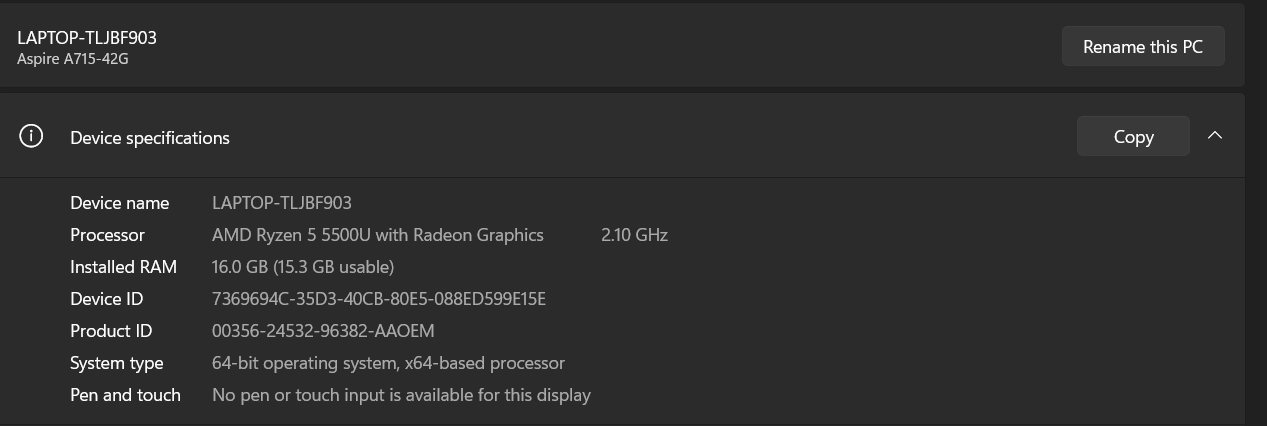
**REPORT TASK 3**

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. RSA**

- Tổng quan:

+ cmd arguments, .dll, GUI C#

+ Vietnamese supported

+ input plaintext/ciphertext from file/keyboard

+ Key format: DER, PEM and Base64

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

- So sánh thời gian keygen/encrypt/decrypt giữa Window/Linux với file có kích thước: 50 bytes với 6 loại key (3072, 4096, 5120, 6144, 7168, 8192 bits).

+ Số lần chạy trung bình: **encrypt** 1000 lần, **decrypt** 100 lần

- Keygen:

|  |  |  |
| --- | --- | --- |
| Key size (bit) | Window | Linux |
| 3072 | 6.626 (s) | 0.582 |
| 4096 | 10.428 | 1.017 |
| 5120 | 25.962 | 4.532 |
| 6144 | 52.921 | 10.205 |
| 7168 | 79.771 | 12.896 |
| 8192 | 161.254 | 16.305 |

- Encrypt/Decrypt (50 bytes file)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Window | | Linux | |
| Key Size (bits) | Encrypt | Decrypt | Encrypt | Decrypt |
| 3072 | 7.252 (ms) | 277.08 | 0.13 | 4.51 |
| 4096 | 7.573 | 394.78 | 0.151 | 5.88 |
| 5120 | 8.795 | 1293.35 | 0.235 | 22.6 |
| 6144 | 9.108 | 1637.18 | 0.259 | 26.75 |
| 7168 | 9.405 | 2026.73 | 0.277 | 31.06 |
| 8192 | 9.689 | 2335.61 | 0.282 | 35.5 |

- Nhận xét:

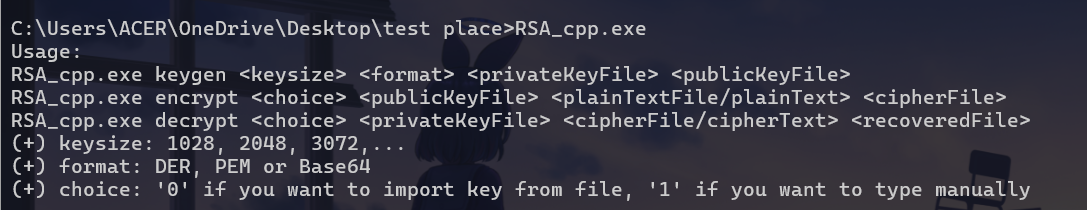
+ File càng lớn, thời gian encrypt/decrypt càng lâu.

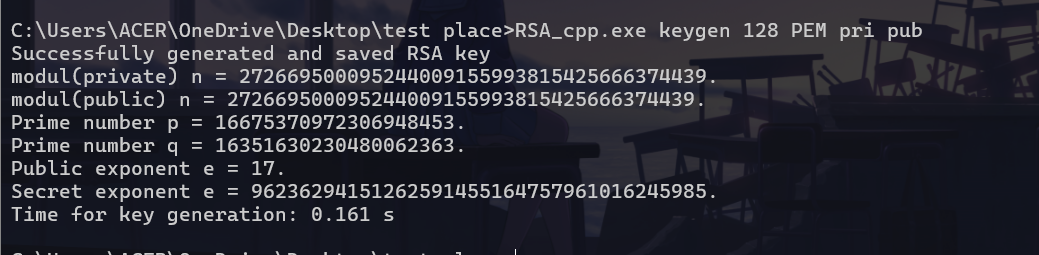
+ Tốc độ encrypt/decrypt phụ thuộc vào kích thước của key, key càng lớn càng tốn thời gian. Do khi kích thước của key tăng, tất cả phép toán cần thực hiện càng phức tạp và mất thời gian nên mặc dù cùng một plaintext nhưng các key có kích thước khác nhau thì có thời gian encrypt/decrypt khác nhau.

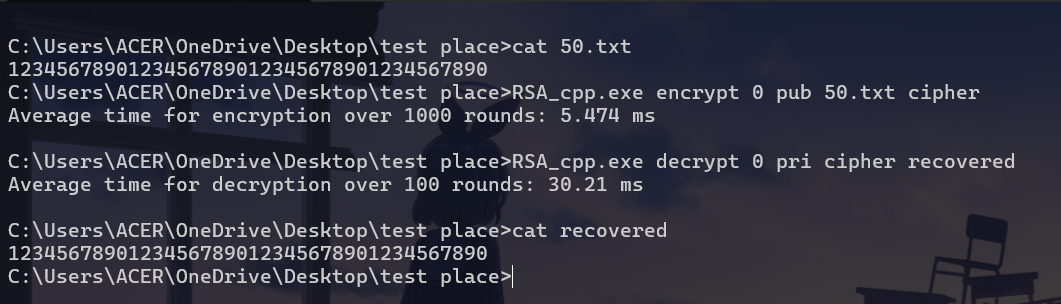
+ Linux chạy nhanh hơn Window khá nhiều, do kiến trúc hệ điều hành nhẹ hơn, tối ưu kernel, quản lý ít tài nguyên hơn window.

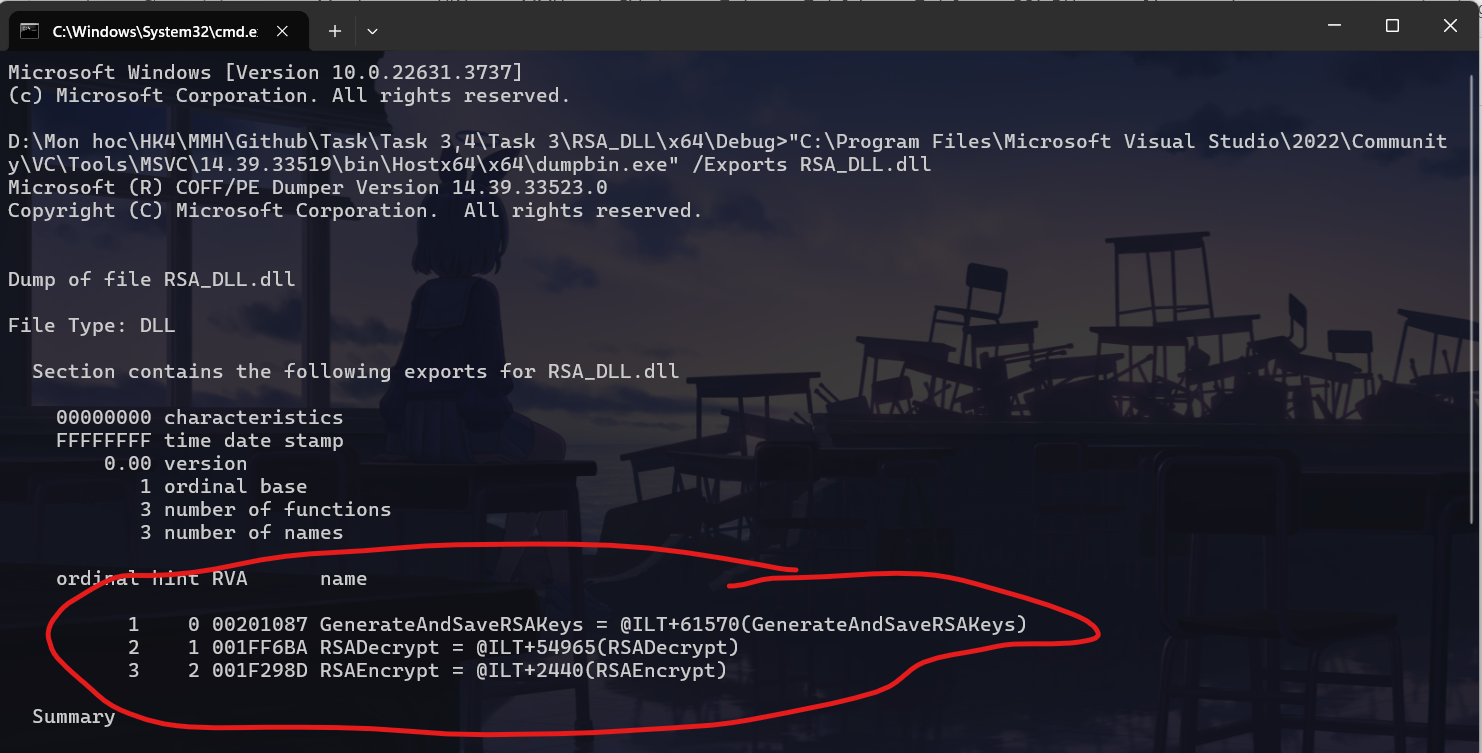
*2. Cmd argument, DLL, GUI C#*

*2.1 Cmd argument*

- keygen:

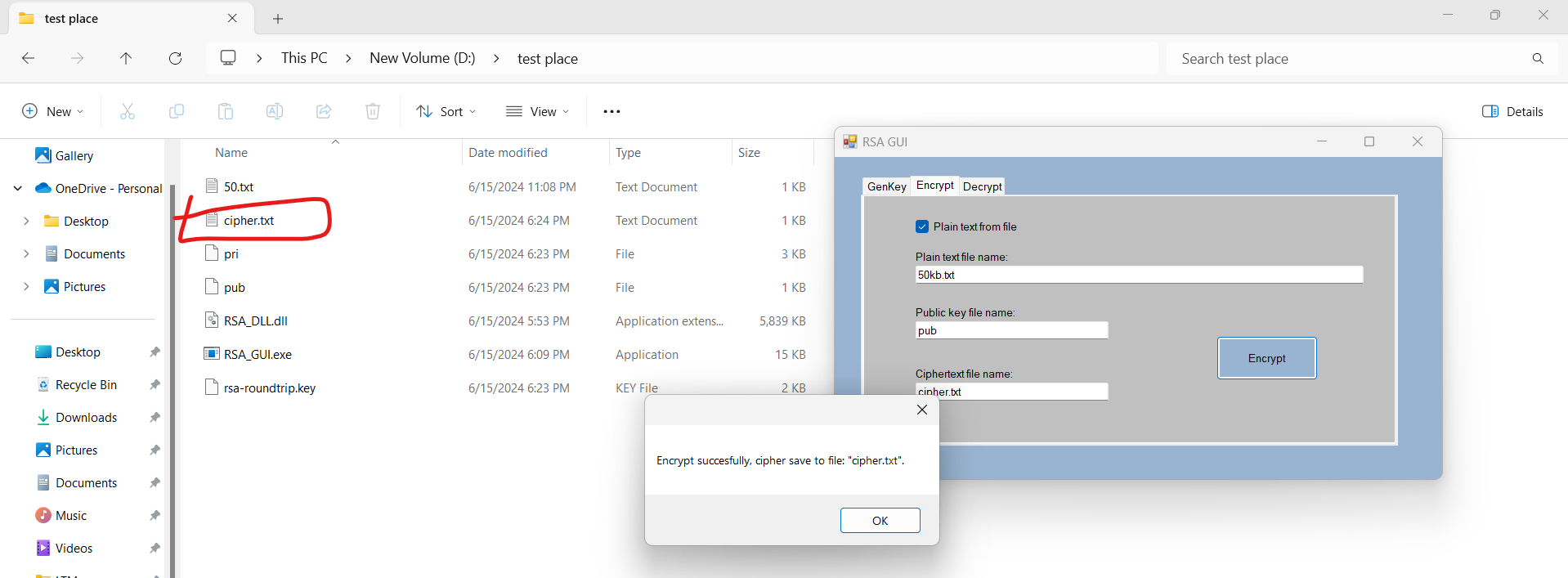
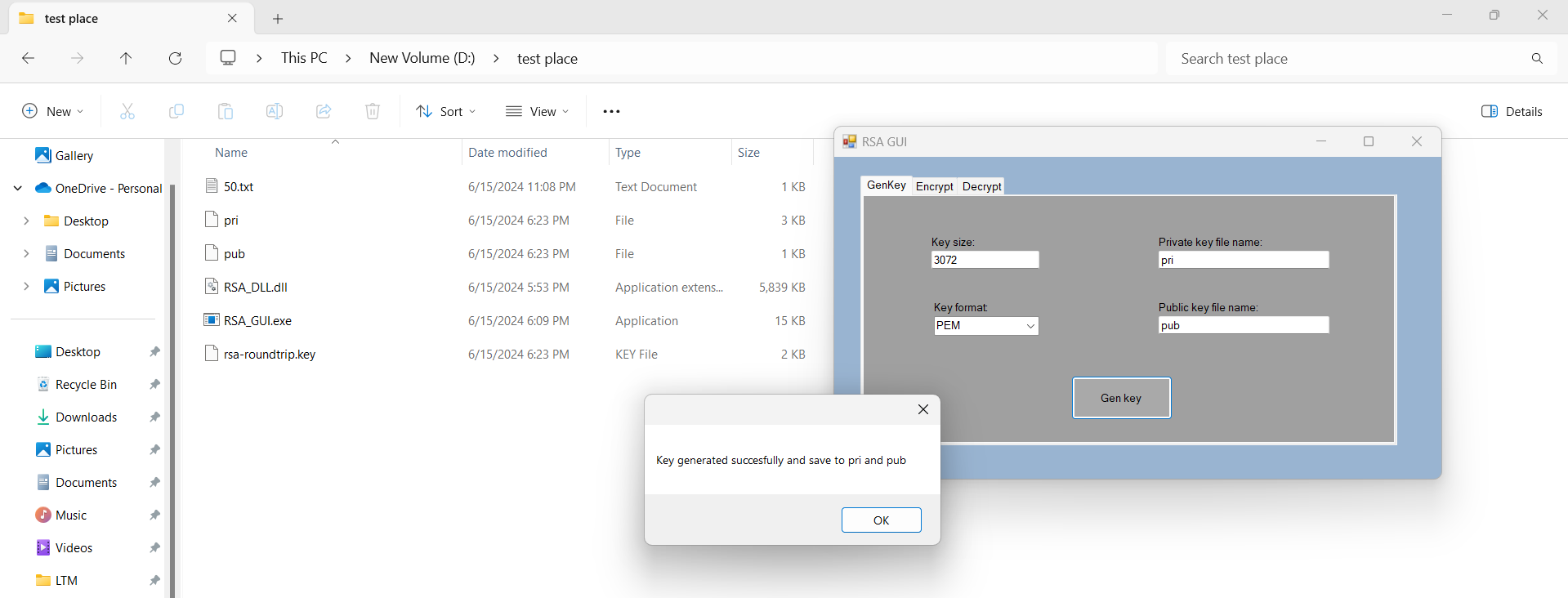
- Encrypt/decrypt

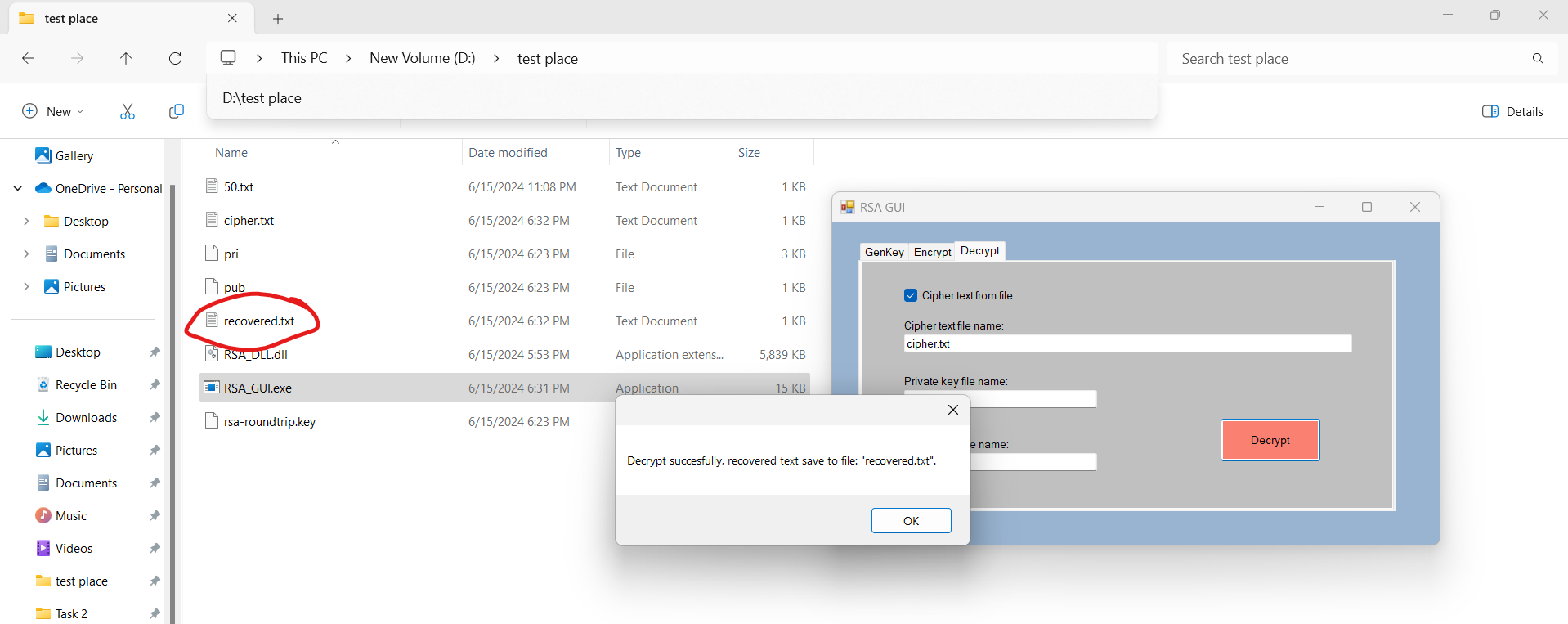


*2.2 Export DLL*

*2.3 GUI C#*

- Keygen:

- Encrypt:

- Decrypt: