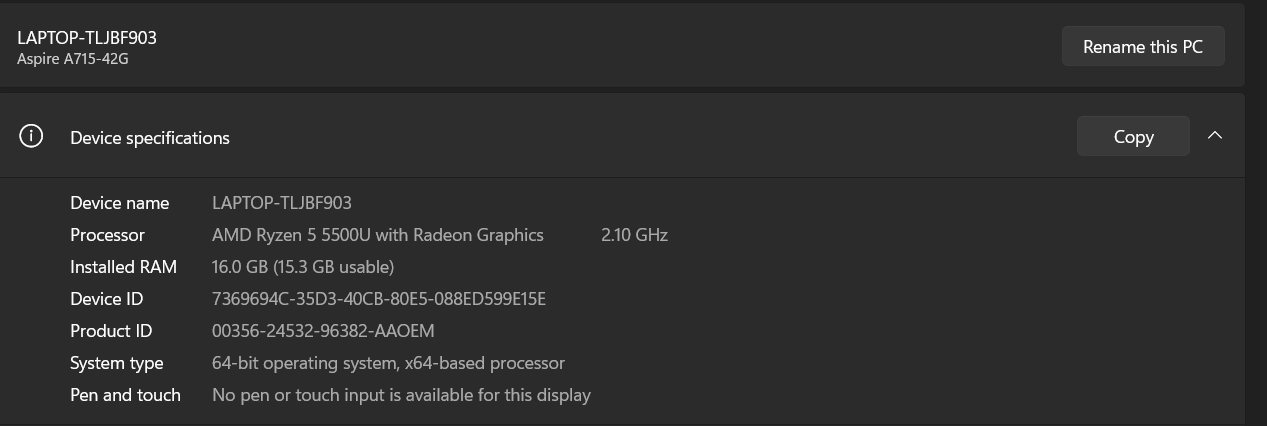
**REPORT TASK 2**

Môn: Mật mã học

Lớp: NT219.O22.ANTT

Giảng viên: Nguyễn Ngọc Tự

Sinh viên thực hiện: Nguyễn Tuấn Phát - 22521076

**I. Hardware resources**

**II. AES not using cryptopp lib**

- Tổng quan:

+ cmd arguments, .dll, GUI C#

+ Vietnamese supported

+ input plaintext/ciphertext from file/keyboard

*1. So sánh thời gian chạy trên window/linux*

- So sánh thời gian encrypt/decrypt giữa Window/Linux với 6 file có kích thước: 10KB, 50KB, 250KB, 500KB, 1MB, 2MB.

+ Key 256 bits: 12345678abcdefghvbnmfgds12345678

+ IV 16 bytes: encryptionIntVec

+ Số lần chạy trung bình: 10000 lần

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| File | Window | | Linux | |
| Encrypt | Decrypt | Encrypt | Decrypt |
| 10KB | 0.0099 (ms) | 0.0103 | 0.0006 | 0.0008 |
| 50KB | 0.0444 | 0.0497 | 0.0037 | 0.0044 |
| 250KB | 0.2115 | 0.2591 | 0.0253 | 0.0295 |
| 500KB | 0.5362 | 0.6901 | 0.0704 | 0.08 |
| 1MB | 1.7488 | 2.0955 | 0.2906 | 0.3881 |
| 2MB | 7.6761 | 8.1444 | 2.736 | 3.4988 |

