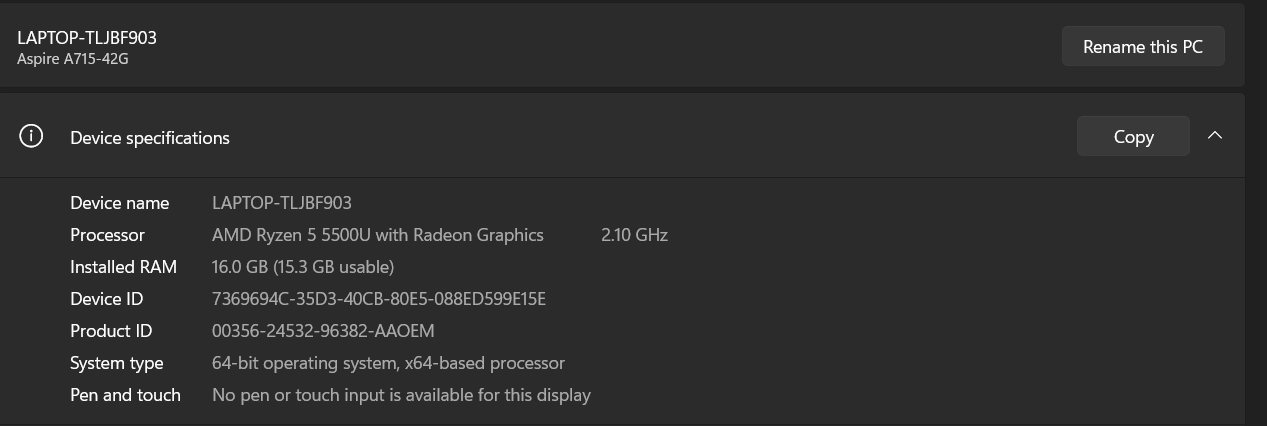
**REPORT TASK 4**

Môn: Mật mã học

Lớp: NT219.O22.ANTT

Giảng viên: Nguyễn Ngọc Tự

Sinh viên thực hiện: Nguyễn Tuấn Phát - 22521076

**\* Hardware resources**

**4.1 Hash Algorithms**

- Tổng quan:

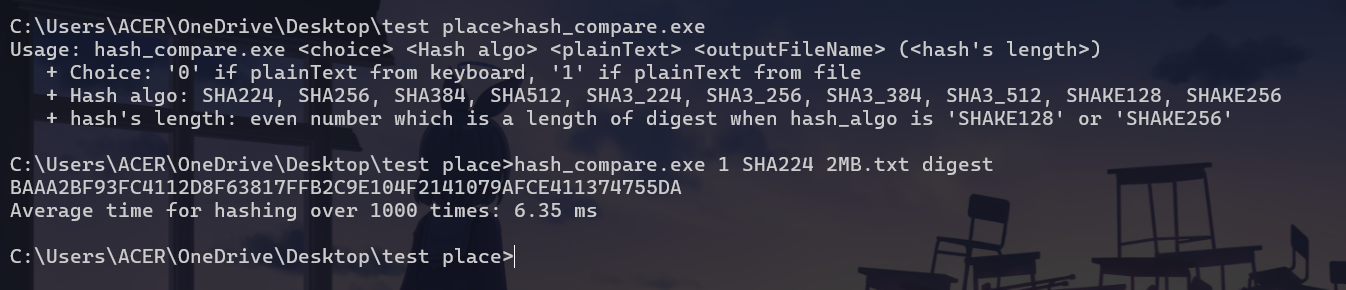
+ Cmd arguments, .dll, GUI C#

+ Vietnamese supported

+ input message from keyboard/file

+ algo supported: SHA224, SHA256, SHA384, SHA512, SHA3\_224, SHA3\_256, SHA3\_384, SHA3\_512, SHAKE128, SHAKE256

+ input digest length for SHAKE128 and SHAKE256



1. So sánh window, linux:

- So sánh thời gian hash giữa Window và Linux với 9 algo trên 6 file có kích thước lần lượt: 2MB, 10MB, 50MB, 250MB, 500MB, 1GB

+ Số lần chạy trung bình: 1000 lần

+ Đơn vị: milisecond (ms)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| WINDOW 11 | | | | | | |
| ALGO | 2MB | 10MB | 50MB | 250MB | 500MB | 1GB |
| SHA224 | 1.0 | 5.2 | 26.2 | 130.5 | 261.7 | 517.3 |
| SHA256 | 1.0 | 5.2 | 25.8 | 129.0 | 257.2 | 515.8 |
| SHA384 | 3.6 | 18.1 | 90.2 | 450.4 | 910.8 | 1935.7 |
| SHA512 | 3.7 | 19.6 | 113.7 | 513.8 | 910.7 | 1822.1 |
| SHA3\_224 | 4.9 | 25.0 | 123.6 | 636.8 | 1346.5 | 2503.3 |
| SHA3\_256 | 5.2 | 26.2 | 133.6 | 663.4 | 1349.7 | 2640.3 |
| SHA3\_512 | 11.8 | 50.4 | 248.2 | 1240.2 | 2490.4 | 5003.4 |
| SHAKE128 (64 bytes) | 4.2 | 22.3 | 106.1 | 533.1 | 1069.3 | 2129.2 |
| SHAKE256 (64 bytes) | 5.2 | 26.1 | 130.5 | 653.3 | 1307.9 | 2628.7 |

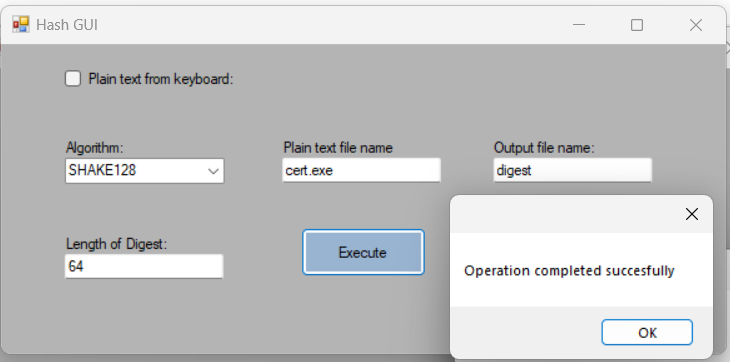
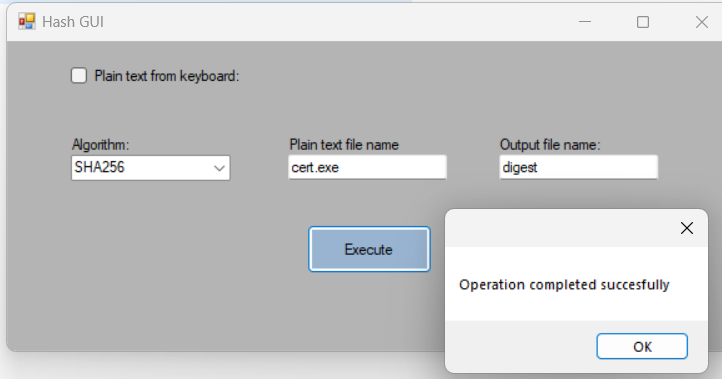
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| LINUX | | | | | | |
| ALGO | 2MB | 10MB | 50MB | 250MB | 500MB | 1GB |
| SHA224 | 1.0 | 5.1 | 25.6 | 128.2 | 256.7 | 516.9 |
| SHA256 | 1.0 | 5.2 | 25.6 | 128.5 | 256.8 | 515.3 |
| SHA384 | 3.7 | 18.6 | 93.2 | 470.6 | 939.7 | 1877.8 |
| SHA512 | 3.7 | 18.6 | 92.9 | 465.2 | 941.3 | 1882 |
| SHA3\_224 | 4.4 | 22.3 | 111 | 563.6 | 1109.1 | 2217.8 |
| SHA3\_256 | 4.7 | 23.4 | 117.5 | 588.7 | 1175.4 | 2351.5 |
| SHA3\_512 | 8.8 | 44.2 | 221.3 | 1105.7 | 2214.6 | 4428.3 |
| SHAKE128 (64 bytes) | 3.8 | 19.2 | 95.1 | 476.4 | 952.5 | 1905.1 |
| SHAKE256 (64 bytes) | 4.7 | 23.5 | 117.5 | 558 | 1175.9 | 2351.1 |

2. Nhận xét:

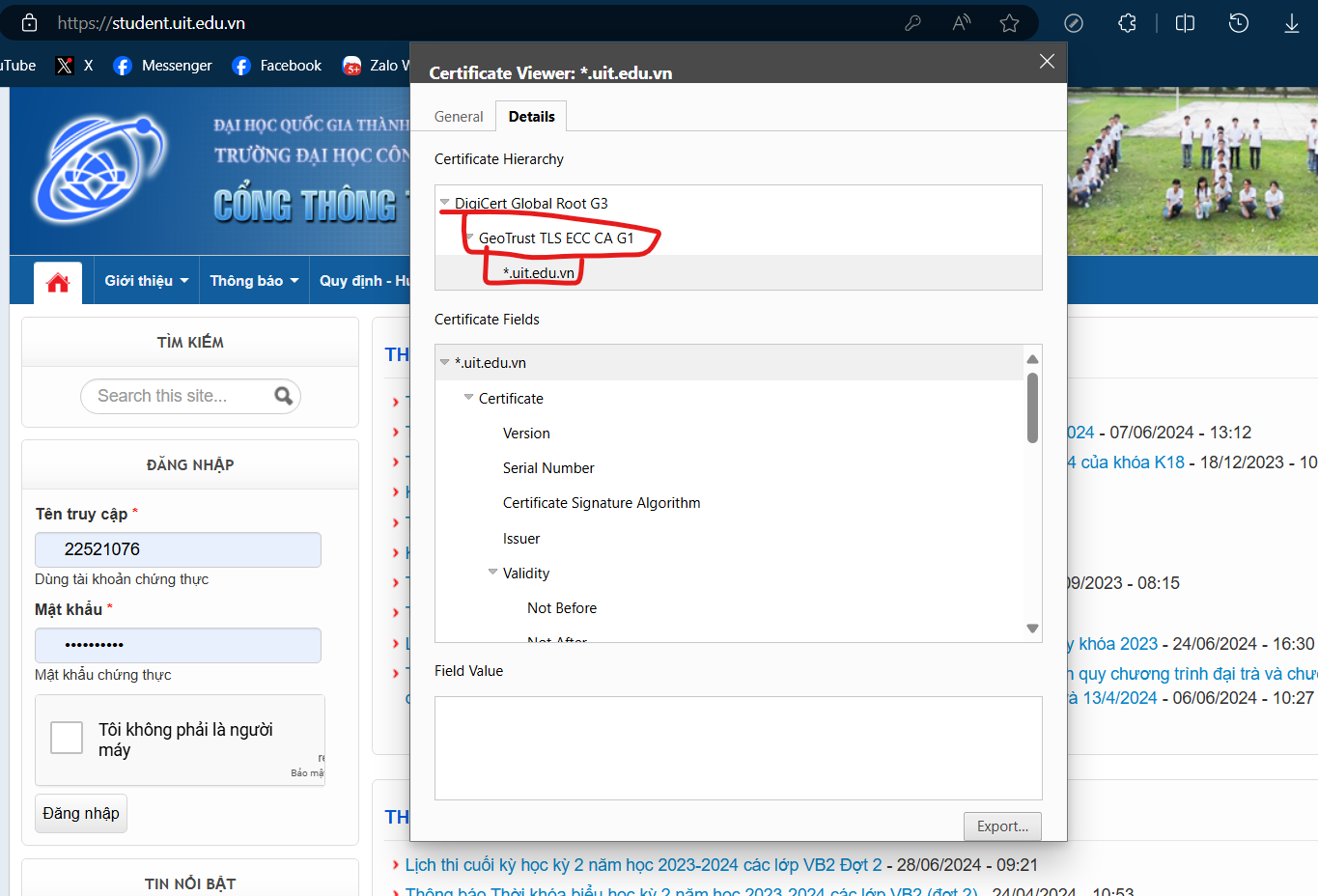
- Có thể dễ dàng nhận thấy, input càng lớn thì thời gian chạy càng tăng, chênh lệch thời gian khá nhiều khi file càng lớn. Các thuật toán hash càng phức tạp thì thời gian thực thi càng lâu.

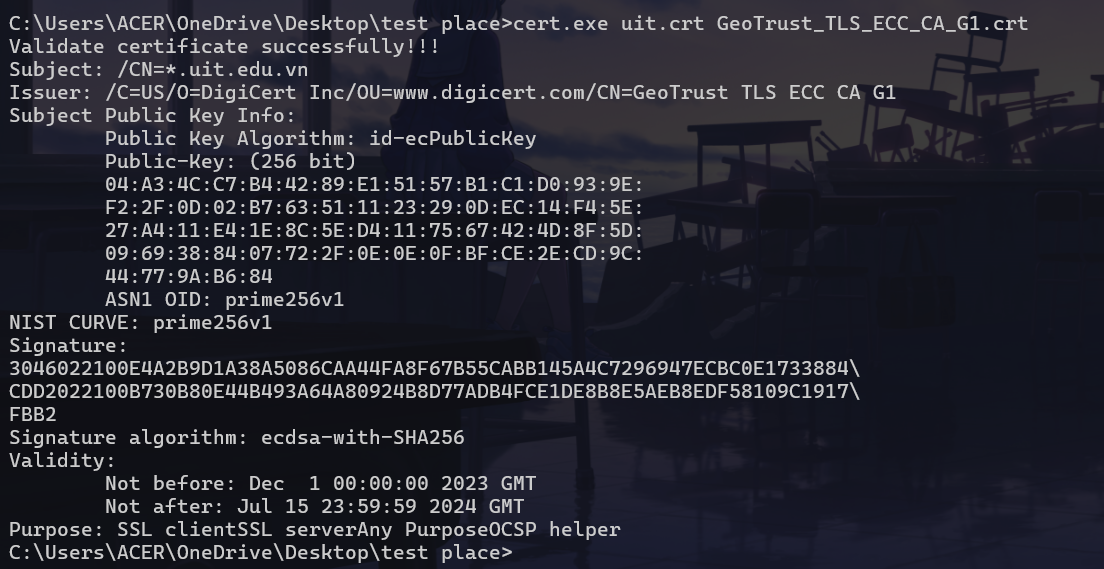
- Khi xét cùng một kích thước file, Linux thực thi nhanh hơn Window.

3. GUI



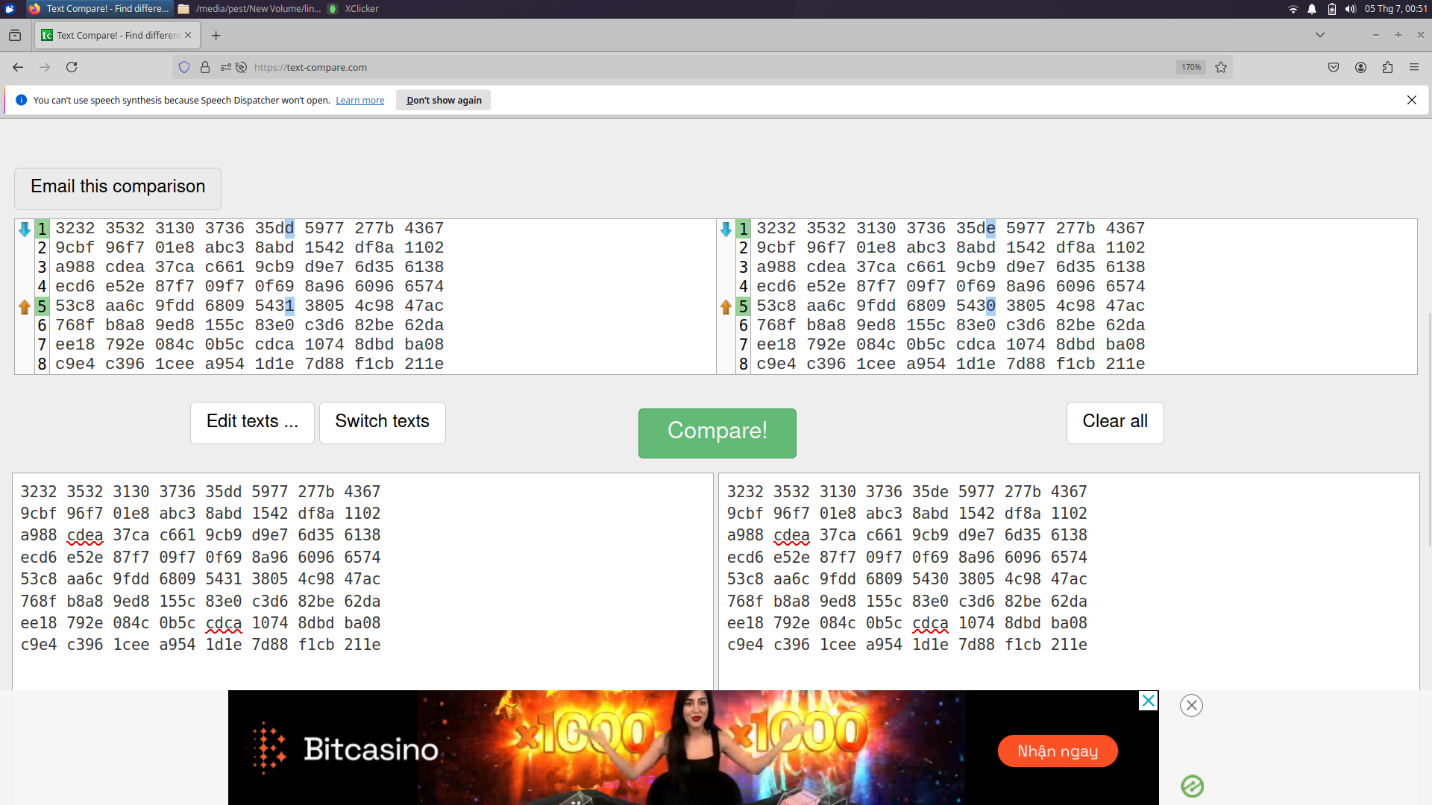
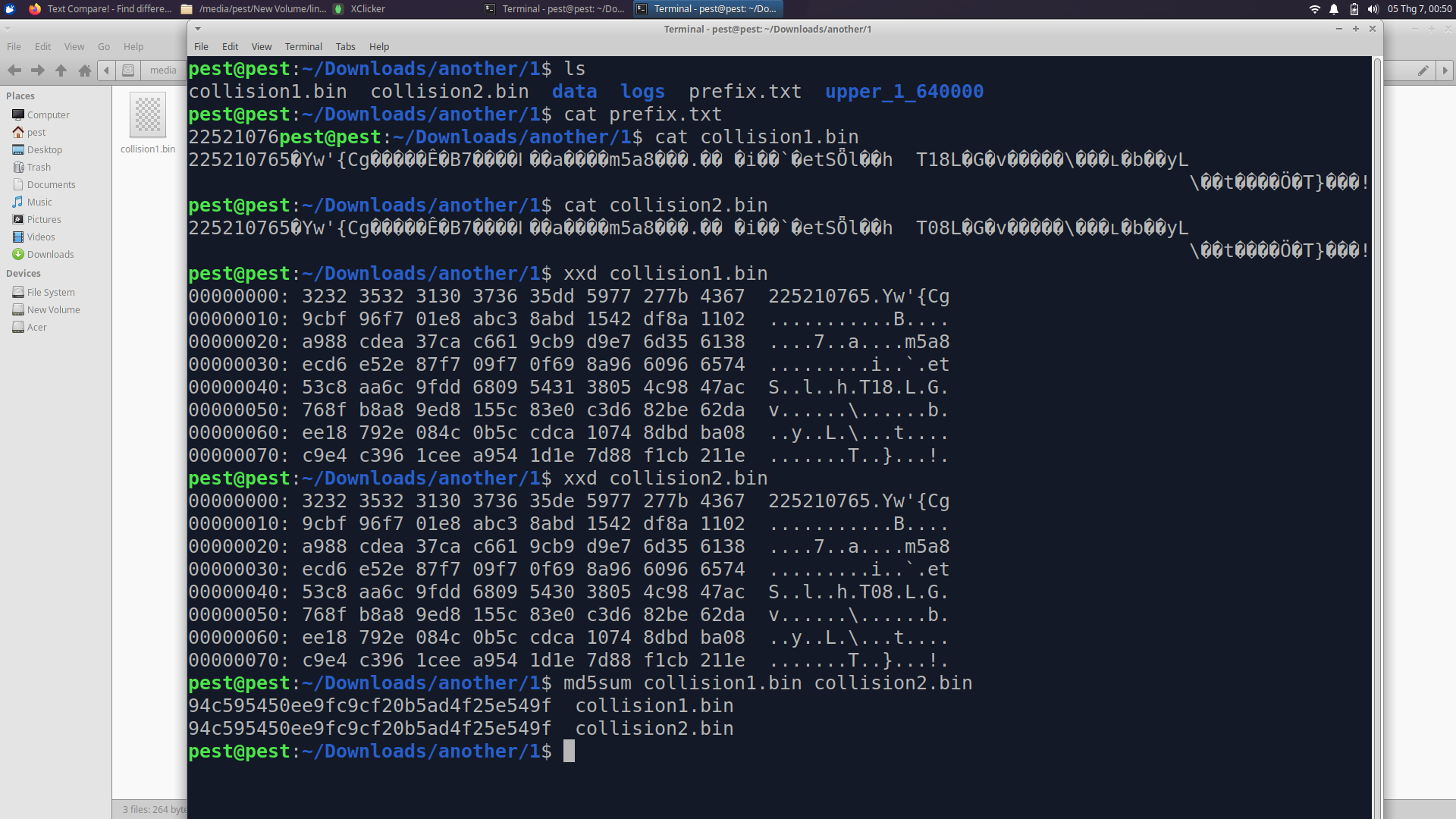
**4.2 PKI and digital certificate**

- Lên student.uit.edu.vn lấy certificate của uit.edu.vn và GeoTrust TLS ECC CA G1 về.

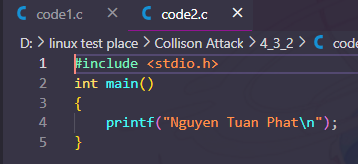
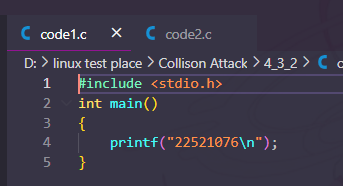
- Chạy chương trình để check cert, nếu validate thì in thông tin của cert:

**4.3 Collision and length extension attacks on Hash functions**

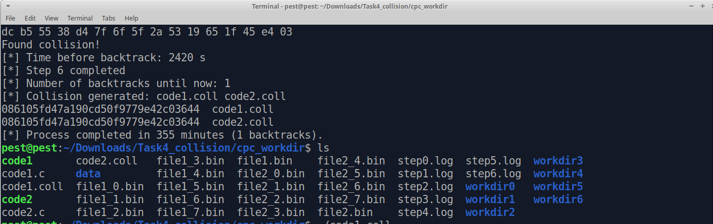
\* Two collision messages have the same prefix string

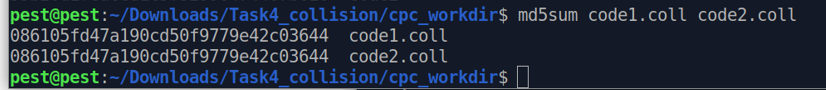
- Dùng hashclash để generate ra 2 file có cùng giá trị hash MD5 và có cùng prefix cho trước (22521076)

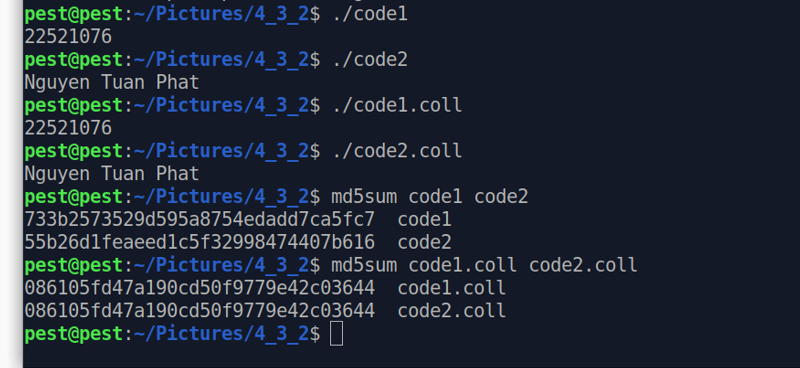
\* Two different C++ programs but have the same MD5;

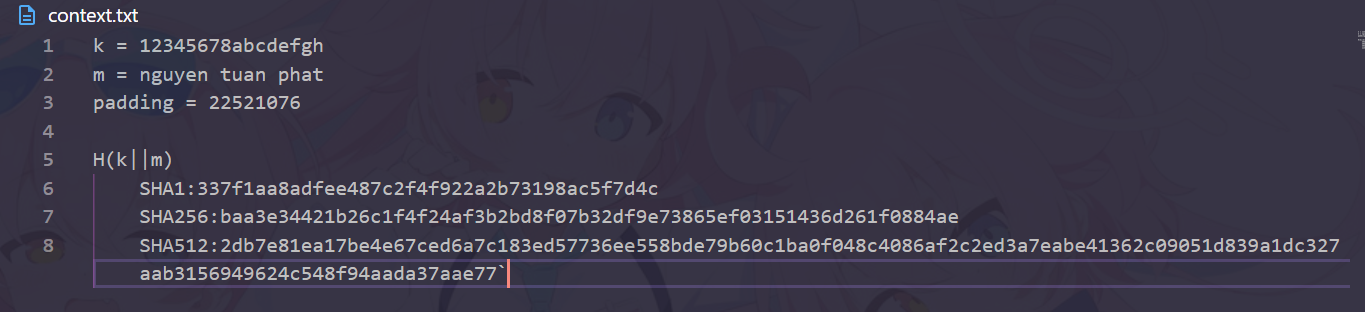
- 2 file code c đơn giản:

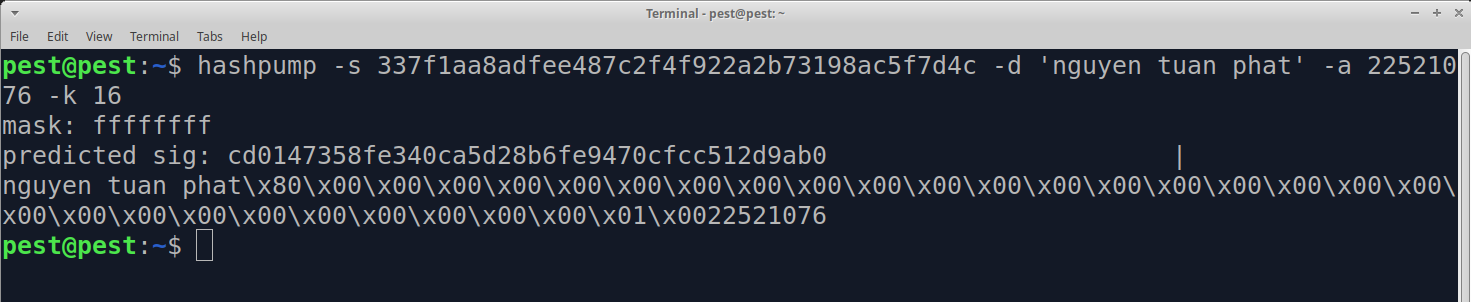
- Compile và check md5sum của 2 file:

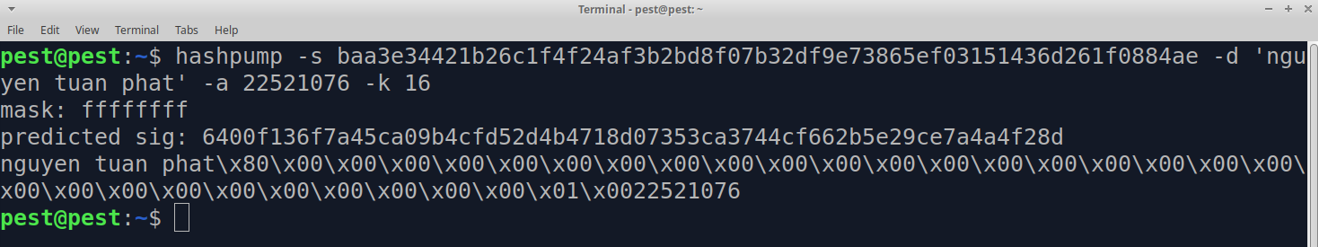
- Dùng tool hashclash để generate ra 2 file mới có chung hash MD5 nhưng lại thực hiện được chức năng khác nhau (mất 355 phút)

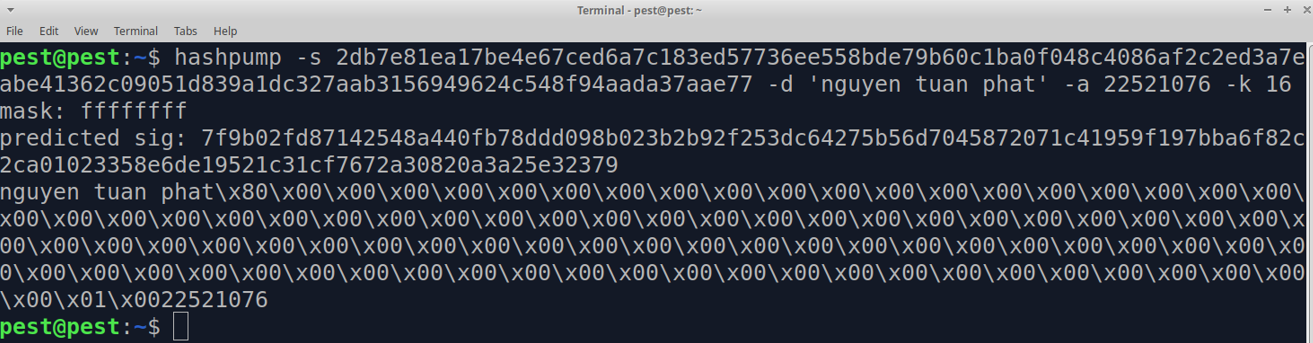
- Kiểm tra hash MD5 của 2 file mới được tạo:

- Thử thực thi:

**4.4 Length extension attacks on MAC  in form: H(k||m), k is secret key**

- SHA1

- SHA256

- SHA512