UNIVERSITY OF INFORMATION TECHNOLOGY
FACULTY OF COMPUTER NETWORK AND COMMUNICATION

REPORT
Subject: Cryptography

Report Lab 5

Lecturer: Nguyen Ngoc Tu

Report Lab 5

Student Information

Full Name: Trương Đức Hào

Student ID Number: 22520407

Class: ATTT2022.1

Device Information

CPU: AMD Ryzen7-5800H @ 3.2 GHz

Ram: 8 GB DDR4

SSD: 500GB

Display chip name: AMD Radeon Graphics – RTX 3050 NVIDIA

4.1 Gen Key:

```
D:\22520407_TruongDucHao_Lab4,5\Lab5\Task5>Task5.exe
Usage:
Task5.exe genkey <private key file> <public key file> <format>
Task5.exe signing <format> <private key file> <file name> <signature file>
Task5.exe verify <format> <public key file> <file name> <signature file>
<format>: [DER|PEM]

D:\22520407_TruongDucHao_Lab4,5\Lab5\Task5>Task5.exe genkey private.pem public.pem PEM
Generate key successfully
```

4.2 Signing:

```
D:\22520407_TruongDucHao_Lab4,5\Lab5\Task5>Task5.exe signing PEM private.pem test.txt signed.bin
Sign successfully
```

4.3 Verify:

```
D:\22520407_TruongDucHao_Lab4,5\Lab5\Task5>Task5.exe verify PEM public.pem test.txt signed.bin
Verify successfully
```

```
D:\22520407_TruongDucHao_Lab4,5\Lab5\Task5>Task5.exe
Running File Path: files/input1.txt
Finished File Path: files/input1.txt
Sign average: 11.442
Verify average: 11.073
Running File Path: files/input2.txt
Finished File Path: files/input2.txt
Sign average: 13.634
Verify average: 13.451
Running File Path: files/input3.txt
Finished File Path: files/input3.txt
Sign average: 12.792
Verify average: 11.968
Running File Path: files/input4.txt
Finished File Path: files/input4.txt
Sign average: 14.597
Verify average: 13.538
Running File Path: files/input5.txt
Finished File Path: files/input5.txt
Sign average: 47.823
Verify average: 41.286
Running File Path: files/input6.txt
Finished File Path: files/input6.txt
Sign average: 194.522
Verify average: 208.014
```

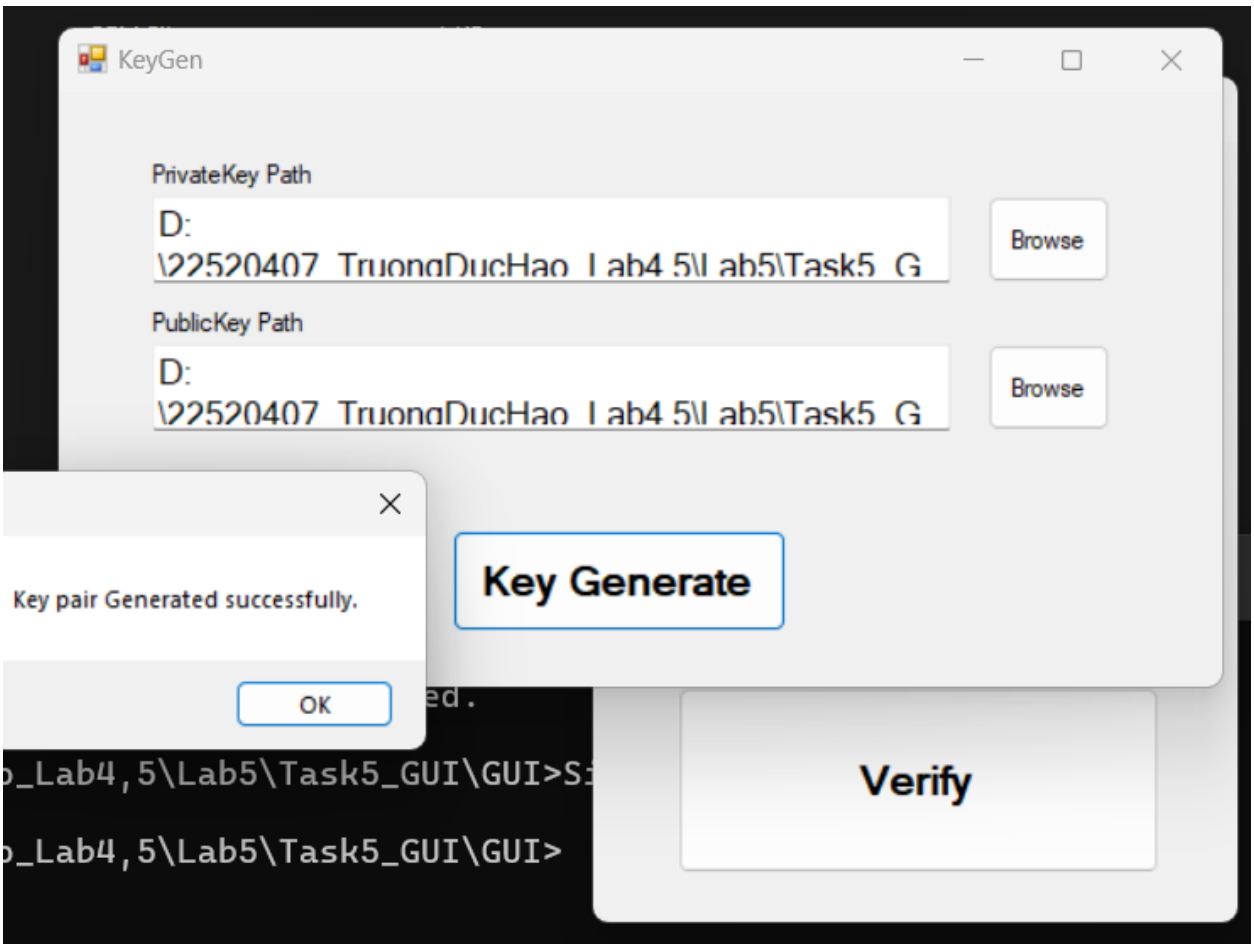
TimeCounter Mili seconds	Sign (Window)	Verify (Window)	Sign (Linux)	Verify (Linux)
1 KB	11.442	11.073	0.15ms	1.19ms
100 KB	13.634	13.451	0.117ms	1.17ms
200 KB	12.792	11.968	0.231ms	1.516ms
1000 KB	14.597	13.538	3.221ms	4.402ms
10000 KB	47.823	41.286	4.297ms	5.494ms
100000 KB	194.522	208.014	6.589ms	7.203ms

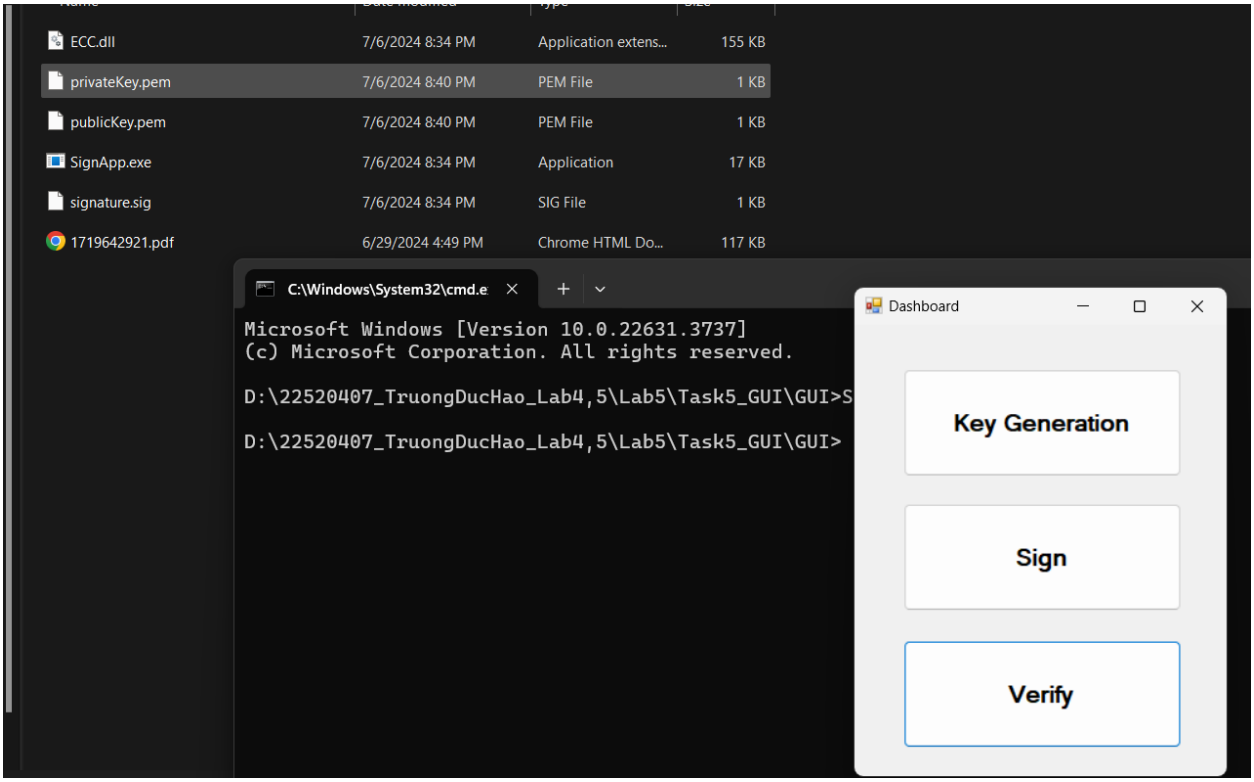
Nhận xét và so sánh:

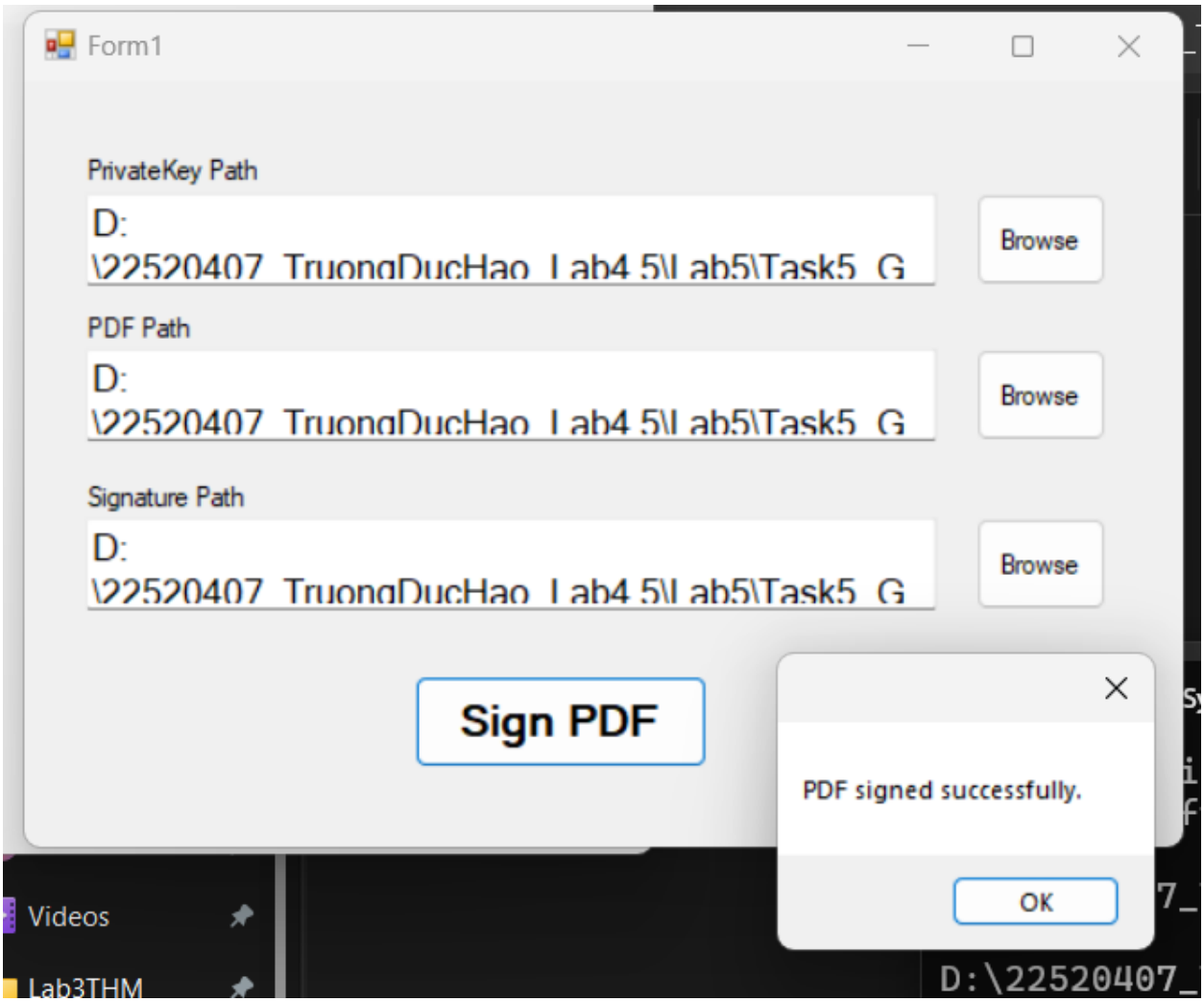
- Thời gian thực thi ở Linux nhanh hơn nhiều so với Windows, nguyên nhân có lẽ đến từ quản lý tài nguyên hệ thống của từng hệ điều hành.
- Thời gian signing ở Windows chậm hơn thời gian verify, ngược lại với Linux.

- Thời gian Verify và Signing ở Windows gần như bằng nhau.
- File đầu vào có kích thước càng lớn thời gian thực thi càng lâu (điều này khá hiển nhiên).

GUI:




ECC.dll 7/6/2024 8:34 PM Application extens... 155 KB
privateKey.pem 7/6/2024 8:40 PM PEM File 1 KB
publicKey.pem 7/6/2024 8:40 PM PEM File 1 KB
SignApp.exe 7/6/2024 8:34 PM Application 17 KB
signature.sig 7/6/2024 8:34 PM SIG File 1 KB
1719642921.pdf 6/29/2024 4:49 PM Chrome HTML Do... 117 KB
C:\Windows\System32\cmd.e
Microsoft Windows [Version 10.0.22631.3737]
(c) Microsoft Corporation. All rights reserved.
D:\22520407_TruongDucHao_Lab4,5\Lab5\Task5_GUI\GUI>S
D:\22520407_TruongDucHao_Lab4,5\Lab5\Task5_GUI\GUI>
Dashboard
Key Generation
Sign
Verify


Form1
PrivateKey Path
D:
\22520407_TruongDucHao_Lab4_5\Lab5\Task5_G
Browse
PDF Path
D:
\22520407_TruongDucHao_Lab4_5\Lab5\Task5_G
Browse
Signature Path
D:
\22520407_TruongDucHao_Lab4_5\Lab5\Task5_G
Browse
Sign PDF
PDF signed successfully.
OK
Videos
Lab3THM
D:\22520407_