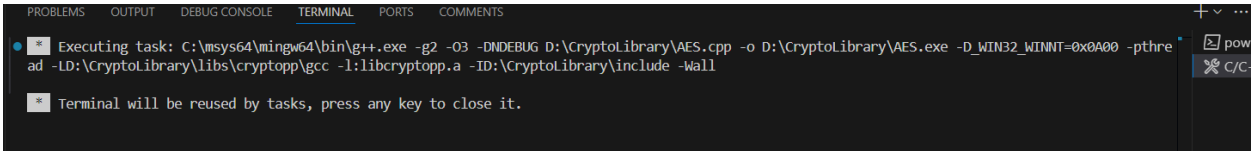
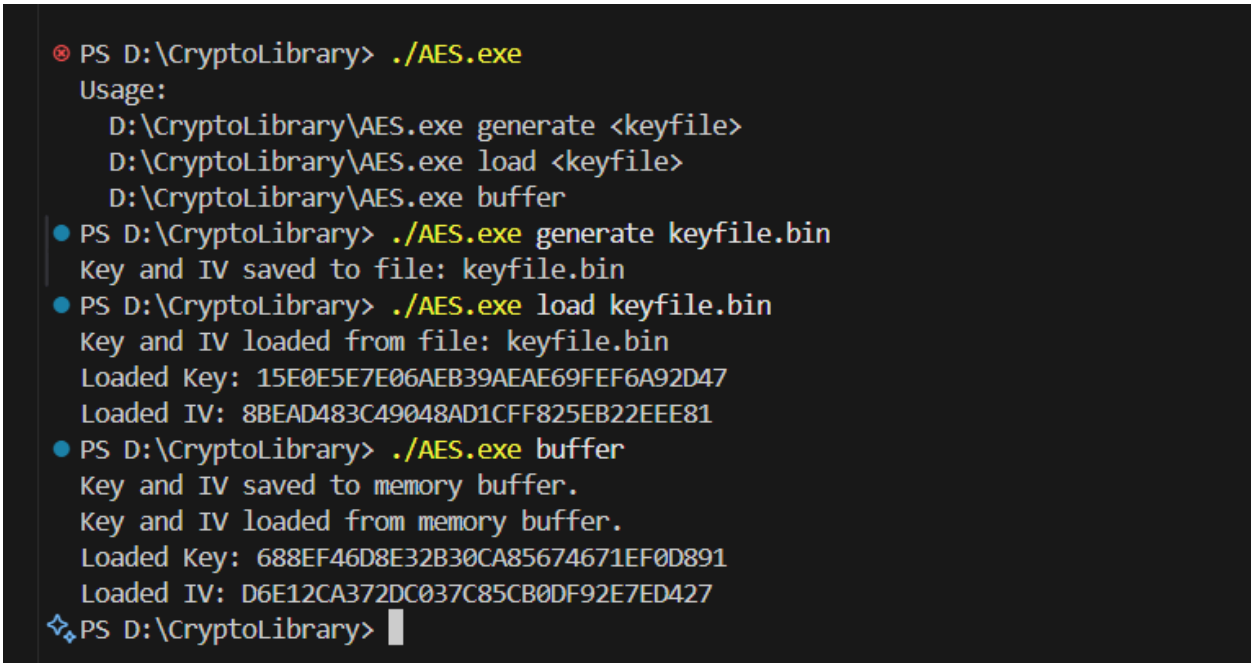
Họ tên: Nguyễn Văn Hưng

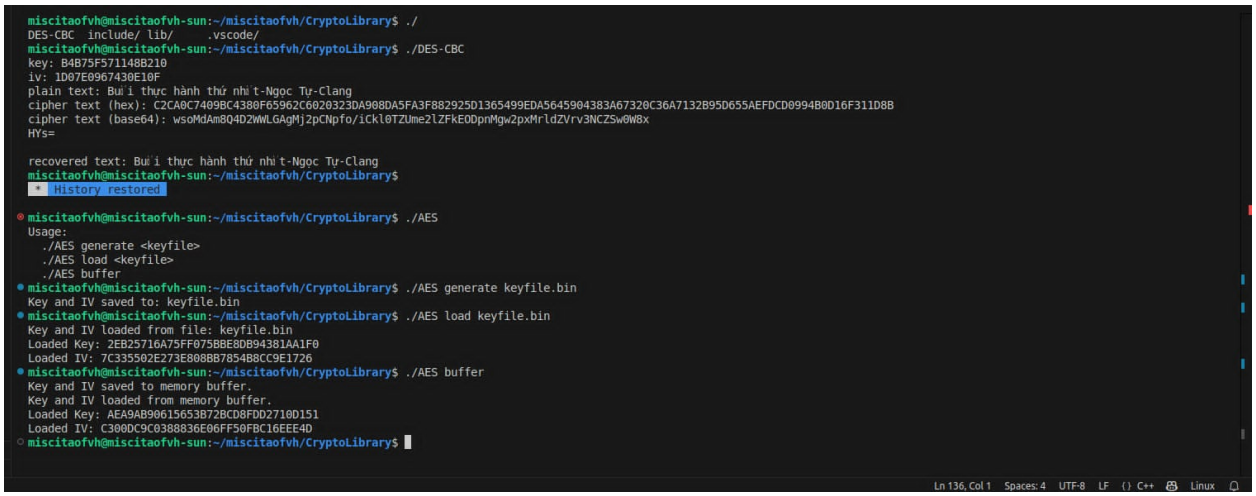
MSSV: 23520569

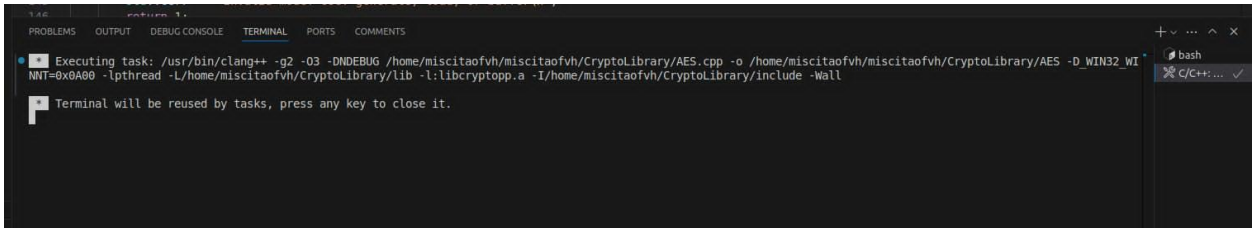
1. Gcc

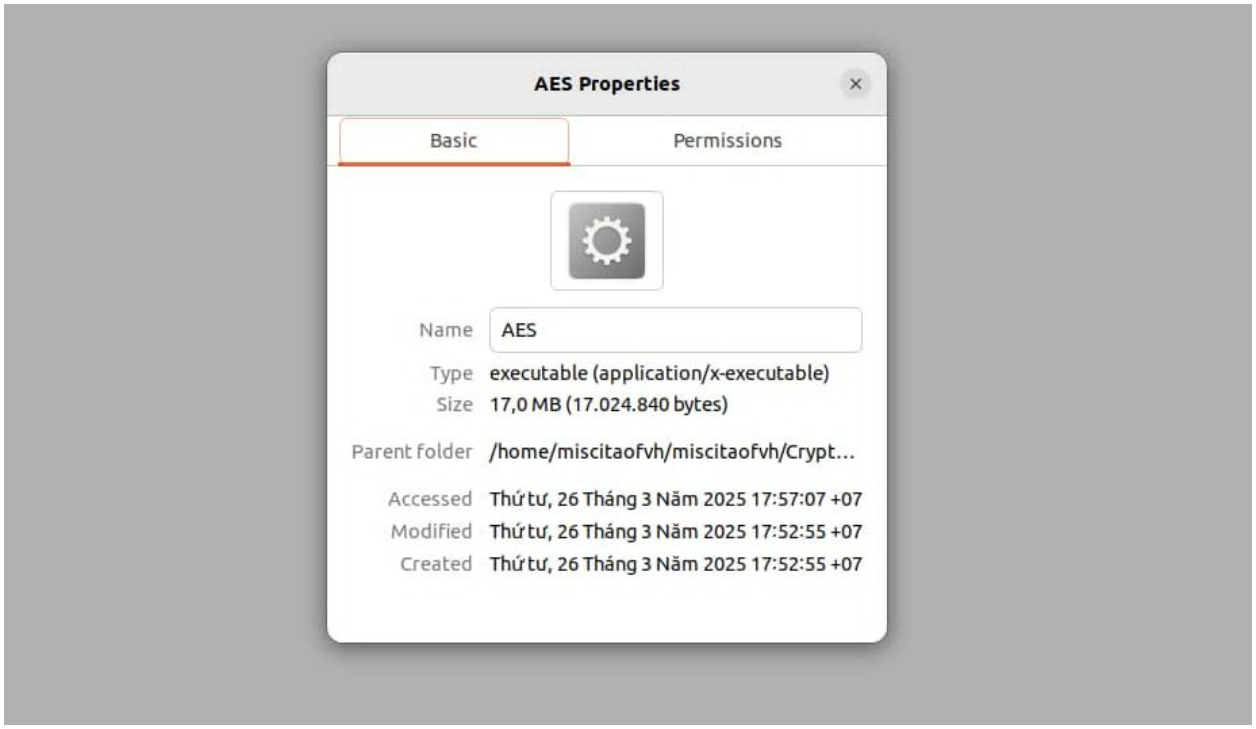




2. Clang


miscitaofvh@miscitaofvh-sun:~/miscitaofvh/CryptoLibrary$ ./
DES-CBC include/ lib/ .vscode/
miscitaofvh@miscitaofvh-sun:~/miscitaofvh/CryptoLibrary$ ./DES-CBC
key: B4B75F571148B210
iv: 1D07E0967430E10F
plain text: Bui i thực hành thứ nhi t-Ngoc Tự-Clang
cipher text (hex): C2CA0C7409BC4380F65962C6020323DA908DA5FA3F882925D1365499EDA5645904383A67320C36A7132B95D655AEFDCD0994B0D16F311D8B
cipher text (base64): wsoMdAm8Q4D2WWLGAgMj2pCNpfo/iCkl0TZUme2lZFkEODpnMgw2pxMrldZVrv3NCZSw0W8x
HYs=
recovered text: Bui i thực hành thứ nhi t-Ngoc Tự-Clang
miscitaofvh@miscitaofvh-sun:~/miscitaofvh/CryptoLibrary$
* History restored
miscitaofvh@miscitaofvh-sun:~/miscitaofvh/CryptoLibrary$ ./AES
Usage:
./AES generate <keyfile>
./AES load <keyfile>
./AES buffer
miscitaofvh@miscitaofvh-sun:~/miscitaofvh/CryptoLibrary$ ./AES generate keyfile.bin
Key and IV saved to: keyfile.bin
miscitaofvh@miscitaofvh-sun:~/miscitaofvh/CryptoLibrary$ ./AES load keyfile.bin
Key and IV loaded from file: keyfile.bin
Loaded Key: 2EB25716A75FF075BBE8DB94381AA1F0
Loaded IV: 7C335502E273E808BB7854B8CC9E1726
miscitaofvh@miscitaofvh-sun:~/miscitaofvh/CryptoLibrary$ ./AES buffer
Key and IV saved to memory buffer.
Key and IV loaded from memory buffer.
Loaded Key: AEA9AB90615653B72BCD8FDD2710D151
Loaded IV: C300DC9C0388836E06FF50FBC16EEE4D
miscitaofvh@miscitaofvh-sun:~/miscitaofvh/CryptoLibrary$
Ln 136, Col 1 Spaces: 4 UTF-8 LF C++ Linux


PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS COMMENTS
Executing task: /usr/bin/clang++ -g2 -O3 -DNDEBUG /home/miscitaofvh/miscitaofvh/CryptoLibrary/AES.cpp -o /home/miscitaofvh/miscitaofvh/CryptoLibrary/AES -D_WIN32_WI
NNT=0x0A00 -lpthread -L/home/miscitaofvh/CryptoLibrary/lib -l:libcryptopp.a -I/home/miscitaofvh/CryptoLibrary/include -Wall
Terminal will be reused by tasks, press any key to close it.
bash
C/C++: ...


AES Properties
Basic
Permissions
Name AES
Type executable (application/x-executable)
Size 17,0 MB (17.024.840 bytes)
Parent folder /home/miscitaofvh/miscitaofvh/Crypt...
Accessed Thứ tư, 26 Tháng 3 Năm 2025 17:57:07 +07
Modified Thứ tư, 26 Tháng 3 Năm 2025 17:52:55 +07
Created Thứ tư, 26 Tháng 3 Năm 2025 17:52:55 +07

3. Msvc

```
cryptlib.lib(sha.obj) : warning LNK4099: PDB '' was not found with 'cryptlib.lib(sha.obj)' or at ''; linking object as if no debug info
cryptlib.lib(rijndael.obj) : warning LNK4099: PDB '' was not found with 'cryptlib.lib(rijndael.obj)' or at ''; linking object as if no debug info
cryptlib.lib(hrtimer.obj) : warning LNK4099: PDB '' was not found with 'cryptlib.lib(hrtimer.obj)' or at ''; linking object as if no debug info
cryptlib.lib(modes.obj) : warning LNK4099: PDB '' was not found with 'cryptlib.lib(modes.obj)' or at ''; linking object as if no debug info
cryptlib.lib(gfpcrypt.obj) : warning LNK4099: PDB '' was not found with 'cryptlib.lib(gfpcrypt.obj)' or at ''; linking object as if no debug info
cryptlib.lib(hmac.obj) : warning LNK4099: PDB '' was not found with 'cryptlib.lib(hmac.obj)' or at ''; linking object as if no debug info
cryptlib.lib(gf2n.obj) : warning LNK4099: PDB '' was not found with 'cryptlib.lib(gf2n.obj)' or at ''; linking object as if no debug info
cryptlib.lib(ec2n.obj) : warning LNK4099: PDB '' was not found with 'cryptlib.lib(ec2n.obj)' or at ''; linking object as if no debug info
cryptlib.lib(ecp.obj) : warning LNK4099: PDB '' was not found with 'cryptlib.lib(ecp.obj)' or at ''; linking object as if no debug info
cryptlib.lib(rng.obj) : warning LNK4099: PDB '' was not found with 'cryptlib.lib(rng.obj)' or at ''; linking object as if no debug info
cryptlib.lib(primetab.obj) : warning LNK4099: PDB '' was not found with 'cryptlib.lib(primetab.obj)' or at ''; linking object as if no debug info
cryptlib.lib(cpu.obj) : warning LNK4099: PDB '' was not found with 'cryptlib.lib(cpu.obj)' or at ''; linking object as if no debug info
cryptlib.lib(sha_simd.obj) : warning LNK4099: PDB '' was not found with 'cryptlib.lib(sha_simd.obj)' or at ''; linking object as if no debug info
cryptlib.lib(rijndael_simd.obj) : warning LNK4099: PDB '' was not found with 'cryptlib.lib(rijndael_simd.obj)' or at ''; linking object as if no deb
ug info
cryptlib.lib(rdtables.obj) : warning LNK4099: PDB '' was not found with 'cryptlib.lib(rdtables.obj)' or at ''; linking object as if no debug info
cryptlib.lib(des.obj) : warning LNK4099: PDB '' was not found with 'cryptlib.lib(des.obj)' or at ''; linking object as if no debug info
cryptlib.lib(gf2n_simd.obj) : warning LNK4099: PDB '' was not found with 'cryptlib.lib(gf2n_simd.obj)' or at ''; linking object as if no debug info
cryptlib.lib(sse_simd.obj) : warning LNK4099: PDB '' was not found with 'cryptlib.lib(sse_simd.obj)' or at ''; linking object as if no debug info
cryptlib.lib(dessp.obj) : warning LNK4099: PDB '' was not found with 'cryptlib.lib(dessp.obj)' or at ''; linking object as if no debug info
 *  Terminal will be reused by tasks, press any key to close it.
```

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS  COMMENTS

PS D:\CryptoLibrary> ./AES.exe
Usage:
  D:\CryptoLibrary\AES.exe generate <keyfile>
  D:\CryptoLibrary\AES.exe load <keyfile>
  D:\CryptoLibrary\AES.exe buffer
PS D:\CryptoLibrary> ./AES.exe generate keyfile.bin
Key and IV saved to file: keyfile.bin
PS D:\CryptoLibrary> ./AES.exe load keyfile.bin
Key and IV loaded from file: keyfile.bin
Loaded Key: 09AEF5913033089E612EA96619B0E71C
Loaded IV: 0ED2C217E672FEF811855ADCBD0D7D6E
PS D:\CryptoLibrary> ./AES.exe buffer
Key and IV saved to memory buffer.
Key and IV loaded from memory buffer.
Loaded Key: 46C3F99180856945DB73800D89752B42
Loaded IV: E27E8CCBF5E308A649A376686C5DF54F
PS D:\CryptoLibrary>
```