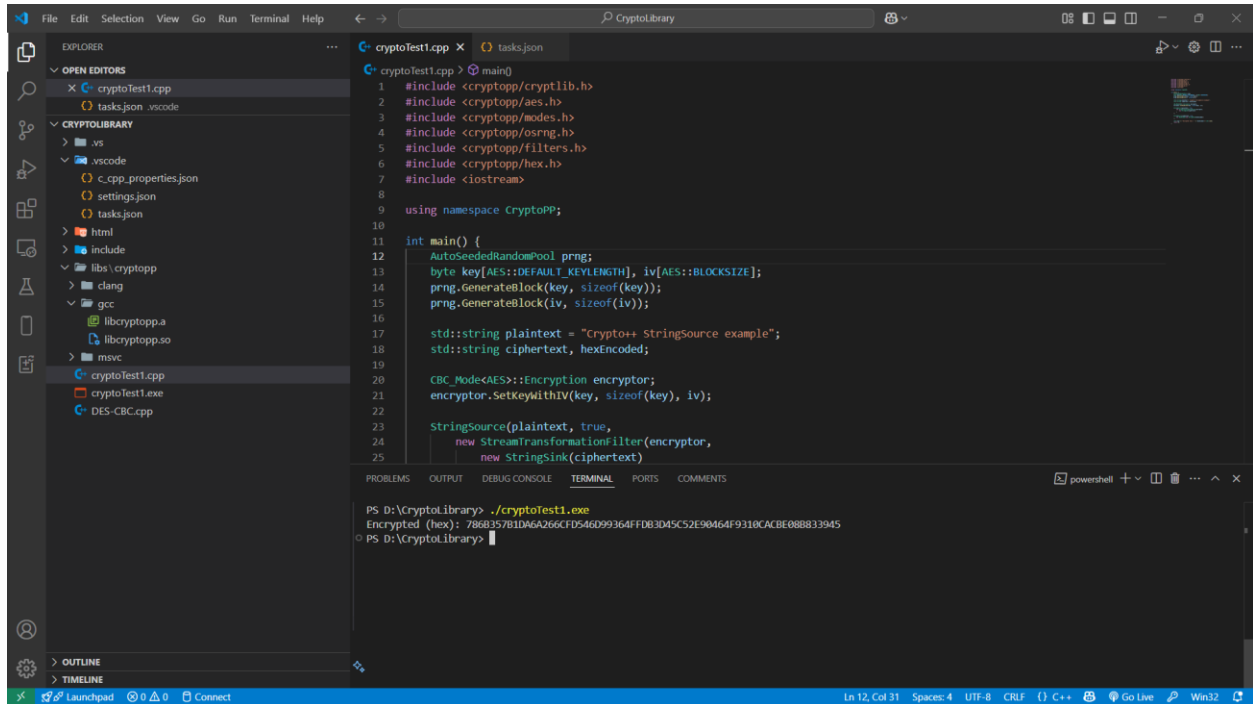


Họ và tên: Nguyễn Văn Hưng

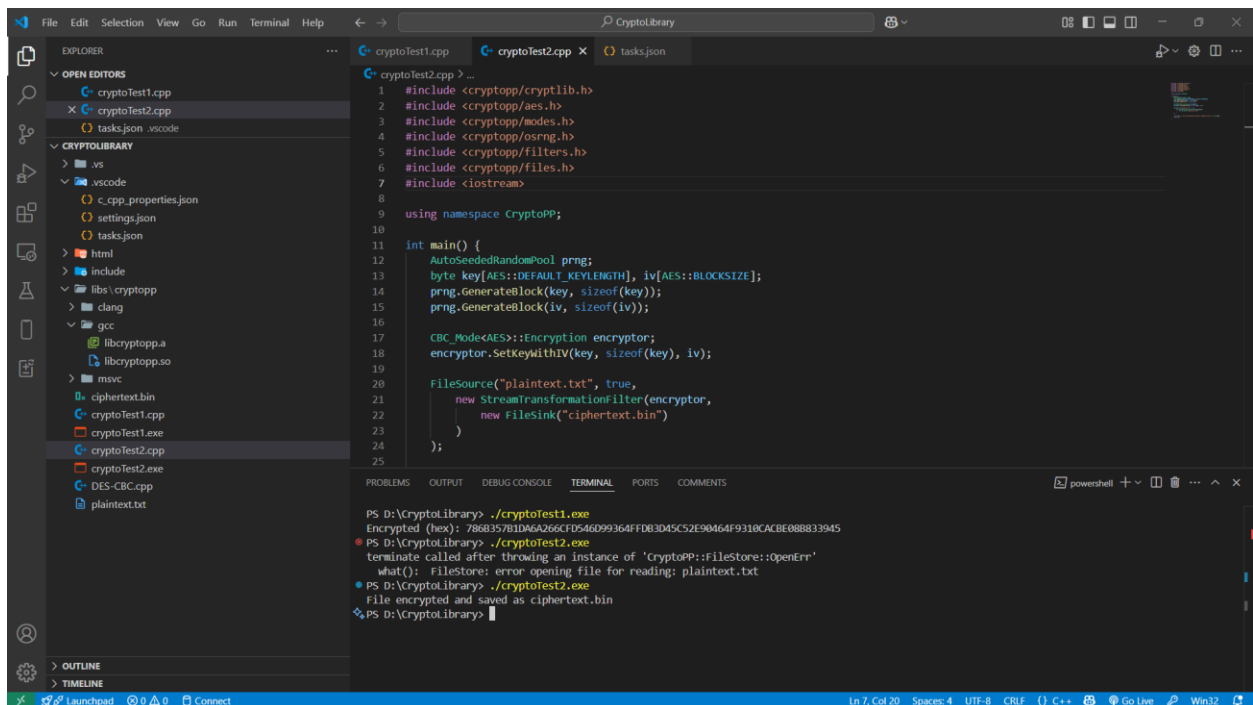
Mssv: 23520569



```
File Edit Selection View Go Run Terminal Help
CryptoLibrary

EXPLORER
OPEN EDITORS
  cryptoTest1.cpp
  tasks.json
CRYPTOLIBRARY
  .vs
  .vscode
    c_cpp_properties.json
    settings.json
    tasks.json
  html
  include
  libs\cryptopp
  clang
  gcc
  libcryptopp.a
  libcryptopp.so
  msvc
  cryptoTest1.cpp
  cryptoTest1.exe
  DES-CBC.cpp

cryptoTest1.cpp
1 #include <cryptopp/cryptlib.h>
2 #include <cryptopp/aes.h>
3 #include <cryptopp/modes.h>
4 #include <cryptopp/osrng.h>
5 #include <cryptopp/filters.h>
6 #include <cryptopp/hex.h>
7 #include <iostream>
8
9 using namespace CryptoPP;
10
11 int main() {
12     AutoSeededRandomPool prng;
13     byte key[AES::DEFAULT_KEYLENGTH], iv[AES::BLOCKSIZE];
14     prng.GenerateBlock(key, sizeof(key));
15     prng.GenerateBlock(iv, sizeof(iv));
16
17     std::string plaintext = "Crypto++ StringSource example";
18     std::string ciphertext, hexEncoded;
19
20     CBC_Mode_AES::Encryption encryptor;
21     encryptor.SetKeyWithIV(key, sizeof(key), iv);
22
23     StringSource(plaintext, true,
24                 new StreamTransformationFilter(encryptor,
25                 new StringSink(ciphertext)))
26
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS COMMENTS
PS D:\CryptoLibrary> ./cryptoTest1.exe
Encrypted (hex): 786835781D46A266CFD546D99364FFDB3D45C52E90464F9310CACBE088833945
PS D:\CryptoLibrary>
```



```
File Edit Selection View Go Run Terminal Help
CryptoLibrary

EXPLORER
OPEN EDITORS
  cryptoTest1.cpp
  cryptoTest2.cpp
  tasks.json
CRYPTOLIBRARY
  .vs
  .vscode
    c_cpp_properties.json
    settings.json
    tasks.json
  html
  include
  libs\cryptopp
  clang
  gcc
  libcryptopp.a
  libcryptopp.so
  msvc
  ciphertext.bin
  cryptoTest1.cpp
  cryptoTest1.exe
  cryptoTest2.cpp
  cryptoTest2.exe
  DES-CBC.cpp
  plaintext.txt

cryptoTest2.cpp
1 #include <cryptopp/cryptlib.h>
2 #include <cryptopp/aes.h>
3 #include <cryptopp/modes.h>
4 #include <cryptopp/osrng.h>
5 #include <cryptopp/filters.h>
6 #include <cryptopp/files.h>
7 #include <iostream>
8
9 using namespace CryptoPP;
10
11 int main() {
12     AutoSeededRandomPool prng;
13     byte key[AES::DEFAULT_KEYLENGTH], iv[AES::BLOCKSIZE];
14     prng.GenerateBlock(key, sizeof(key));
15     prng.GenerateBlock(iv, sizeof(iv));
16
17     CBC_Mode_AES::Encryption encryptor;
18     encryptor.SetKeyWithIV(key, sizeof(key), iv);
19
20     FileSource("plaintext.txt", true,
21               new StreamTransformationFilter(encryptor,
22               new FileSink("ciphertext.bin")))
23
24
25
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS COMMENTS
PS D:\CryptoLibrary> ./cryptoTest1.exe
Encrypted (hex): 786835781D46A266CFD546D99364FFDB3D45C52E90464F9310CACBE088833945
PS D:\CryptoLibrary> ./cryptoTest2.exe
terminate called after throwing an instance of 'CryptoPP::FileStore::OpenErr'
what(): FileStore: error opening file for reading: plaintext.txt
PS D:\CryptoLibrary> ./cryptoTest2.exe
File encrypted and saved as ciphertext.bin
PS D:\CryptoLibrary>
```

```

PS D:\CryptoLibrary> .\cryptotest3.exe
Encrypted 16 bytes using ArraySource and ArraySink.
• PS D:\CryptoLibrary> cat plaintext.txt
hihihahahuhu
❌ PS D:\CryptoLibrary> hexdump ciphertest.bin
hexdump: ciphertest.bin: No such file or directory
hexdump: all input file arguments failed
• PS D:\CryptoLibrary> hexdump ciphertext.bin
00000000 ae15 30e7 9cd5 3965 f3fa a63a 0f11 6916
0000010
○ PS D:\CryptoLibrary>

```