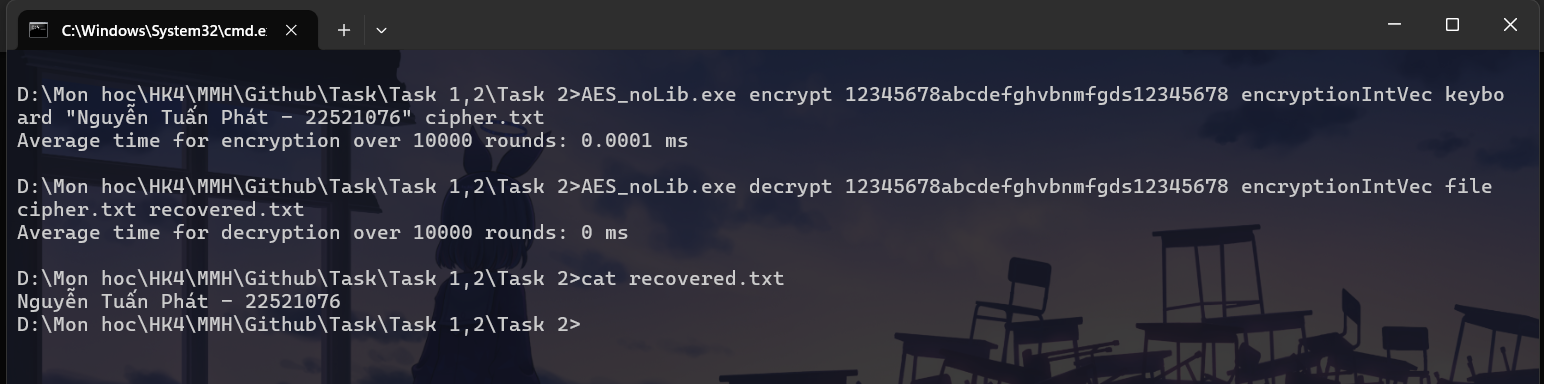
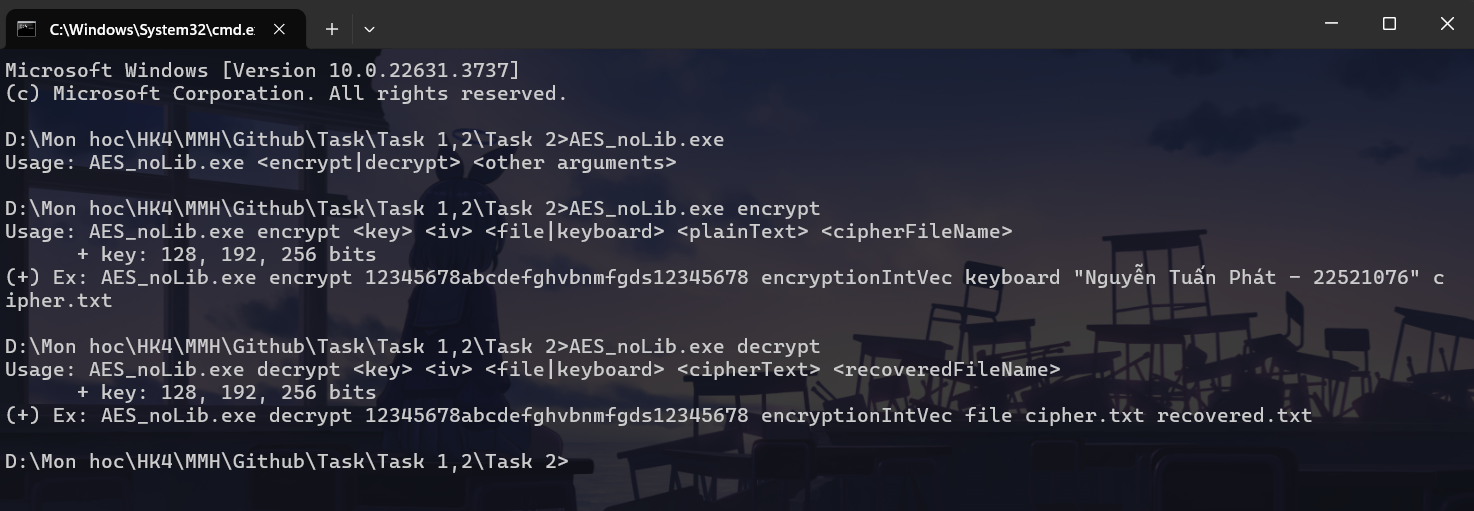
- Nhận xét:

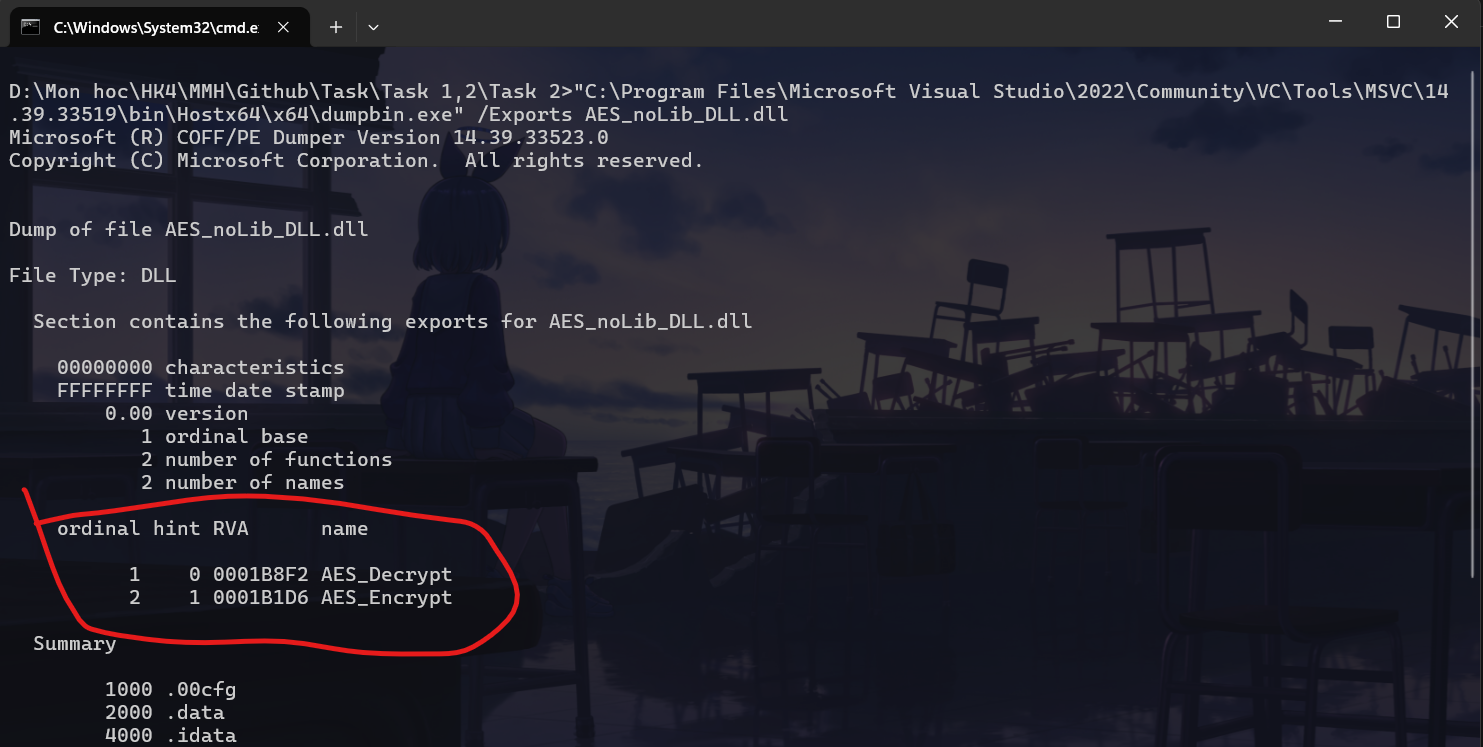
+ File càng lớn, thời gian encrypt càng lâu

+ Tốc độ chạy trên linux nhanh hơn window khá nhiều, do linux được build đơn giản hơn window, có môi trường tốt hơn.

*2. Cmd argument, DLL, GUI C#*

*2.1 Cmd argument*

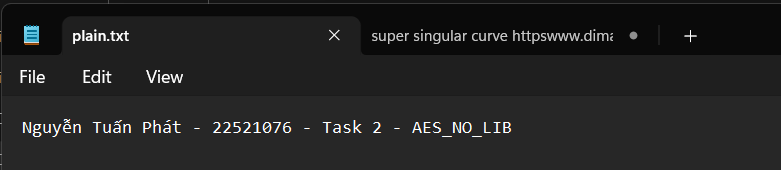


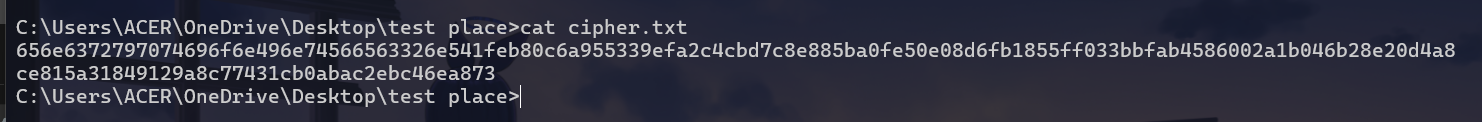
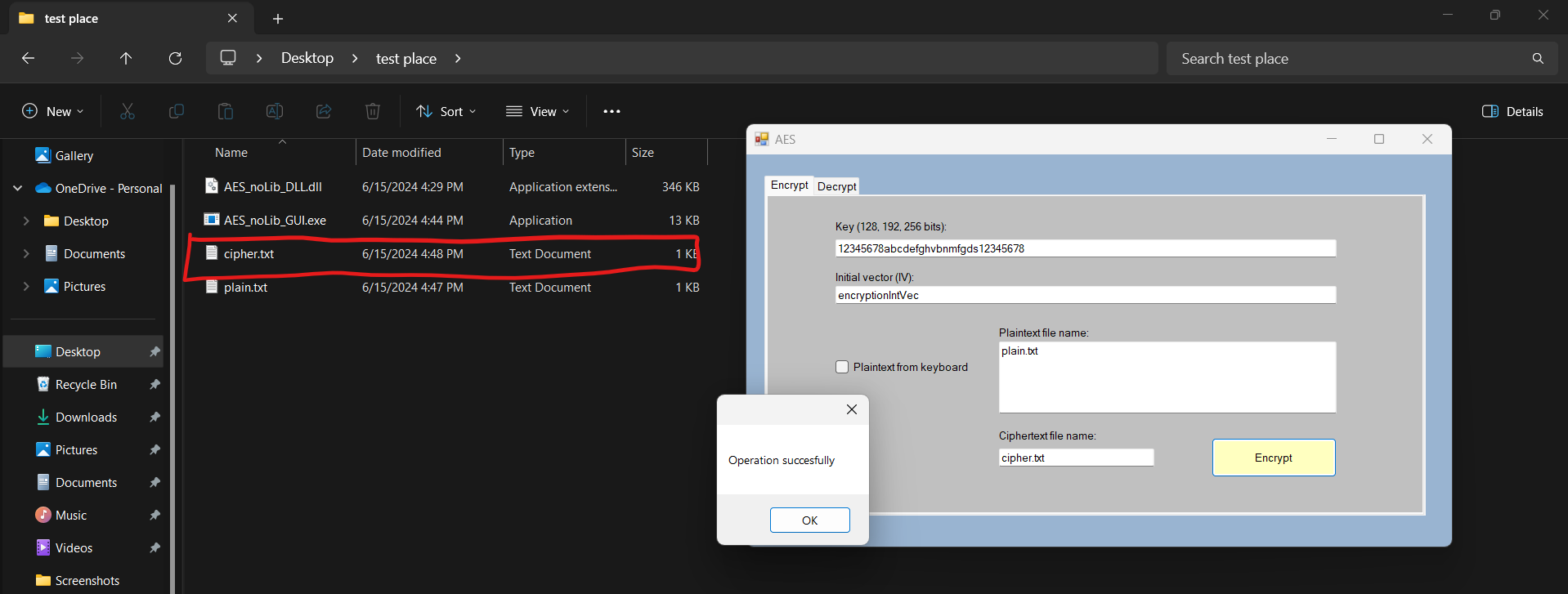
*2.2 Export DLL*

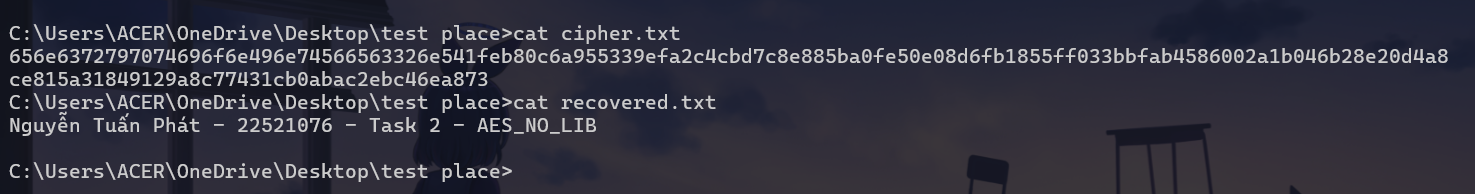
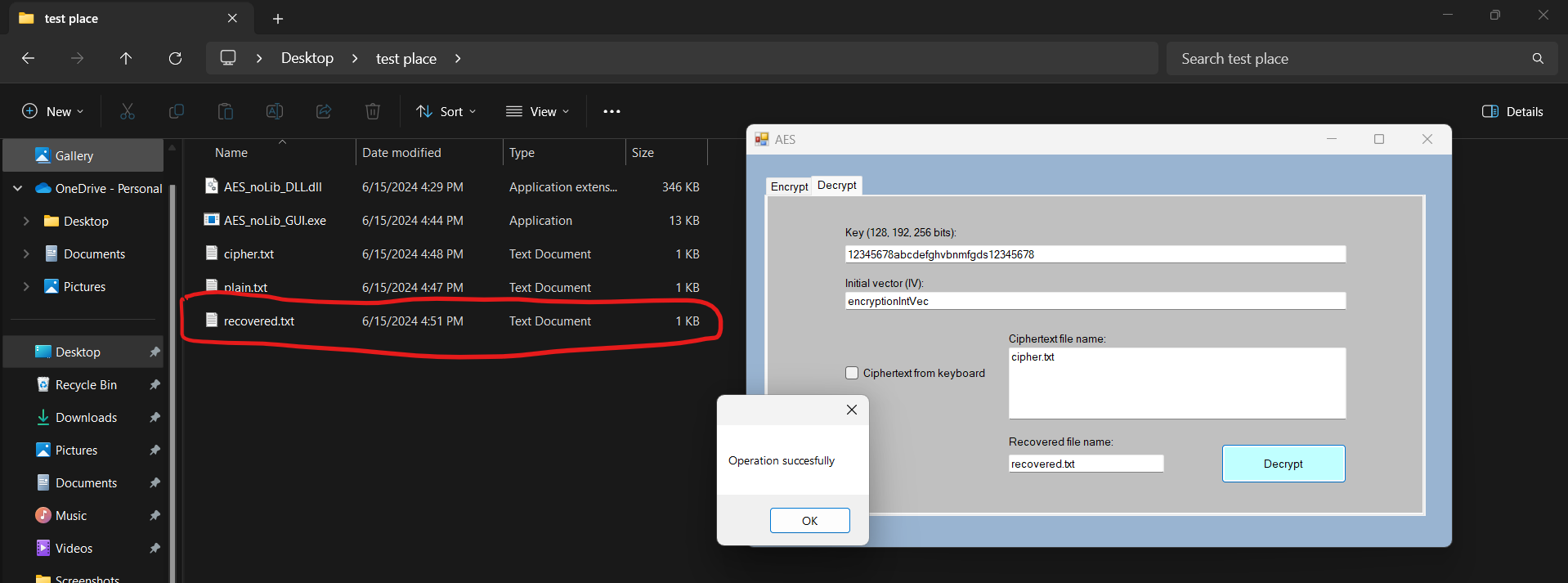
*2.3 GUI C#*

- Key 256 bits: 12345678abcdefghvbnmfgds12345678

- IV 16 bytes: encryptionIntVec

- Plaintext:

- Encrypt:

- Decrypt: