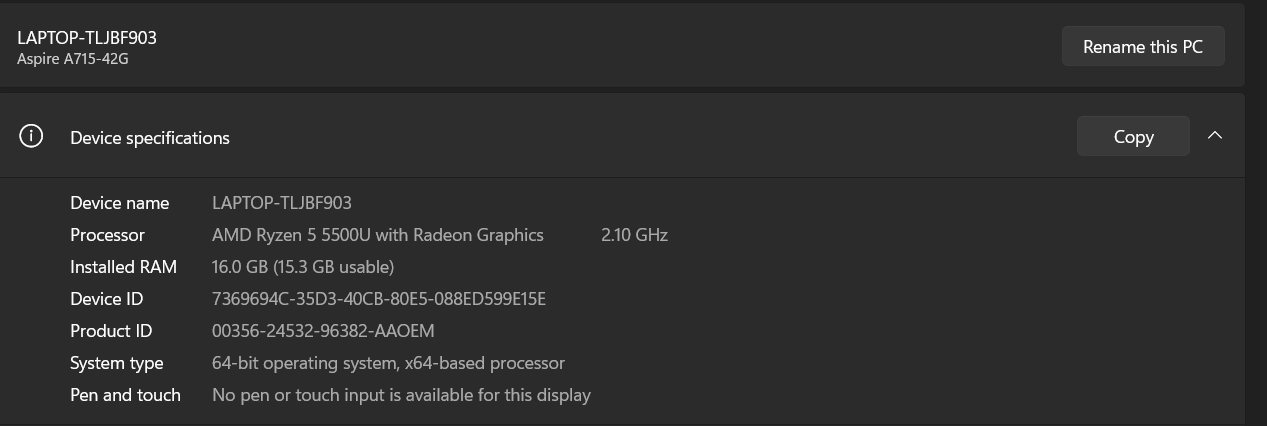
**REPORT TASK 1**

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 – DES**

- Tổng quan:

+ Cmd arguments, .dll, GUI C#

+ Vietnamese supported

+ input plaintext/ciphertext from keyboard/file

1. So sánh window, linux:

- So sánh thời gian encrypt/decrypt giữa Window và Linux với 8 modes trên 6 file có kích thước lần lượt: 10KB, 50KB, 250KB, 500KB, 1MB, 2MB.

+ Số lần chạy trung bình: Encrypt 10000 lần, Decrypt 10000 lần

+ Key: 9CFB357E293CF594FD1515CAF49BCFDBC33E508811339C80840AFC4DFA09BE80

+ IV: 60E5B739886F324EB7CB96AE44A8470F

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Window 11 | | | | | | | |
| Modes |  | 10KB | 50KB | 250KB | 500KB | 1MB | 2MB |
| ECB | Encrypt | 0.006(ms) | 0.047 | 0.104 | 0.114 | 0.471 | 1.163 |
|  | Decrypt | 0.005 | 0.031 | 0.067 | 0.111 | 0.463 | 1.16 |
| CBC | Encrypt | 0.014 | 0.064 | 0.282 | 0.584 | 1.394 | 2.966 |
|  | Decrypt | 0.006 | 0.016 | 0.062 | 0.124 | 0.566 | 1.263 |
| OFB | Encrypt | 0.016 | 0.062 | 0.286 | 0.653 | 1.379 | 3.031 |
|  | Decrypt | 0.014 | 0.062 | 0.286 | 0.637 | 1.395 | 3.117 |
| CFB | Encrypt | 0.016 | 0.06 | 0.287 | 0.572 | 1.37 | 3.036 |
|  | Decrypt | 0.006 | 0.023 | 0.095 | 0.191 | 0.61 | 1.641 |
| CTR | Encrypt | 0.005 | 0.015 | 0.066 | 0.13 | 0.501 | 1.265 |
|  | Decrypt | 0.005 | 0.017 | 0.069 | 0.154 | 0.54 | 1.341 |
| XTS | Encrypt | 0.011 | 0.041 | 0.207 | 0.457 | 1.043 | 2.327 |
|  | Decrypt | 0.011 | 0.039 | 0.209 | 0.414 | 1.045 | 2.353 |
| CCM | Encrypt | 0.018 | 0.073 | 0.331 | 0.902 | 1.561 | 3.406 |
|  | Decrypt | 0.02 | 0.072 | 0.34 | 0.71 | 1.58 | 3.511 |
| GCM | Encrypt | 0.008 | 0.023 | 0.109 | 0.254 | 0.816 | 2.011 |
|  | Decrypt | 0.013 | 0.033 | 0.151 | 0.456 | 0.91 | 3.29 |

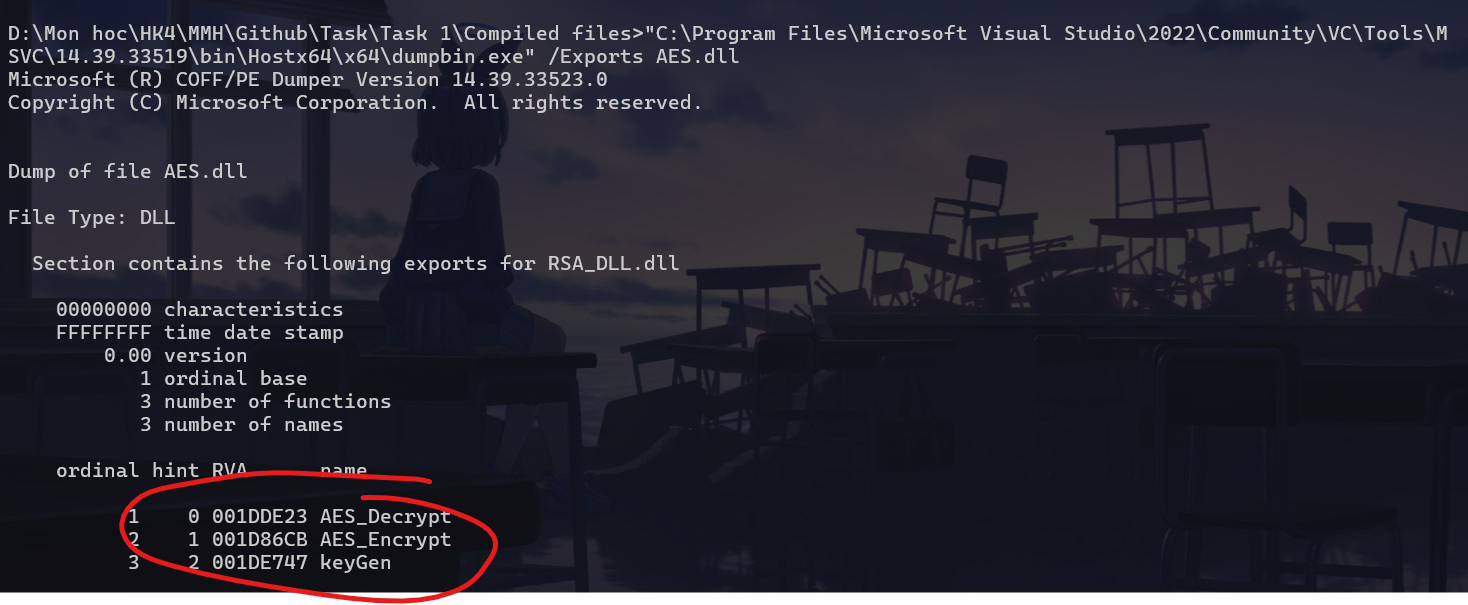
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Linux | | | | | | | |
| Modes |  | 10KB | 50KB | 250KB | 500KB | 1MB | 2MB |
| ECB | Encrypt | 0.003(ms) | 0.011 | 0.049 | 0.097 | 0.243 | 0.702 |
|  | Decrypt | 0.003 | 0.011 | 0.049 | 0.098 | 0.247 | 0.722 |
| CBC | Encrypt | 0.012 | 0.056 | 0.274 | 0.546 | 1.141 | 2.46 |
|  | Decrypt | 0.003 | 0.012 | 0.054 | 0.109 | 0.302 | 0.868 |
| OFB | Encrypt | 0.012 | 0.057 | 0.278 | 0.556 | 1.164 | 3.147 |
|  | Decrypt | 0.012 | 0.057 | 0.277 | 0.557 | 1.153 | 2.533 |
| CFB | Encrypt | 0.012 | 0.056 | 0.275 | 0.548 | 1.144 | 2.473 |
|  | Decrypt | 0.005 | 0.018 | 0.085 | 0.17 | 0.424 | 1.118 |
| CTR | Encrypt | 0.003 | 0.013 | 0.06 | 0.119 | 0.284 | 0.793 |
|  | Decrypt | 0.003 | 0.013 | 0.06 | 0.121 | 0.327 | 0.834 |
| XTS | Encrypt | 0.008 | 0.036 | 0.183 | 0.37 | 0.798 | 1.795 |
|  | Decrypt | 0.007 | 0.035 | 0.181 | 0.37 | 0.832 | 1.837 |
| CCM | Encrypt | 0.014 | 0.066 | 0.323 | 0.648 | 1.351 | 2.866 |
|  | Decrypt | 0.015 | 0.067 | 0.323 | 0.649 | 1.406 | 2.973 |
| GCM | Encrypt | 0.005 | 0.022 | 0.116 | 0.212 | 0.523 | 1.384 |
|  | Decrypt | 0.007 | 0.033 | 0.13 | 0.506 | 1.317 | 2.096 |

- Nhận xét:

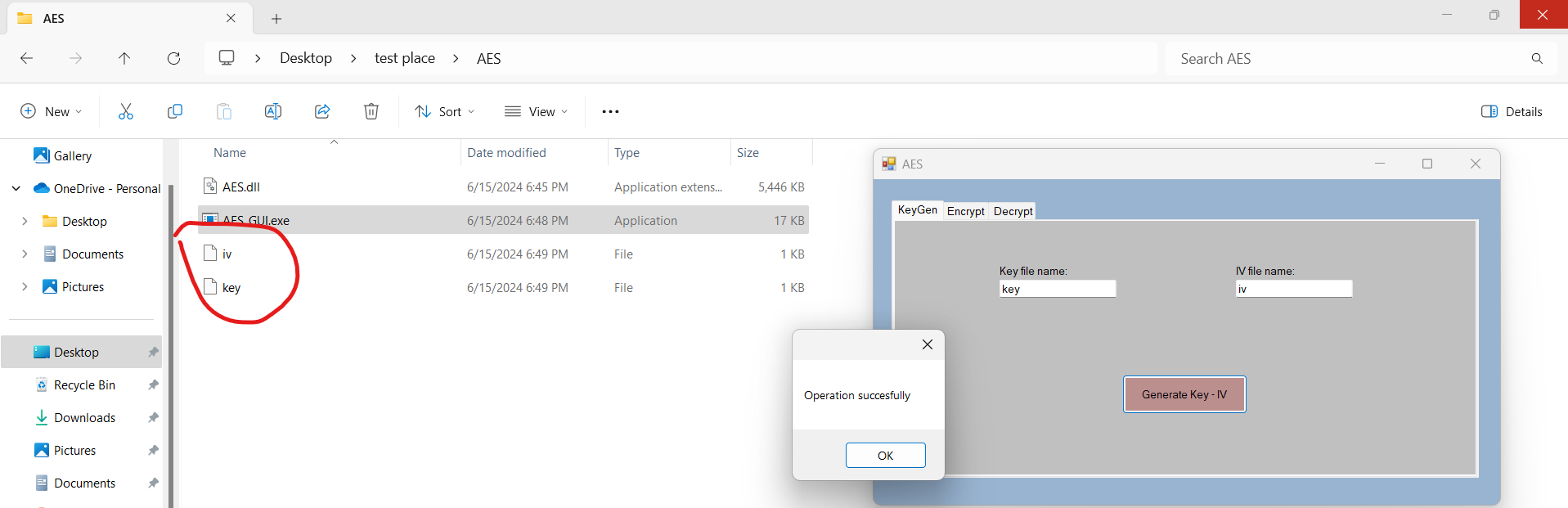
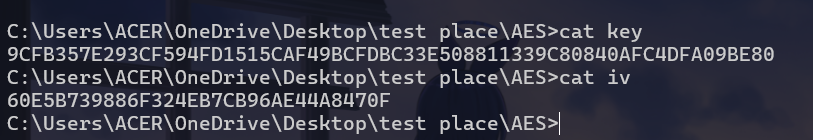
+ Linux chạy nhanh hơn Window khá nhiều, do kiến trúc hệ điều hành nhẹ hơn, tối ưu kernel, quản lý ít tài nguyên hơn window.

+ Mode ECB có thời gian thực thi nhanh nhất do có thiết kế đơn giản nhất, thời gian thực thi của CCM khá lâu do có authentication.

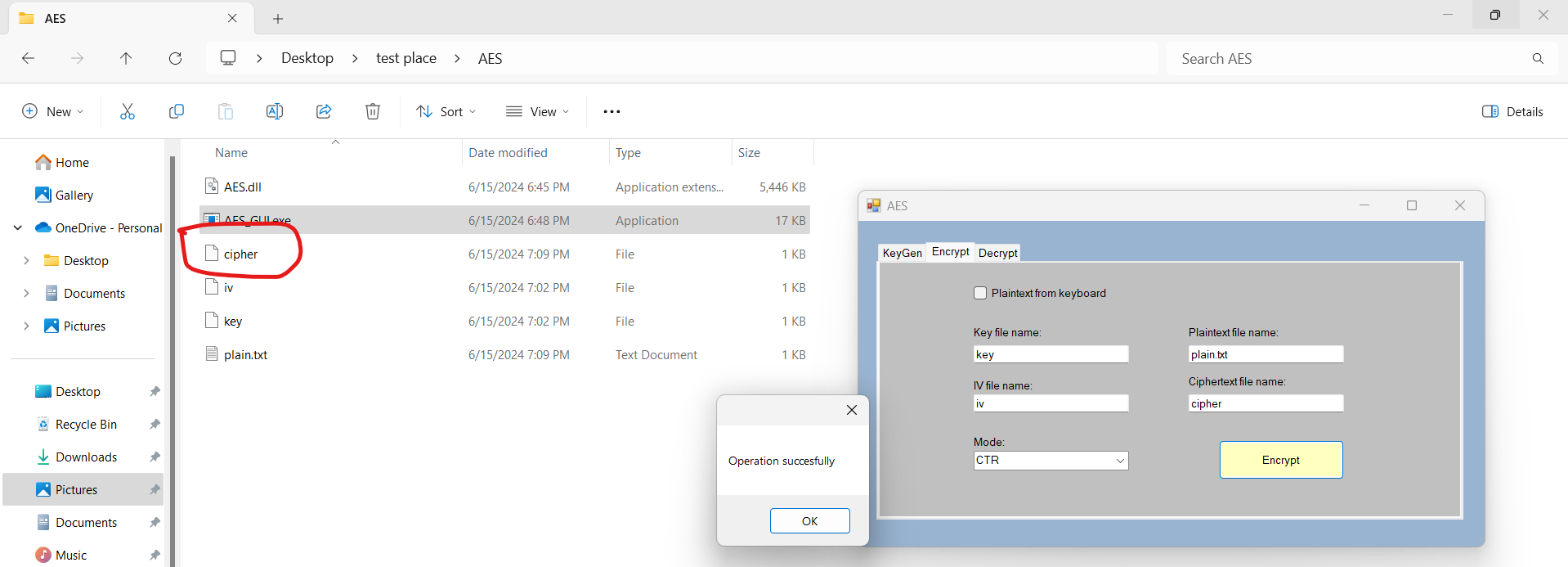
+ File càng lớn, thời gian encrypt/decrypt càng lớn.

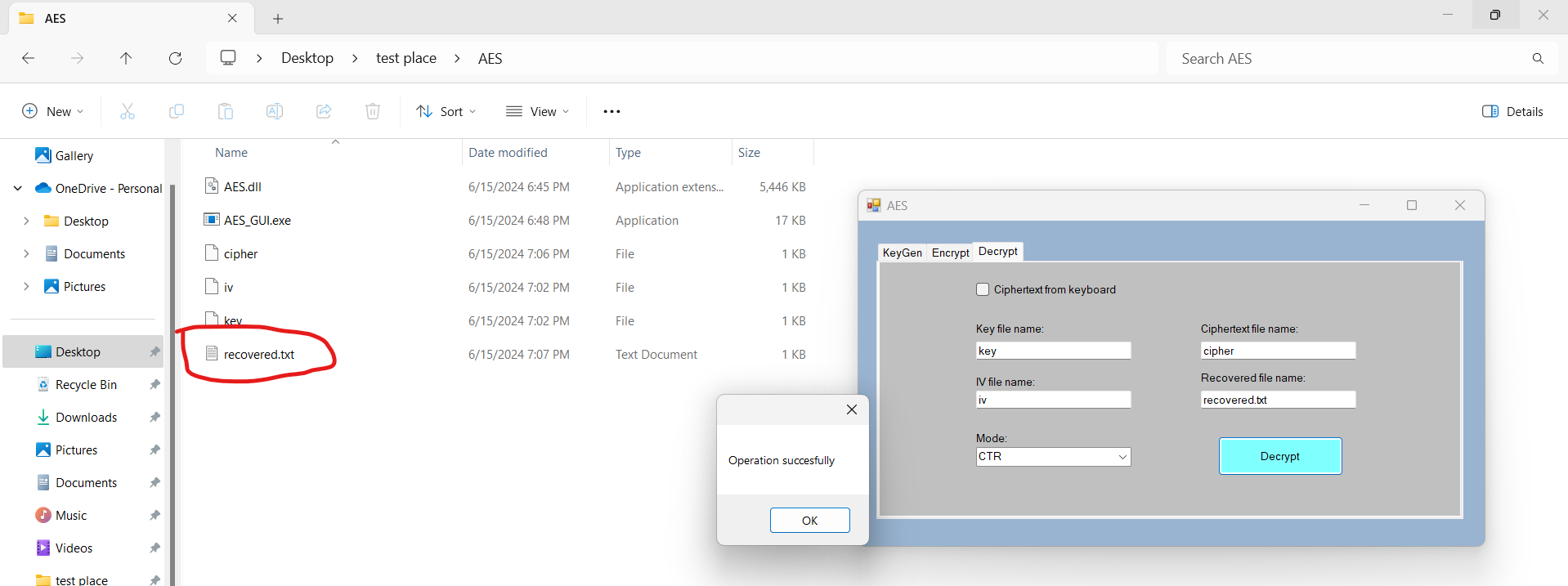
2. DLL Export:

3.0 GUI C# (Key gen):



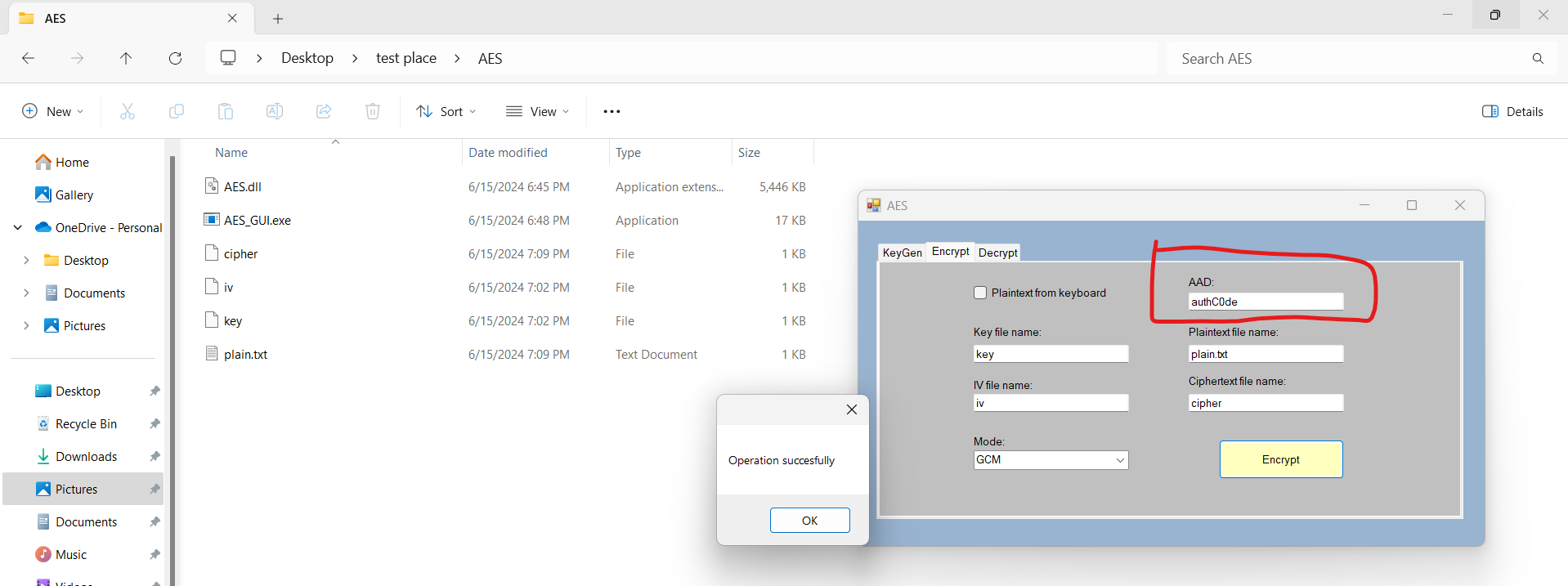
3.1 GUI C# (Mode != GCM):

- Encrypt:

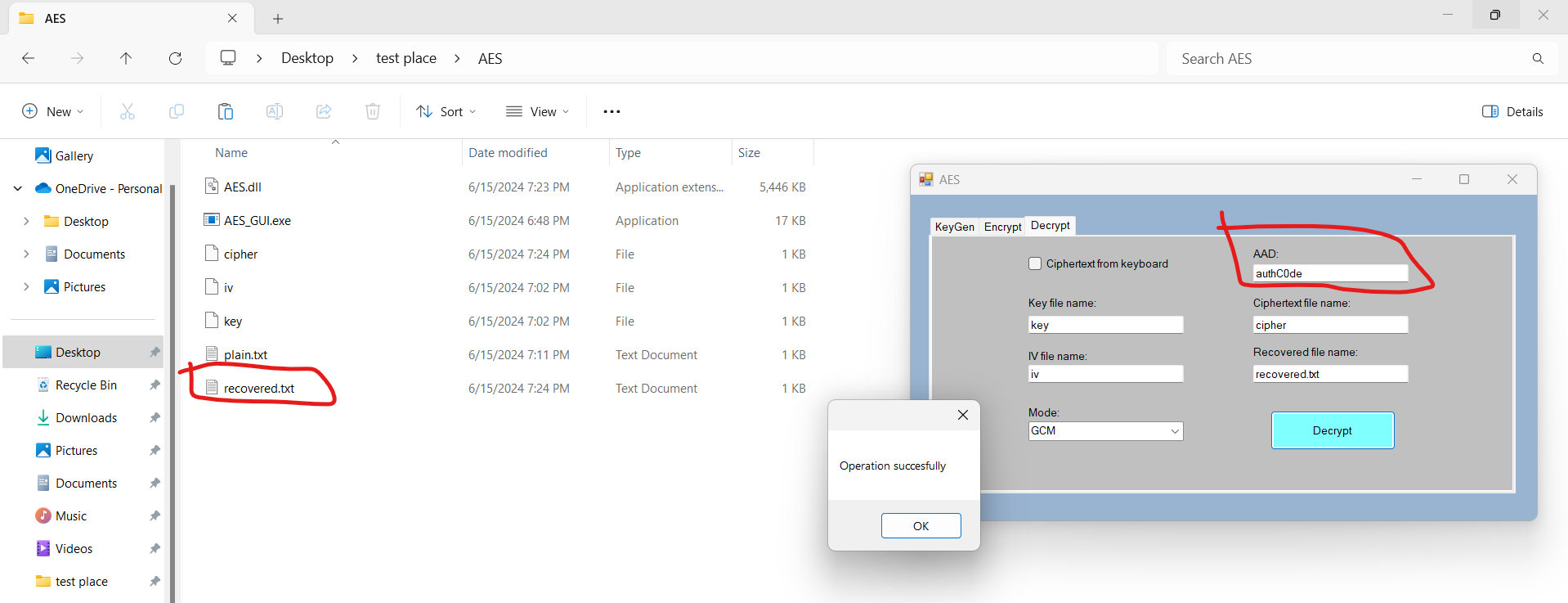
- Decrypt:

- Check:

3.2 GUI C# (Mode == GCM):

- Encrypt:

- Decrypt:



- Check:

