UNIVERSITY OF INFORMATION TECHNOLOGY

FACULTY OF COMPUTER NETWORK AND COMMUNICATION

Logo, company name

Description automatically generated

|  |  |
| --- | --- |
| Lecturer: | Nguyễn Ngọc Tự |
| Class: | NT219.O21.ANTT.2 |
| Student: | Trần Thế Hữu Phúc |
| Student ID Number: | 22521143 |

CRYPTOGRAPHY

Report Lab 4

PKI AND HASK FUNCTIONS

**Hồ Chí Minh City, June 2024**

# 1. Hardware Resources

|  |  |
| --- | --- |
| **Device** | MacBook Pro |
| **Chip** | Apple M1   * 8-core CPU * 8-core GPU * 16-core Neural Engine |
| **Memory** | 8GB LPDDR4 |
| **Storage** | 256GB SSD |
| **Operating Systems** | * macOS 14.5 Sonoma * Windows 11 Pro Version 23H2 * Ubuntu 22.04.4 LTS |

# 2. Nội dung thực hành

# 2.1. Task 4.1 - Hash Functions

| **Hashes on macOS (milisecconds)** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Algorithm** | 1MB | 128MB | 256MB | 512MB | 1GB |
| SHA244 | 10.210 | 685.581 | 1312.584 | 2558.079 | 5502.351 |
| SHA256 | 15.546 | 597.229 | 1136.327 | 2581.946 | 5563.693 |
| SHA384 | 8.676 | 782.069 | 1704.912 | 3413.875 | 7414.320 |
| SHA512 | 8.711 | 778.326 | 1537.318 | 3222.195 | 7198.348 |
| SHA3-224 | 8.105 | 701.007 | 1448.720 | 3033.958 | 6547.456 |
| SHA3-256 | 8.340 | 737.031 | 1478.542 | 3165.886 | 6741.554 |
| SHA3-384 | 8.489 | 811.146 | 1622.060 | 3401.734 | 7372.462 |
| SHA3-512 | 9.825 | 949.416 | 1884.840 | 3951.955 | 8472.205 |
| SHAKE128 | 7.737 | 682.606 | 1354.198 | 2947.605 | 6408.623 |
| SHAKE256 | 8.306 | 718.898 | 1500.900 | 3149.664 | 6527.109 |
| pasted-movie.png | | | | | |

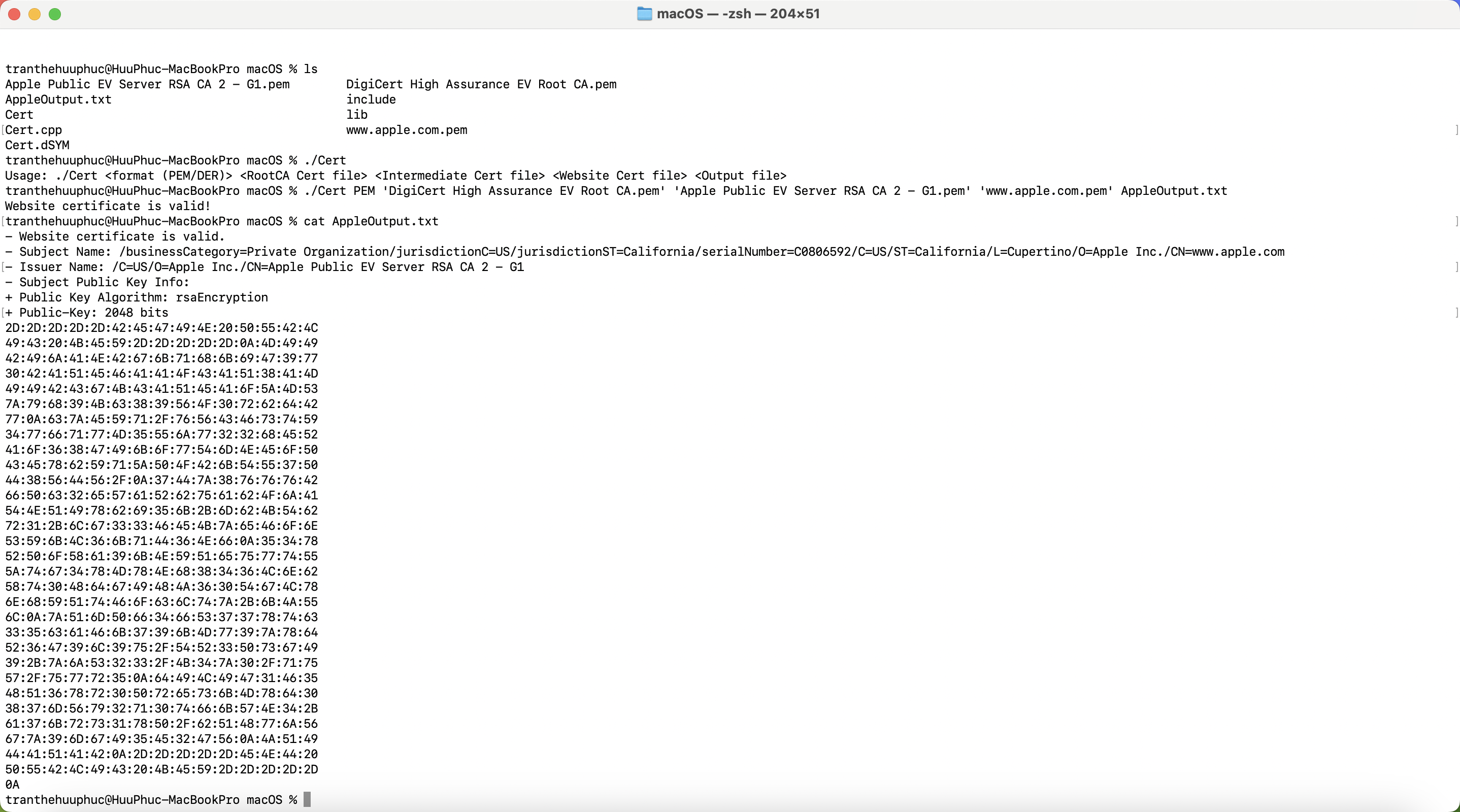
| **Hashes on Windows (milisecconds)** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Algorithm** | 1MB | 128MB | 256MB | 512MB | 1GB |
| SHA244 | 40.281 | 6975.308 | 12406.888 | 20552.470 | 48140.125 |
| SHA256 | 44.930 | 3667.596 | 8960.458 | 20700.544 | 43438.135 |
| SHA384 | 240.887 | 3097.685 | 8361.366 | 15840.299 | 35986.011 |
| SHA512 | 24.572 | 2625.058 | 8364.163 | 17152.380 | 47359.577 |
| SHA3-224 | 44.782 | 3236.513 | 6023.234 | 14452.976 | 32143.246 |
| SHA3-256 | 28.480 | 2323.125 | 4854.378 | 12339.293 | 37645.120 |
| SHA3-384 | 91.647 | 2779.569 | 7040.928 | 13327.062 | 34223.414 |
| SHA3-512 | 78.157 | 2814.647 | 6155.643 | 16861.408 | 35662.452 |
| SHAKE128 | 54.080 | 2812.712 | 6275.754 | 12967.962 | 31567.277 |
| SHAKE256 | 49.910 | 2865.933 | 6025.094 | 11956.503 | 27505.346 |
| pasted-movie.png | | | | | |

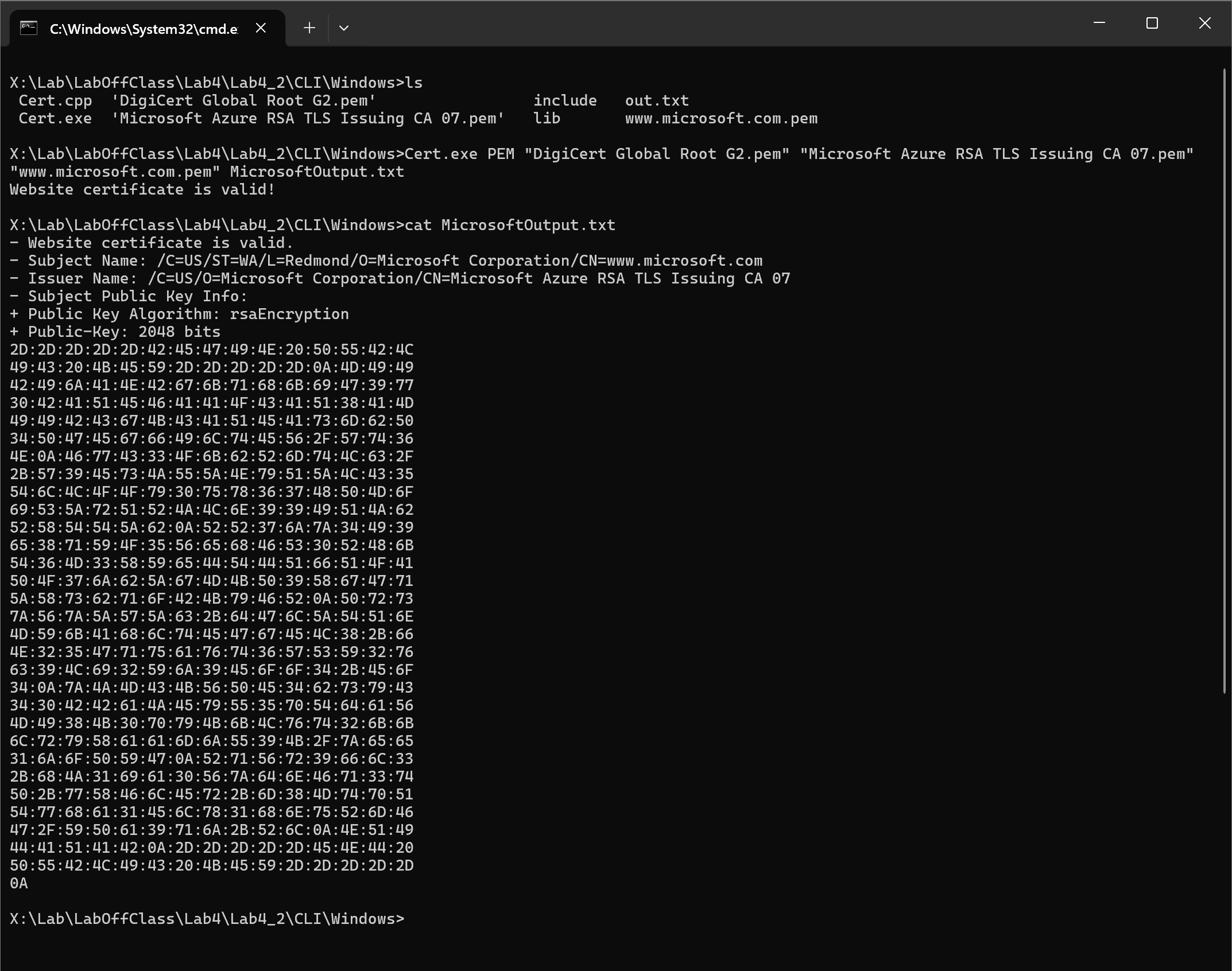
| **Hashes on Linux (milisecconds)** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Algorithm** | 1MB | 128MB | 256MB | 512MB | 1GB |
| SHA244 | 19.545 | 2001.504 | 3604.652 | 7708.738 | 20529.077 |
| SHA256 | 12.618 | 1703.131 | 3486.865 | 7864.551 | 26487.313 |
| SHA384 | 18.936 | 2066.204 | 4036.093 | 9767.283 | 23964.939 |
| SHA512 | 16.496 | 1966.837 | 3706.772 | 8482.769 | 25223.064 |
| SHA3-224 | 15.229 | 1904.379 | 4067.334 | 7899.868 | 25947.014 |
| SHA3-256 | 15.256 | 1947.085 | 3593.704 | 7819.240 | 24787.704 |
| SHA3-384 | 19.140 | 1888.384 | 3822.059 | 8239.696 | 23851.026 |
| SHA3-512 | 18.020 | 2098.999 | 4085.737 | 8959.649 | 23802.103 |
| SHAKE128 | 15.107 | 1838.470 | 3550.473 | 7438.861 | 22434.433 |
| SHAKE256 | 14.838 | 1828.092 | 3949.792 | 9581.485 | 23352.628 |
| pasted-movie.png | | | | | |

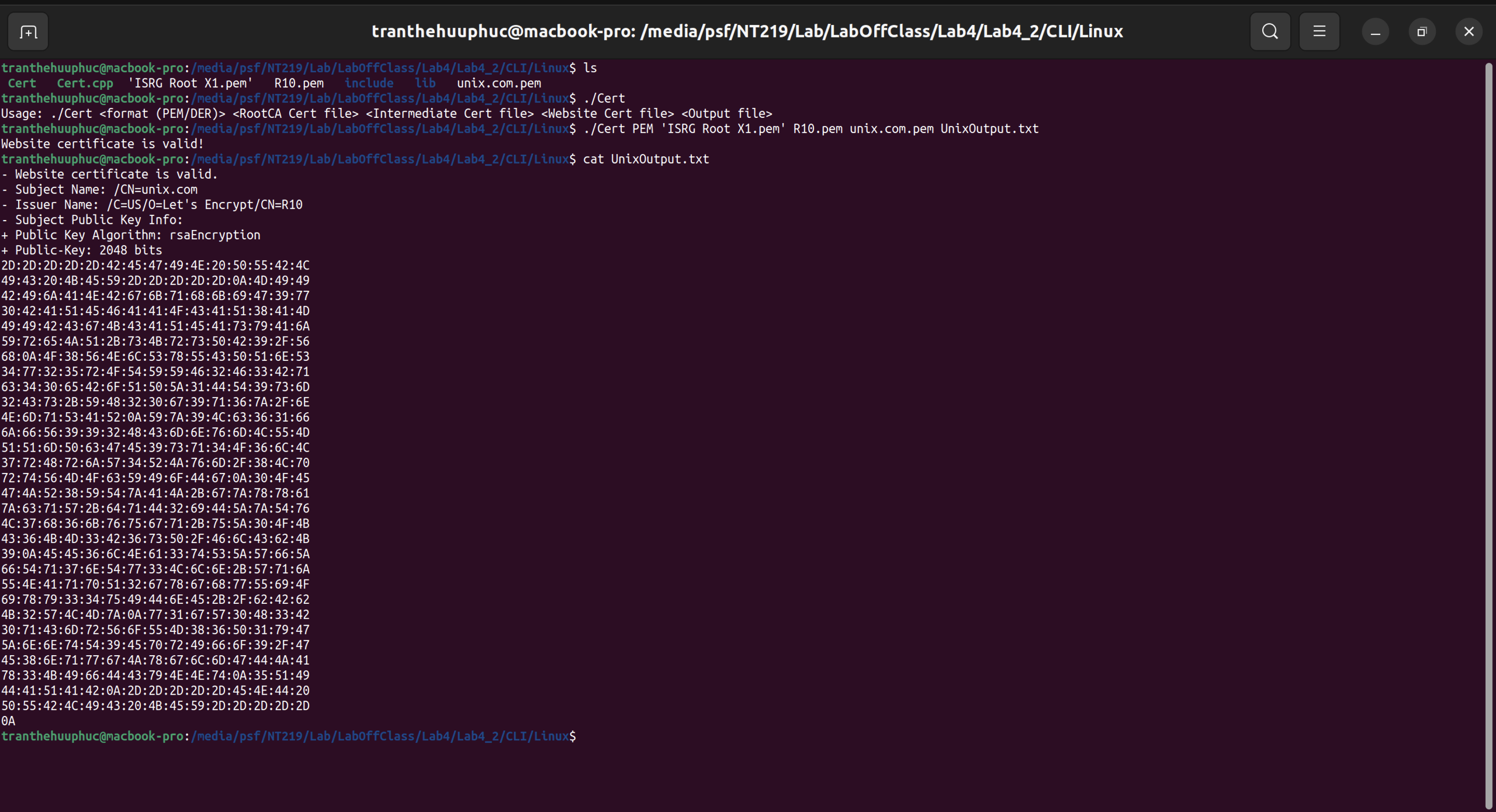
# ⌥ Phân tích và so sánh

* **Thời gian thực thi:**
  + - Trên Linux: Thời gian thực thi trung bình thấp hơn so với macOS và Windows đối với hầu hết các thuật toán và kích thước file. Điều này cho thấy hiệu suất thực thi trên Linux tốt hơn so với hai hệ điều hành còn lại.
    - Trên macOS: Thời gian thực thi cũng khá ổn định và thấp hơn so với Windows đối với nhiều thuật toán. Tuy nhiên, có một số thuật toán như SHA-224 và SHA-256 thì lại có thời gian thực thi trung bình cao hơn so với Linux.
    - Trên Windows: Thời gian thực thi trung bình cao nhất, đặc biệt là với các thuật toán như SHA-384 và SHA-512.
* **So sánh:**
  + - **SHA-256 và SHA3-256**: Cả ba hệ điều hành đều có thời gian thực thi tương đối gần nhau. Tuy nhiên, Windows có thời gian thực thi cao hơn một chút so với Linux và macOS.
    - **SHA-512**: Windows có thời gian thực thi cao nhất, trong khi Linux và macOS có thời gian thực thi tương đối gần nhau và thấp hơn.
    - **SHAKE128 và SHAKE256**: Windows có thời gian thực thi cao hơn rõ rệt so với Linux và macOS.
* **Thời gian chạy tăng theo kích thước file**: Tất cả các hàm băm đều có thời gian chạy tăng dần theo kích thước file. Điều này là hợp lý vì lượng dữ liệu cần xử lý tăng lên.

# 2.2. Task 4.2 - PKI and Digital Certificate

* Verify **apple.com** trên macOS:
* Verify **microsoft.com** trên Windows:



* Verify **unix.com** trên Linux:

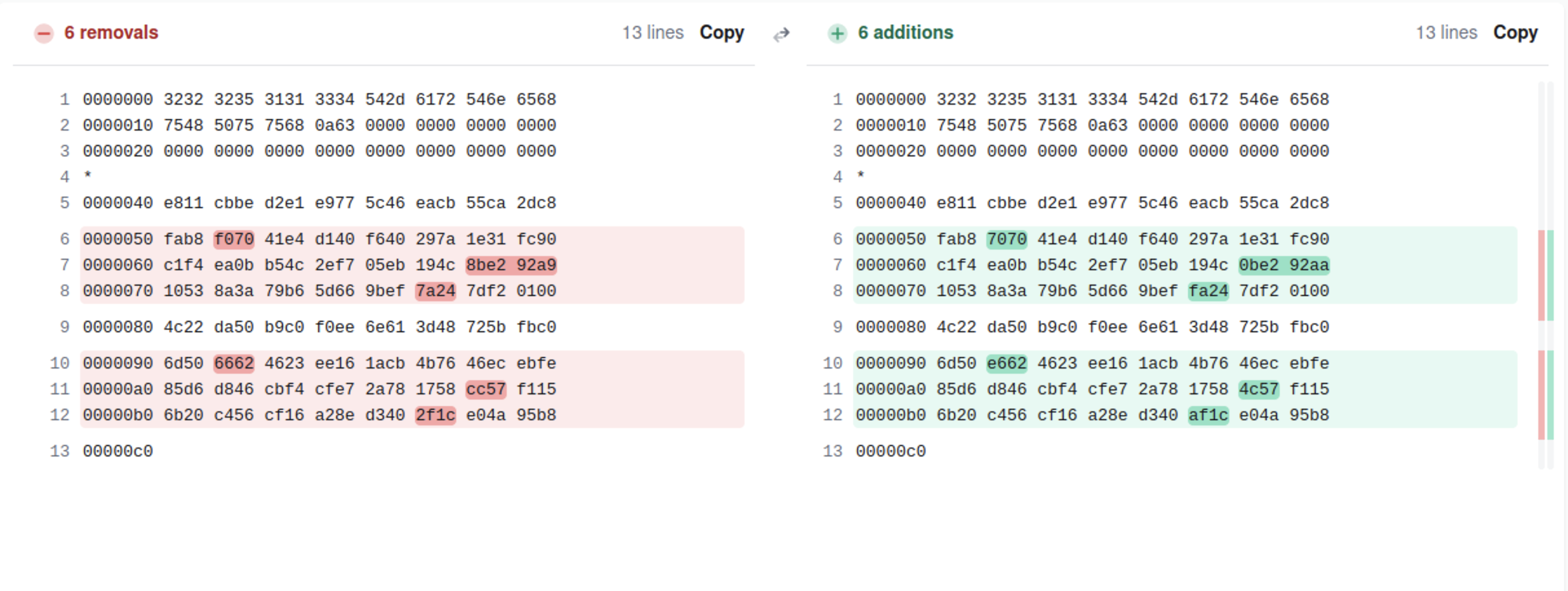
# 2.3. Task 4.3 - Collision and length extension attacks on Hash functions

# Task 4.3.1: Two collision messages have the same prefix string

# Generate.png

* Tạo prefix: **22521143-TranTheHuuPhuc**
* Dùng **md5\_fastcoll** để tạo 2 file khác nhau nhưng có cùng prefix và cùng MD5 digest.
* Dùng **md5sum** để tính và hiển thị MD5 digest của **attack1.bin** và **attack2.bin**.
* Dùng **hexdump** để xem giá trị hex, ta thấy 2 file có nội dung khác nhau tuy nhiên lại có cùng MD5 digest.

=> ***Collision***

******

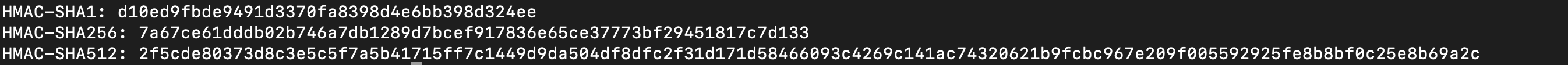
# Task 4.3.2: Two different C++ programs but have the same MD5:

# Compare.png

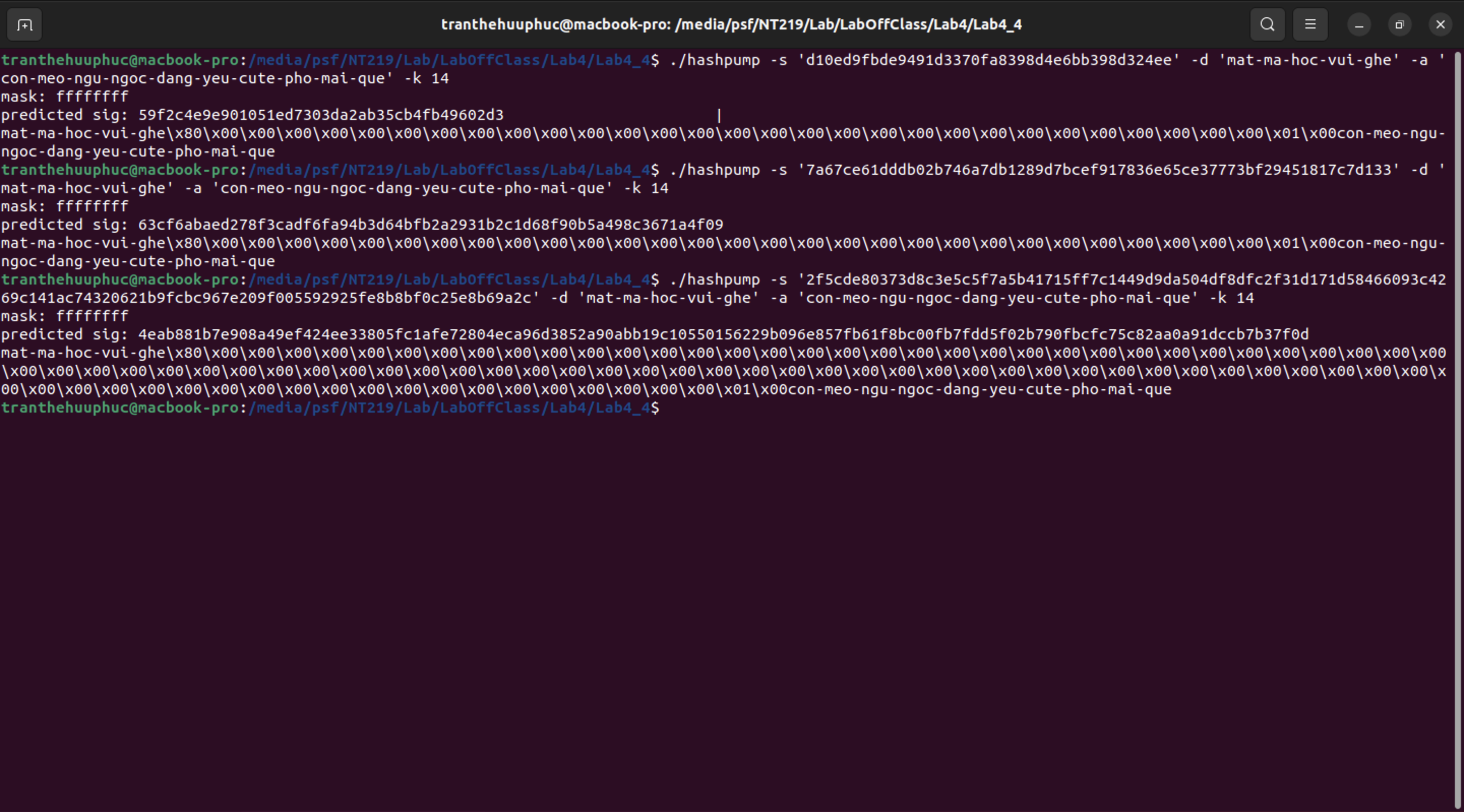
# 2.4. Task 4.4 - Length extension attacks on MAC in form: H(k||m), k is secret key

# Show length extension attacks on MAC using SHA1, SHA256, SHA512 using hashpump tool:

* Chạy **HMAC.py** để tạo các giá trị HMAC:



* Kết quả tấn công:



# Coding self programs that can attacks on MAC using SHA256:

# Compare.png