

UNIVERSITY OF INFORMATION TECHNOLOGY  
FACULTY OF COMPUTER NETWORK AND COMMUNICATION

---



# CRYPTOGRAPHY

## Report Lab 4

## PKI AND HASH FUNCTIONS

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

Hồ Chí Minh City, June 2024

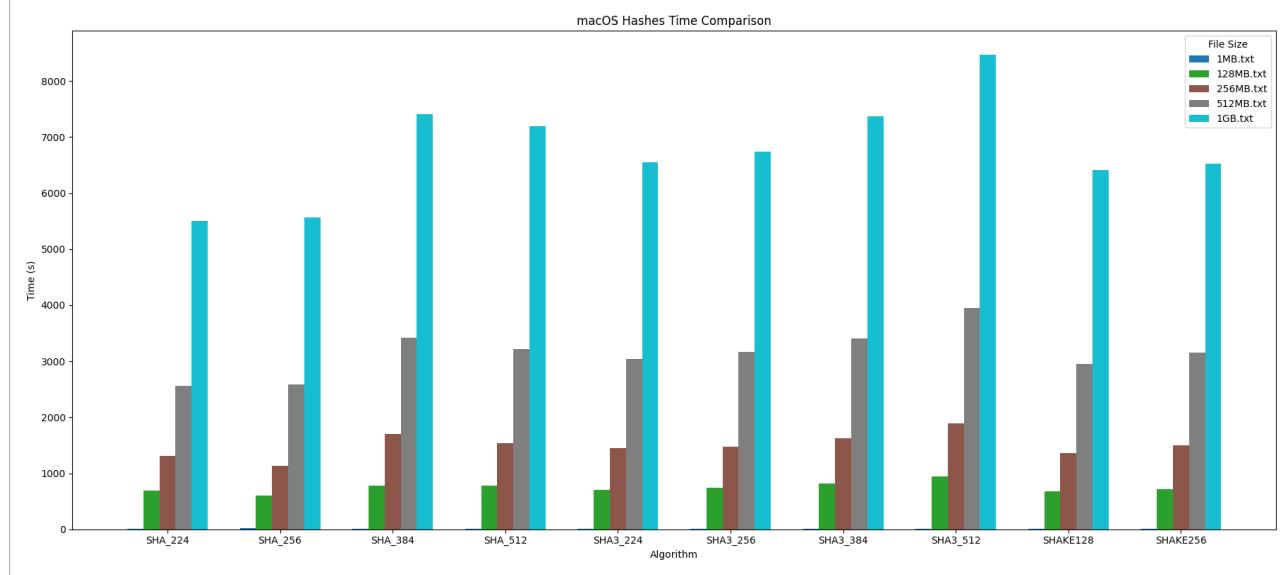
## 1. Hardware Resources

|                          |  |
|--------------------------|--|
| <b>Device</b>            | MacBook Pro  |
| <b>Chip</b>              | Apple M1 <ul style="list-style-type: none"><li>• 8-core CPU</li><li>• 8-core GPU</li><li>• 16-core Neural Engine</li></ul>             |
| <b>Memory</b>            | 8GB LPDDR4   |
| <b>Storage</b>           | 256GB SSD  |
| <b>Operating Systems</b> | <ul style="list-style-type: none"><li>• macOS 14.5 Sonoma</li><li>• Windows 11 Pro Version 23H2</li><li>• Ubuntu 22.04.4 LTS</li></ul> |

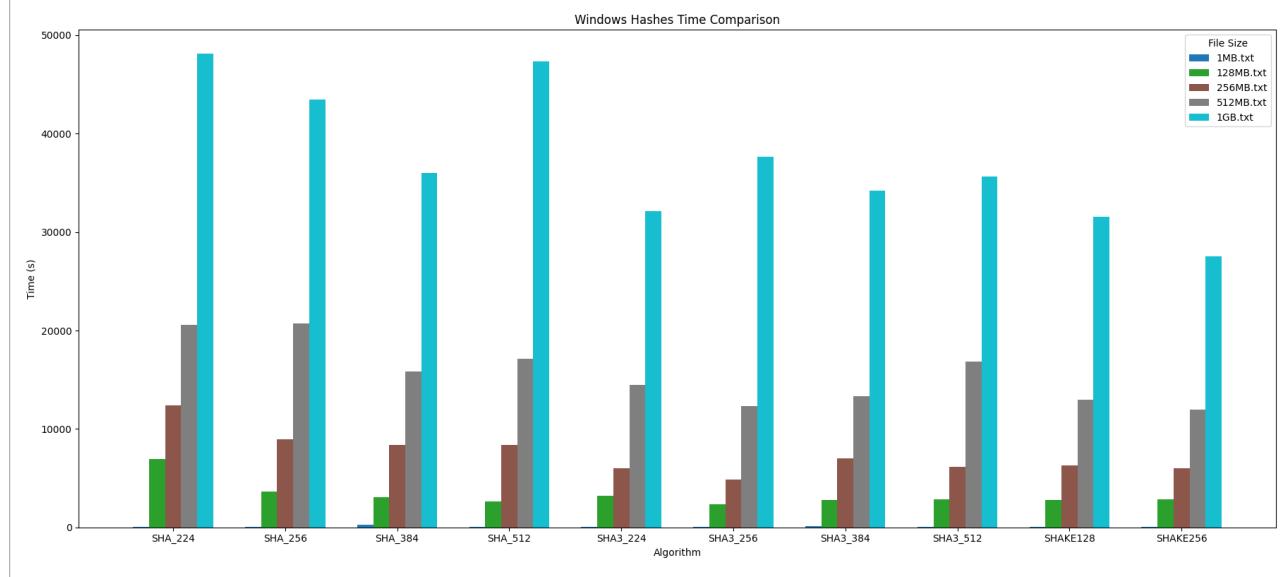
## 2. Nội dung thực hành

### 2.1. Task 4.1 - Hash Functions

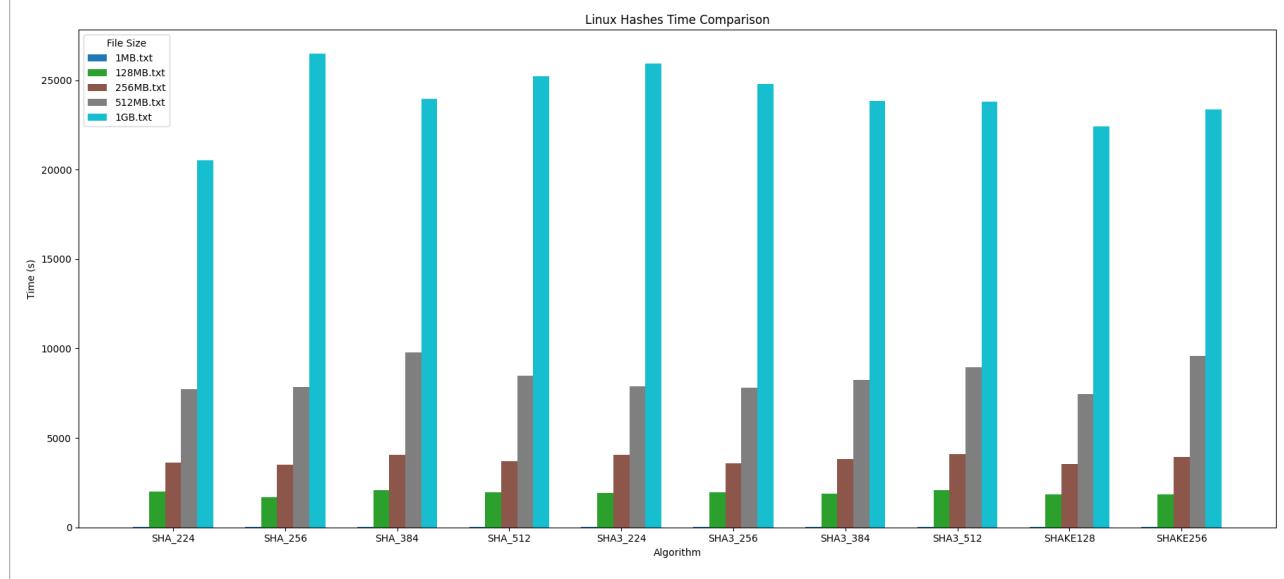
| Hashes on macOS (miliseconds) |        |         |          |          |          |
|-------------------------------|--------|---------|----------|----------|----------|
| Algorithm                     | 1MB    | 128MB   | 256MB    | 512MB    | 1GB      |
| SHA244                        | 10.210 | 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 |



| Hashes on Windows (miliseconds) |         |          |           |           |           |
|---------------------------------|---------|----------|-----------|-----------|-----------|
| 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 |



| Hashes on Linux (miliseconds) |        |          |          |          |           |
|-------------------------------|--------|----------|----------|----------|-----------|
| 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 |



## IV 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:

```

tranthehuuphuc@HuuPhuc-MacBookPro macOs % ls
Apple Public EV Server RSA CA 2 - G1.pem      DigiCert High Assurance EV Root CA.pem
AppleOutput.txt          include
Cert                           lib
Cert.cpp                     www.apple.com.pem
Cert.dSYM
tranthehuuphuc@HuuPhuc-MacBookPro macOs % ./Cert
Usage: ./Cert <format (PEM/DER)> <RootCA Cert file> <Intermediate Cert file> <Website Cert file> <Output file>
tranthehuuphuc@HuuPhuc-MacBookPro macOs % ./Cert PEM 'DigiCert High Assurance EV Root CA.pem' 'Apple Public EV Server RSA CA 2 - G1.pem' 'www.apple.com.pem' AppleOutput.txt
Website certificate is valid!
tranthehuuphuc@HuuPhuc-MacBookPro macOs % cat AppleOutput.txt
- Website certificate is valid.
- Subject Name: /businessCategory=Private Organization/jurisdictionC=US/jurisdictionST=California/serialNumber=C0806592/C=US/ST=California/L=Cupertino/O=Apple Inc./CN=www.apple.com
- Issuer Name: /C=US/O=Apple Inc./CN=Apple Public EV Server RSA CA 2 - G1
- Subject Public Key Info:
+ Public Key Algorithm: rsaEncryption
+ Public-Key: 2048 bits
2D:2D:2D:2D:42:45:47:49:4E:20:50:55:42:4C
49:43:20:4B:45:59:2D:2D:2D:2D:0A:4D:49:49
42:49:6A:41:4E:42:67:6B:68:6B:69:47:39:77
38:42:41:51:4C:43:44:43:44:4F:44:4D:44:41:40
49:45:43:42:47:48:41:51:49:41:6F:62:63:59
7A:79:68:71:4B:63:39:39:56:4F:38:72:62:44:42
77:0A:63:7A:45:59:71:2F:76:56:43:44:79:74:59
34:77:66:71:47:4D:35:55:6A:77:32:32:6B:45:52
41:46:36:38:47:49:6B:6F:77:54:4D:4E:45:45:52
33:45:78:67:59:71:5A:50:4F:42:48:54:55:37:58
44:38:56:44:56:2F:8A:37:44:7A:38:76:76:76:42
66:50:63:32:46:57:61:52:62:75:61:62:4F:6A:43
54:4E:51:49:78:62:69:35:6B:2B:62:62:4B:54:62
72:31:2B:6C:67:33:33:46:45:4B:7A:65:46:6F:6E
53:59:6B:4D:36:6B:71:44:36:4E:66:8A:35:34:78
52:50:6F:5B:61:39:6B:4E:59:51:65:75:77:74:55
5A:74:67:34:78:4D:78:4E:6B:38:34:36:4C:6E:62
58:74:30:4B:64:67:49:48:4A:36:38:54:67:4C:78
6E:68:59:51:74:46:6F:63:6C:74:7A:2B:6B:8A:55
6C:9A:7A:51:6D:50:66:34:66:53:37:37:78:74:63
33:35:63:61:46:6B:37:39:6B:4D:77:39:7A:78:64
52:36:47:39:6C:39:75:2F:54:52:33:50:73:67:49
39:2B:7A:6A:53:32:33:2F:4B:34:7A:30:2F:71:75
57:2F:75:77:72:35:9A:44:49:4C:49:47:31:46:35
48:51:36:78:72:38:58:72:65:73:6B:4D:78:64:38
38:37:6D:56:79:32:71:38:74:66:6B:67:4E:34:2B
61:37:6B:72:73:31:78:50:2F:62:51:77:77:6A:56
67:71:4A:39:6D:67:49:38:45:32:47:56:84:4A:51:49
40:41:51:41:42:9A:2D:2D:2D:2D:45:4E:44:28
50:58:42:4C:49:43:2B:48:45:59:2D:2D:2D:2D:2D
0A
tranthehuuphuc@HuuPhuc-MacBookPro macOs %

```

- Verify **microsoft.com** trên Windows:

```

C:\Windows\System32\cmd.e  X + 
X: \Lab\LabOffClass\Lab4\Lab4_2\CLI\Windows>ls
Cert.cpp   'DigiCert Global Root G2.pem'           include    out.txt
Cert.exe   'Microsoft Azure RSA TLS Issuing CA 07.pem' lib      www.microsoft.com.pem

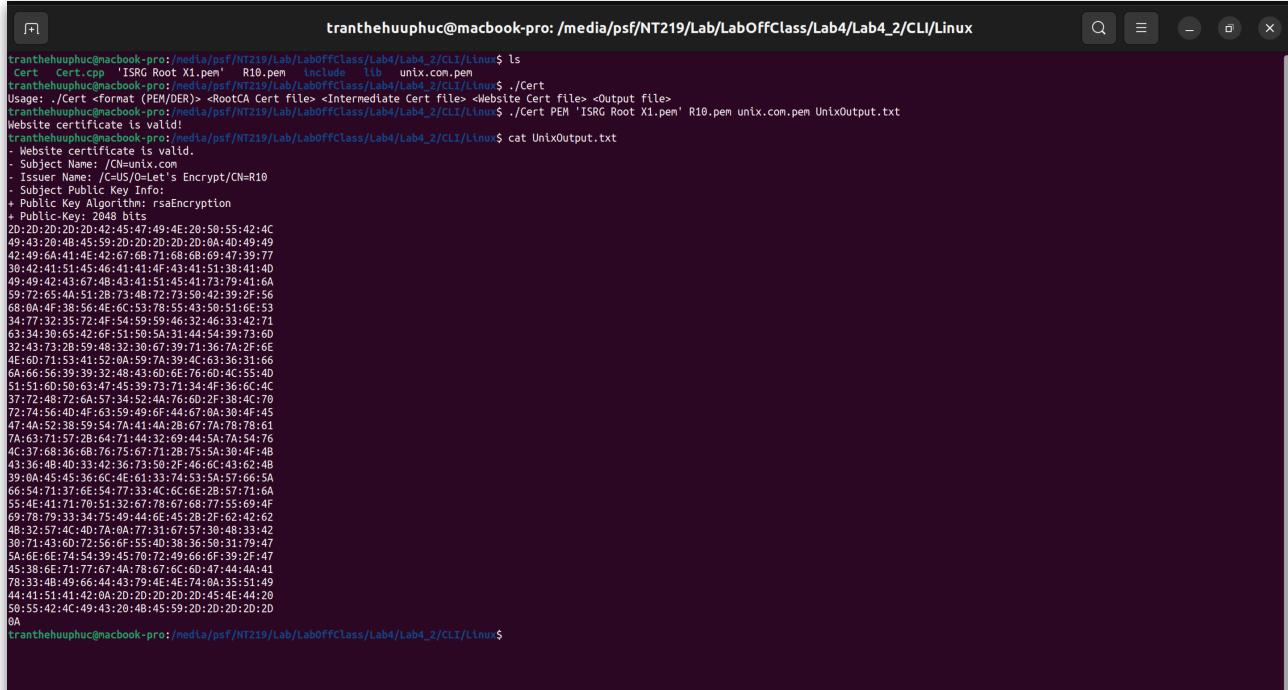
X:\Lab\LabOffClass\Lab4\Lab4_2\CLI\Windows>Cert.exe PEM "DigiCert Global Root G2.pem" "Microsoft Azure RSA TLS Issuing CA 07.pem" "www.microsoft.com.pem" MicrosoftOutput.txt
Website certificate is valid!

X:\Lab\LabOffClass\Lab4\Lab4_2\CLI\Windows>cat MicrosoftOutput.txt
- Website certificate is valid.
- Subject Name: /C=US/ST=WA/L=Redmond/O=Microsoft Corporation/CN=www.microsoft.com
- Issuer Name: /C=US/O=Microsoft Corporation/CN=Microsoft Azure RSA TLS Issuing CA 07
- Subject Public Key Info:
+ Public Key Algorithm: rsaEncryption
+ Public-Key: 2048 bits
2D:2D:2D:2D:42:45:47:49:4E:20:50:55:42:4C
49:43:20:4B:45:59:2D:2D:2D:2D:0A:4D:49:49
42:49:6A:41:4E:42:67:6B:68:6B:69:47:39:77
30:42:41:51:45:46:41:41:4F:43:41:51:38:41:4D
49:49:42:43:67:4B:43:41:51:45:41:73:6D:62:50
34:50:47:45:67:66:49:46:74:45:56:2F:57:74:36
4E:0A:46:77:43:33:4F:6B:62:52:6D:74:4C:63:2F
2B:57:39:45:73:4A:55:5A:4E:79:51:5A:4C:43:35
54:6C:4C:4F:4F:79:30:75:78:36:37:48:50:4D:6F
69:53:5A:72:51:52:4A:4C:6E:39:39:49:51:4A:62
52:58:54:54:5A:62:0A:52:52:37:6A:7A:34:49:39
65:38:71:59:4F:35:56:65:68:46:53:30:52:48:6B
54:36:4D:33:58:59:65:44:54:44:51:66:51:4F:41
50:4F:37:6A:62:5A:67:4D:4B:50:39:58:67:47:71
5A:58:73:62:71:6F:42:4B:79:46:52:20:A5:72:73
7A:56:7A:5A:57:5A:63:2B:64:47:6C:5A:54:51:6E
4D:59:6B:41:68:6C:74:45:47:67:45:4C:38:2B:66
4E:32:35:47:71:75:61:76:74:36:57:53:59:32:76
63:39:4C:69:32:59:6A:39:45:6F:6F:34:2B:45:6F
34:0A:7A:4A:4D:43:4B:56:50:45:34:62:73:79:43
34:30:42:42:61:4A:45:79:55:35:70:54:64:61:56
4D:49:38:4B:30:70:79:4B:6B:4C:76:74:32:6B:6B
6C:72:79:58:61:61:6D:6A:55:39:4B:2F:7A:65:65
31:6A:6F:50:59:47:0A:52:71:56:72:39:66:6C:33
2B:68:4A:31:69:61:30:56:7A:64:6E:46:71:33:74
50:2B:77:58:46:6C:45:72:2B:6D:38:4D:74:70:51
54:77:68:61:31:45:6C:78:31:68:6E:75:52:6D:46
47:2F:59:50:61:39:71:6A:2B:52:6C:0A:4E:51:49
44:41:51:41:42:0A:2D:2D:2D:2D:45:4E:44:20
50:55:42:4C:49:43:2B:48:45:59:2D:2D:2D:2D:2D
0A
X:\Lab\LabOffClass\Lab4\Lab4_2\CLI\Windows>

```

## Cryptography - Lab 4

- Verify **unix.com** trên Linux:

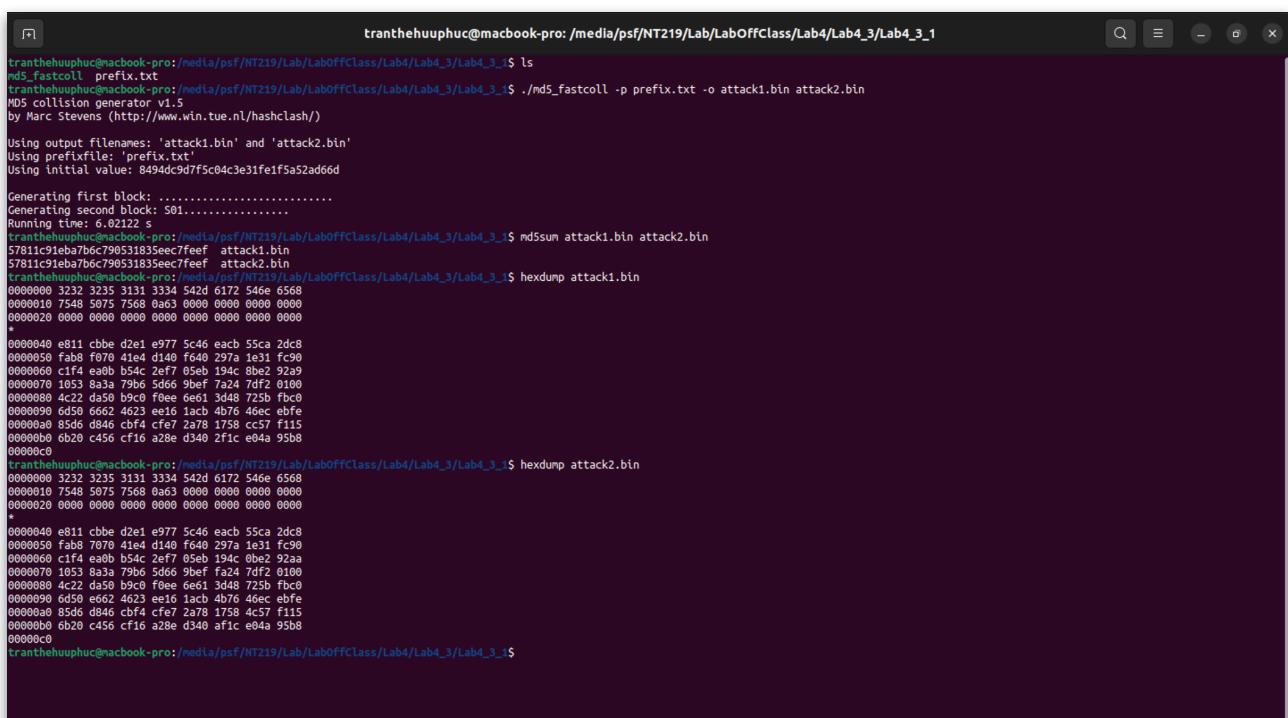


```
tranthehuuphuc@macbook-pro: /media/psf/NT219/Lab/LabOffClass/Lab4/Lab4_2/CLI/Linux$ openssl s_client -connect unix.com:443 > /tmp/sslcert
Cert is self signed
-----
-----
```

Cert: Cert.Cpp 'ISRG Root X1.pem' R10.pem include lib unix.com.pem  
tranthehuuphuc@macbook-pro: /media/psf/NT219/Lab/LabOffClass/Lab4/Lab4\_2/CLI/Linux\$ ./Cert  
Usage: ./Cert <format (PEM/DER> <RootCA Cert file> <Intermediate Cert file> <Website Cert file> <Output file>  
tranthehuuphuc@macbook-pro: /media/psf/NT219/Lab/LabOffClass/Lab4/Lab4\_2/CLI/Linux\$ ./Cert PEM 'ISRG Root X1.pem' R10.pem unix.com.pem UnixOutput.txt  
Website certificate is valid!  
tranthehuuphuc@macbook-pro: /media/psf/NT219/Lab/LabOffClass/Lab4/Lab4\_2/CLI/Linux\$ cat UnixOutput.txt  
-----  
Website certificate is valid.  
- Website Name: /CN=unix.com  
- Issuer Name: /C=US/O=Let's Encrypt/CN=R10  
- Subject Public Key Info:  
+ Public Key Algorithm: rsaEncryption  
Public-Key: 2048 bits  
-----  
0D:00:2D:2D:0B:42:45:47:49:4E:20:59:55:42:4C  
49:43:41:45:46:43:20:2D:2D:0A:40:39:49  
42:49:6A:41:4E:42:67:6B:71:68:6B:69:47:39:77  
30:42:41:51:45:46:41:41:4F:43:41:51:38:41:4D  
49:49:42:42:43:67:4B:43:41:51:45:41:73:79:41:6A  
59:72:65:4A:51:2B:73:4B:72:73:50:42:39:2F:56  
68:0A:4F:38:56:4E:OC:53:78:55:43:50:51:6E:53  
34:77:32:35:72:4F:54:59:59:46:32:46:33:42:71  
63:34:30:65:42:6F:51:50:5A:31:44:54:39:73:6D  
32:43:73:2B:59:48:32:30:67:39:71:36:7A:2F:6E  
4E:6D:71:53:41:52:0A:59:7A:39:4C:63:36:31:66  
6A:66:56:39:39:32:48:43:60:61:76:6D:4C:55:4D  
51:51:60:50:63:47:45:39:73:71:34:4F:36:6C:4C  
37:72:48:72:6A:57:34:52:4A:76:6D:2F:38:4C:70  
72:74:56:45:63:67:6A:63:44:4F:46:49:39:4F:45  
74:74:38:59:41:7A:41:44:20:67:7A:39:51:61  
7A:63:71:57:2B:64:71:44:32:69:44:5A:7A:54:76  
4C:37:69:36:6B:76:75:67:71:2B:75:5A:39:4F:4B  
43:36:4B:4D:33:42:36:73:59:2F:46:6C:43:62:4B  
39:8A:45:45:36:6C:4E:61:33:74:53:5A:57:66:5A  
66:54:71:37:6E:54:77:33:4C:6E:2B:57:71:6A  
55:4E:41:71:70:51:32:67:78:67:68:77:55:69:4F  
69:78:79:33:34:75:49:44:6E:45:2B:2F:62:42:62  
4B:32:57:4C:4D:7A:0A:77:31:67:57:30:4B:33:42  
30:71:43:6D:72:56:6F:55:4D:30:36:50:31:79:47  
5A:6E:6E:74:54:39:45:70:72:49:66:6F:39:2F:47  
45:38:6E:71:77:67:4A:78:67:6C:6D:47:44:4A:41  
78:33:4B:49:66:44:43:79:4E:4E:74:0A:35:51:49  
44:41:51:41:42:0A:2D:2D:2D:2D:45:4E:40:20  
50:55:42:4C:49:43:20:4B:45:59:2D:2D:2D:20  
0A  
tranthehuuphuc@macbook-pro: /media/psf/NT219/Lab/LabOffClass/Lab4/Lab4\_2/CLI/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



```
tranthehuuphuc@macbook-pro: /media/psf/NT219/Lab/LabOffClass/Lab4/Lab4_3/Lab4_3_1$ ls
md5_fastcoll prefix.txt
tranthehuuphuc@macbook-pro: /media/psf/NT219/Lab/LabOffClass/Lab4/Lab4_3/Lab4_3_1$ ./md5_fastcoll -p prefix.txt -o attack1.bin attack2.bin
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

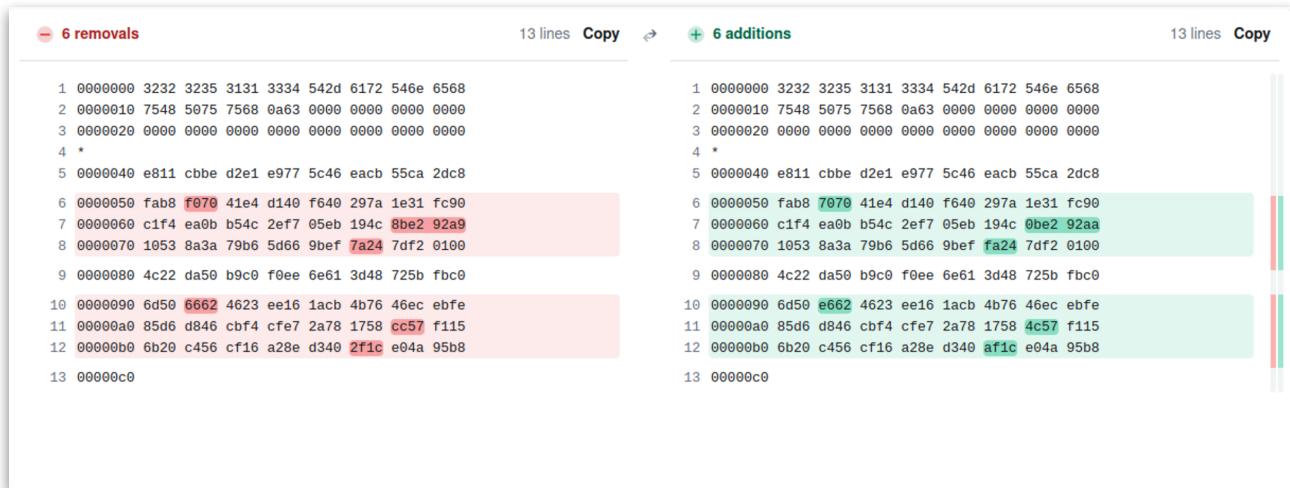
Using output filenames: 'attack1.bin' and 'attack2.bin'
Using prefixfile: 'prefix.txt'
Using initial value: 8494dc9d7f5c04c3e31feff5a52ad66d

Generating first block: .....
Generating second block: $01.....
Running time: 6.02122 s
tranthehuuphuc@macbook-pro: /media/psf/NT219/Lab/LabOffClass/Lab4/Lab4_3/Lab4_3_1$ md5sum attack1.bin attack2.bin
57811c91eba7bc790531835ec7feef attack1.bin
57811c91eba7bc790531835ec7feef attack2.bin
tranthehuuphuc@macbook-pro: /media/psf/NT219/Lab/LabOffClass/Lab4/Lab4_3/Lab4_3_1$ hexdump attack1.bin
00000000 3232 3235 3131 3334 542d 6172 546e 6568
00000010 7548 5075 7568 0a63 0000 0000 0000 0000
00000020 0000 0000 0000 0000 0000 0000 0000 0000
* 
00000040 e811 cbbe d2e1 e977 5c46 eacb 55ca 2dc8
00000050 fab8 7f70 41e4 d140 f640 297a 1e31 fc90
00000060 c1f4 ea0b b54c 2ef7 05eb 194e 0be2 92a9
00000070 1053 8a3a 79b6 5d66 9be7 fa24 7df2 0100
00000080 4c22 d5a0 b9c0 f0ee 6e61 3d4d 725b fbc0
00000090 6d50 6662 4623 ee16 1acb 4b76 46ec ebfe
000000a0 85d6 0846 cbf4 cf7e 2a78 1758 cc57 f115
000000b0 6b20 c456 cf16 a28e d340 af1c e04a 95bb
000000c0
tranthehuuphuc@macbook-pro: /media/psf/NT219/Lab/LabOffClass/Lab4/Lab4_3/Lab4_3_1$ hexdump attack2.bin
00000000 3232 3235 3131 3334 542d 6172 546e 6568
00000010 7548 5075 7568 0a63 0000 0000 0000 0000
00000020 0000 0000 0000 0000 0000 0000 0000 0000
* 
00000040 e811 cbbe d2e1 e977 5c46 eacb 55ca 2dc8
00000050 fab8 7f70 41e4 d140 f640 297a 1e31 fc90
00000060 c1f4 ea0b b54c 2ef7 05eb 194e 0be2 92aa
00000070 1053 8a3a 79b6 5d66 9be7 fa24 7df2 0100
00000080 4c22 d5a0 b9c0 f0ee 6e61 3d4d 725b fbc0
00000090 6d50 6662 4623 ee16 1acb 4b76 46ec ebfe
000000a0 85d6 0846 cbf4 cf7e 2a78 1758 cc57 f115
000000b0 6b20 c456 cf16 a28e d340 af1c e04a 95bb
000000c0
tranthehuuphuc@macbook-pro: /media/psf/NT219/Lab/LabOffClass/Lab4/Lab4_3/Lab4_3_1$
```

- 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**.

## Cryptography - Lab 4

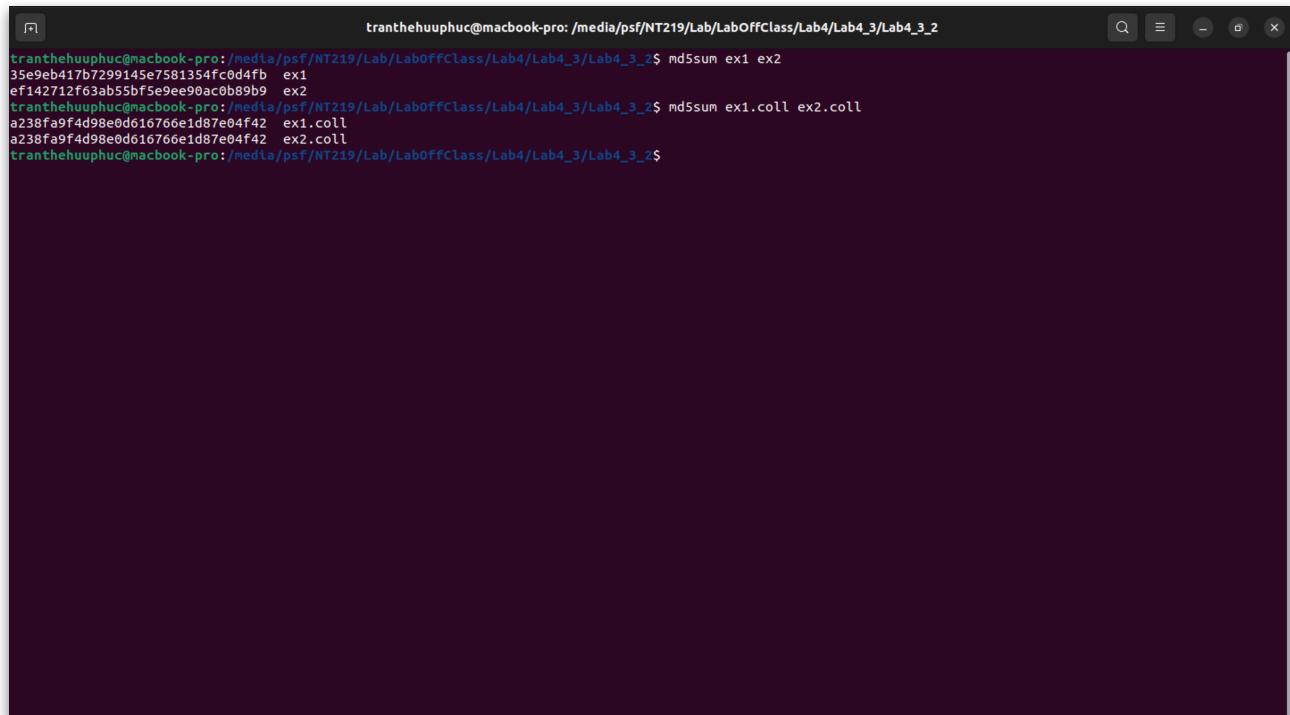
- Dùng **hexdump** để xem giá trị hex, ta thấy 2 file có nội dung khác nhau tuy nhiên lại có cùng MD5 digest.  
=> **Collision**



The screenshot shows a hex editor interface with two panes. The left pane displays a file with 6 removals, and the right pane displays a file with 6 additions. Both files have the same MD5 digest. The hex values are shown in pairs of four digits, with some specific bytes highlighted in red or green boxes.

| Left File (6 removals)  | Right File (6 additions)  |
|---|---|
| 1 0000000 3232 3235 3131 3334 542d 6172 546e 6568               | 1 0000000 3232 3235 3131 3334 542d 6172 546e 6568               |
| 2 0000010 7548 5075 7568 0a63 0000 0000 0000 0000               | 2 0000010 7548 5075 7568 0a63 0000 0000 0000 0000               |
| 3 0000020 0000 0000 0000 0000 0000 0000 0000 0000               | 3 0000020 0000 0000 0000 0000 0000 0000 0000 0000               |
| 4 *   | 4 *   |
| 5 0000040 e811 cbbe d2e1 e977 5c46 eacb 55ca 2dc8               | 5 0000040 e811 cbbe d2e1 e977 5c46 eacb 55ca 2dc8               |
| 6 0000050 fab8 <b>f070</b> 41e4 d140 f640 297a 1e31 fc90        | 6 0000050 fab8 <b>7070</b> 41e4 d140 f640 297a 1e31 fc90        |
| 7 0000060 c1f4 ea0b b54c 2ef7 05eb 194c <b>8be2</b> <b>92a9</b> | 7 0000060 c1f4 ea0b b54c 2ef7 05eb 194c <b>0be2</b> <b>92aa</b> |
| 8 0000070 1053 8a3a 79b6 5d66 9bef <b>7a24</b> 7df2 0100        | 8 0000070 1053 8a3a 79b6 5d66 9bef <b>fa24</b> 7df2 0100        |
| 9 0000080 4c22 da50 b9c0 f0ee 6e61 3d48 725b fb0                | 9 0000080 4c22 da50 b9c0 f0ee 6e61 3d48 725b fb0                |
| 10 0000090 6d50 <b>6662</b> 4623 ee16 1acb 4b76 46ec ebfe       | 10 0000090 6d50 <b>e662</b> 4623 ee16 1acb 4b76 46ec ebfe       |
| 11 00000a0 85d6 d846 cbf4 cfe7 2a78 1758 <b>cc57</b> f115       | 11 00000a0 85d6 d846 cbf4 cfe7 2a78 1758 <b>4c57</b> f115       |
| 12 00000b0 6b20 c456 cf16 a28e d340 <b>2f1c</b> e04a 95b8       | 12 00000b0 6b20 c456 cf16 a28e d340 <b>af1c</b> e04a 95b8       |
| 13 00000c0  | 13 00000c0  |

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



```
tranthehuuphuc@macbook-pro: /media/psf/NT219/Lab/LabOffClass/Lab4/Lab4_3/Lab4_3_2$ md5sum ex1 ex2
35e9eb417b7299145e7581354fc0d4fb ex1
ef142712f63ab5b5f5e9e90ac0b89b9 ex2
tranthehuuphuc@macbook-pro: /media/psf/NT219/Lab/LabOffClass/Lab4/Lab4_3/Lab4_3_2$ md5sum ex1.coll ex2.coll
a238fa9f4d98e0d616766e1d87e04f42 ex1.coll
a238fa9f4d98e0d616766e1d87e04f42 ex2.coll
tranthehuuphuc@macbook-pro: /media/psf/NT219/Lab/LabOffClass/Lab4/Lab4_3/Lab4_3_2$
```

## **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:

HMAC-SHA1: d10ed9fbdbe9491d3370fa8398d4e6bb398d324ee  
HMAC-SHA256: 7a67ce61ddd7b46a7db1987d1fb9ef17836e65ce37773bf29451817c7d133  
HMAC-SHA512: 2f5ed08373dc83e57f5ab41715ff744949da504df8dfc2f31d71d5846693c4269c141ac74320621b9fcbc967e209f005592925fe8b8bf0c25e8b69a2c

- #### - Kết quả tấn công:

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