REPORT CRYTOGRAPHY –TASK 4

Student: Trịnh Thị Bích Thảo

ID: 22521376

Lecturer: Nguyễn Ngọc Tự

---

1. Hardware resources.

a. Windows

Current Date/Time:	Friday, June 14, 2024, 9:38:15 AM
Computer Name:	SEIPIEH
Operating System:	Windows 11 Home Single Language 64-bit (10.0, Build 22631)
Language:	English (Regional Setting: English)
System Manufacturer:	ASUSTeK COMPUTER INC.
System Model:	VivoBook_ASUSLaptop X421EAY_A415EA
BIOS:	X421EAY.308
Processor:	11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz (8 CPUs), ~2.4GHz
Memory:	8192MB RAM
Page file:	11903MB used, 11341MB available
DirectX Version:	DirectX 12

b. Linux (ubuntu)

```
sei@TrinhThiBichThao-22521376:~$ lscpu
Architecture:                    x86_64
CPU op-mode(s):                  32-bit, 64-bit
Byte Order:                      Little Endian
Address sizes:                   39 bits physical, 48 bits virtual
CPU(s):                          8
On-line CPU(s) list:             0-7
Thread(s) per core:              2
Core(s) per socket:              4
Socket(s):                       1
NUMA node(s):                    1
Vendor ID:                       GenuineIntel
CPU family:                      6
Model:                           140
Model name:                      11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz
Stepping:                        1
CPU MHz:                         2400.000
CPU max MHz:                     4200,0000
CPU min MHz:                     400,0000
BogoMIPS:                        4838.40
Virtualization:                  VT-x
L1d cache:                       192 KiB
L1i cache:                       128 KiB
L2 cache:                        5 MiB
L3 cache:                        8 MiB
NUMA node0 CPU(s):               0-7
```

2. Giới thiệu.

- Bài báo cáo task 4 bao gồm việc triển khai mã nguồn để thực hiện các hàm Hash bằng ngôn ngữ C++, sử dụng thư viện OpenSSL để hỗ trợ. Xây dựng mã nguồn kiểm tra Certificate và thử nghiệm các attack như collision và length extension attack trong hàm băm.

3. TASK 4

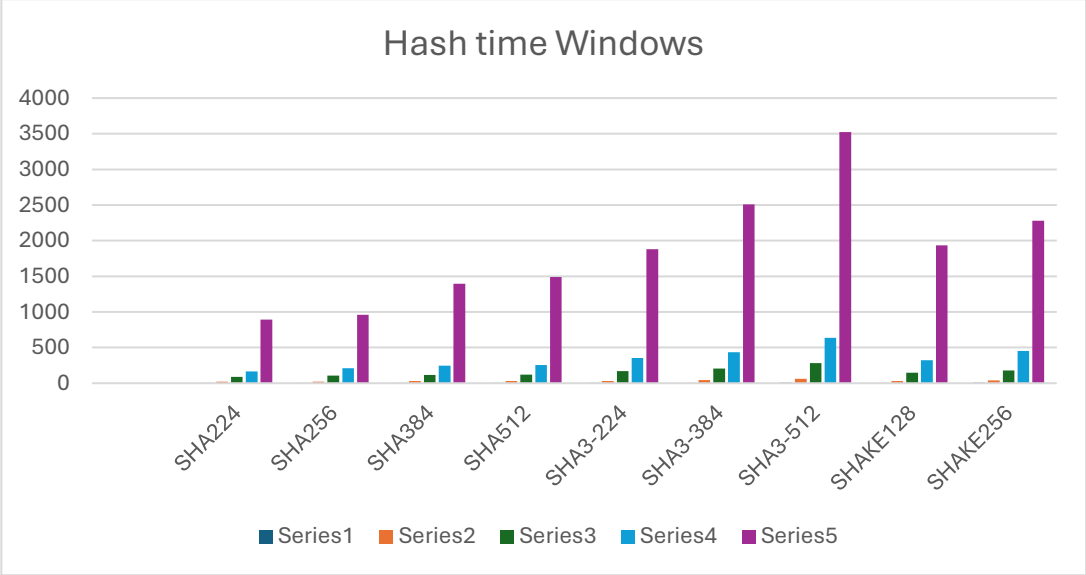
(Task 4.1)

a. Thống kê thời gian.

Em tiến hành băm các file input theo 5 size khác nhau (milliseconds). Thời gian có tính thêm thời gian đọc file.

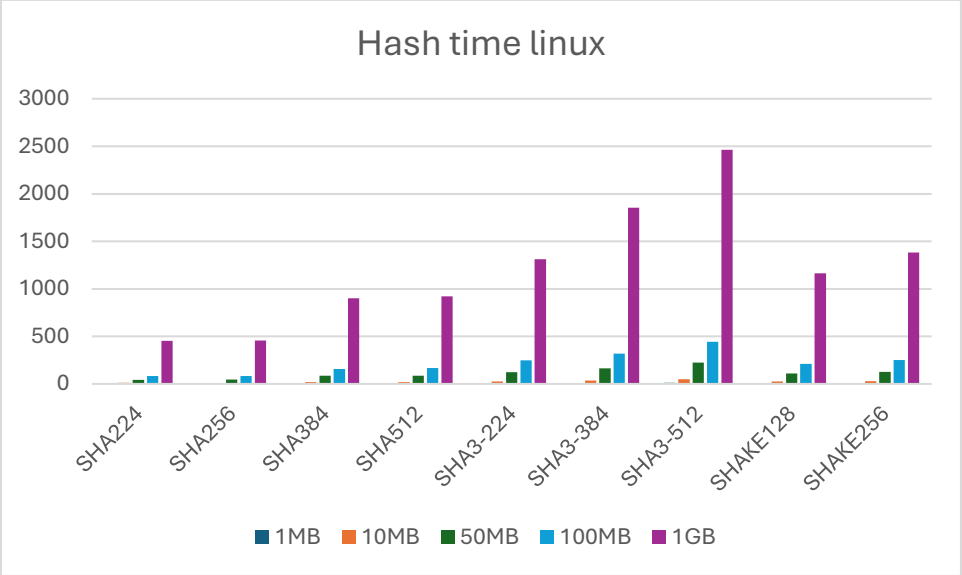
Windows:

	1MB	10MB	50MB	100MB	1GB
SHA224	3.007	21.194	86.84	165.434	891.609
SHA256	3.207	20.931	105.25	211.455	959.949
SHA384	3.544	31.051	117.314	247.328	1395.09
SHA512	4.439	29.646	122.479	256.915	1487.87
SHA3-224	4.442	32.334	167.64	353.107	1879.439
SHA3-384	5.242	42.282	207.741	432.582	2508.639
SHA3-512	6.846	62.096	282.975	634.975	3522.146
SHAKE128	5.556	31.326	147.612	322.608	1932.8
SHAKE256	6.179	40.541	178.948	451.37	2281.097



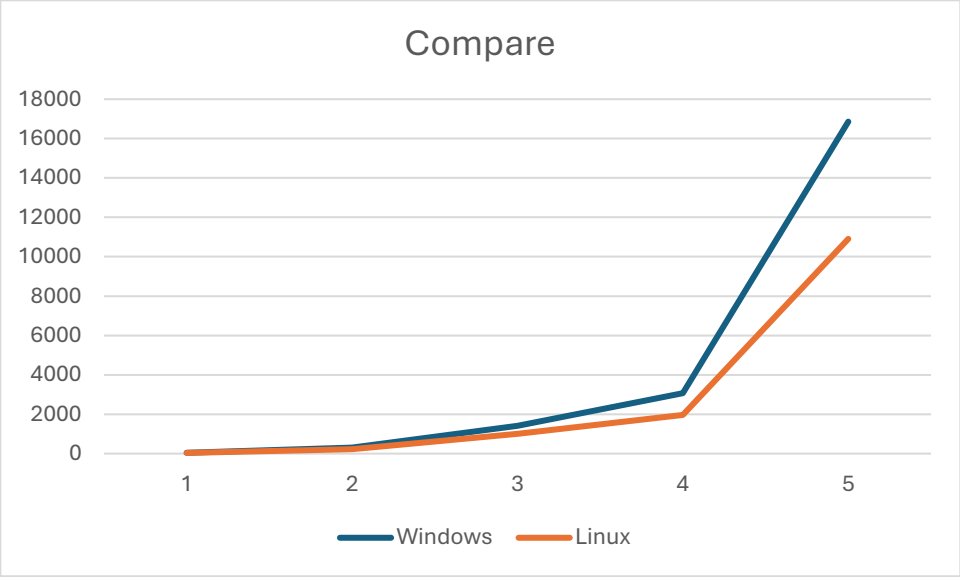
Linux:

	1MB	10MB	50MB	100MB	1GB
SHA224	2,226	10,332	42,798	84,329	454,649
SHA256	2,599	10,073	43,983	83,580	455,823
SHA384	2,875	20,032	84,683	157,016	902,073
SHA512	2,956	19,241	85,060	165,211	920,754
SHA3-224	3,616	27,028	121,525	246,416	1311.043
SHA3-384	4,689	35,422	163,637	317,567	1852.557
SHA3-512	10,890	47,387	224,053	443,192	2461.733
SHAKE128	3,301	23,812	108,528	209,110	1165.039
SHAKE256	3,939	28,037	127,103	252,201	1381.936



⇨ Tổng thời gian băm giữa linux và windows có sự chênh lệch rõ rệt
⇨ Linux chạy nhanh hơn windows nhiều lần

	1MB	10MB	50MB	100MB	1GB
Windows	42.462	311.401	1416.799	3075.744	16858.639
Linux	37.091	221.364	1001.37	1958.622	10905.607



TASK4.2

Khi nhập certificate vào chúng ta có thể xác định được certificate đó hợp lệ không. Certificate sẽ có dạng đuôi der, pem nhưng em đã gom chung lại để chúng ta có thể nhập cả 2. Ở đây có ví dụ về certificate của facebook. Khi nhập cert cả facebook và cert của tổ chức kí cho cert ấy, nếu đúng thì sẽ hiện ra thông tin chi tiết của cert.

```
E:\Term4\TASK5.2>verify_cert.exe
Usage: verify_cert.exe <certificate-file> <intermediate-certificate>
        You can choose both type DER and PEM
E:\Term4\TASK5.2>verify_cert.exe fb.crt inter_fb.crt
Validate certificate successfully!!!
Subject: /C=US/ST=California/L=Menlo Park/O=Meta Platforms, Inc./CN=*.facebook.com
Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 High Assurance Server CA
Subject Public Key Info:
        Public Key Algorithm: id-ecPublicKey
        Public-Key: (256 bit)
        04:E8:85:9F:24:DD:DE:D1:66:C2:DB:CA:2E:FF:25:
        24:87:DA:F7:D8:5C:F9:50:13:43:57:42:8D:F8:60:
        59:DF:B9:70:B8:E2:58:13:DA:1E:E9:55:3D:4A:40:
        4C:BC:F6:83:8B:CF:6C:A0:E6:48:37:4A:41:82:82:
        81:C7:CC:1B:D7
        ASN1 OID: prime256v1
NIST CURVE: prime256v1
Signature:
A86065B9DDBB003E1150734F9F459AE3605F456FC7FE8630238E805EF7C7CE3F0D0E72\
E111BDA439932C5C19BFE53EF6520B135D2B87C973C3BEF594AA2931D5497AFD945F32\
9F800C29358D6797F7FA30F288E1AA61A5292B56D52AD8A8AC00FADBBF62DE9BA4126C\
4C98FD2534CC8D13A63F20850E16D5728C978A5F2430C1CF161D369F60071E8224B124\
74CB590FBE204762377877808D664B99380C305D978FB49C40D99655C5125141627B1C\
9074234620D0A2861FAD6C758060736FB3AE2B4884578FC31C7C5953D00737009B6D14\
7AF66693A0230A0ACA8831334D19C2A298E6049AA1180DAD715A8ADC4D3BE35B9321BF\
D739BEE82A7456CD9EDB73
Signature algorithm: sha256WithRSAEncryption
Validity:
        Not before: Sep 26 00:00:00 2023 GMT
        Not after: Dec 25 23:59:59 2023 GMT
Purpose: SSL client SSL server Any Purpose OCSP helper
```

Còn nếu certificate không phù hợp thì không thể kiểm tra thông tin của certificate.

```
E:\Term4\TASK5.2>verify_cert.exe fb.crt rootfb.crt
Failed to validate certificate!!!
```

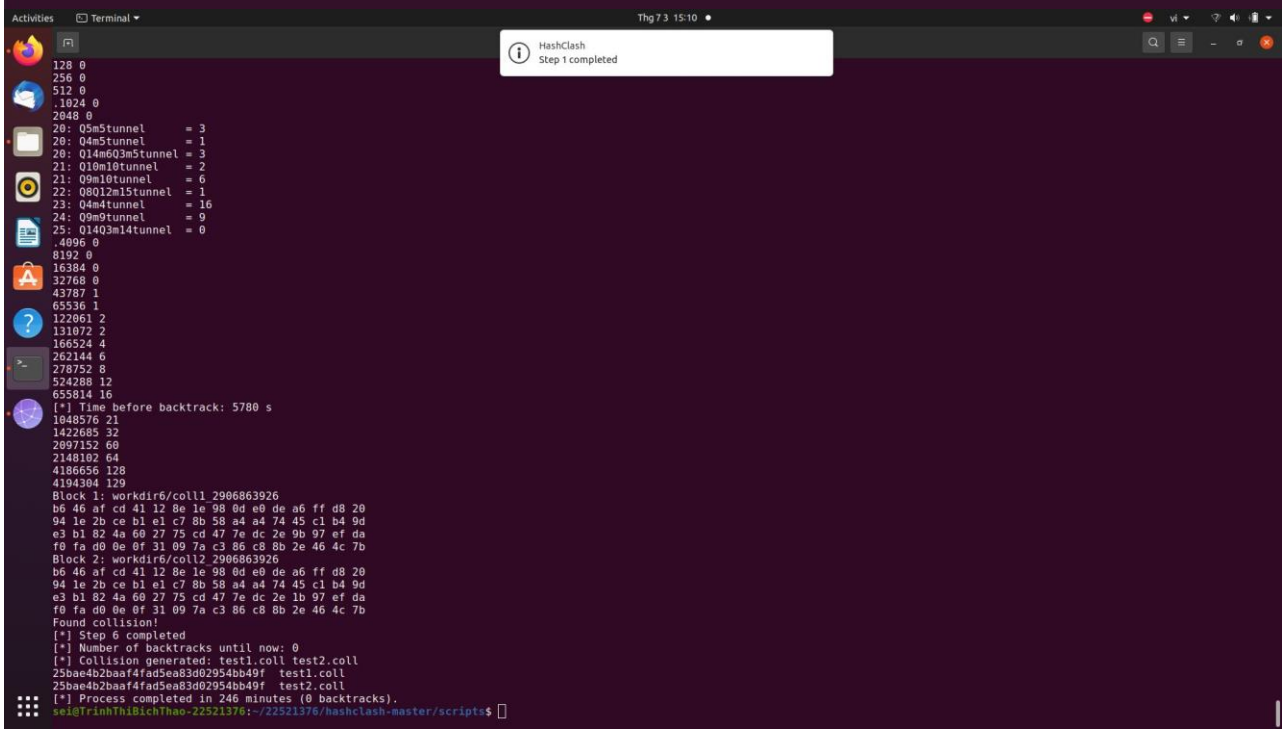
TASK4.3

Collision attack về 1 file tạo ra 2 file collision

```
sei@TrinhThiBichThao-22521376:~/22521376/Labsetup$ ./md5collgen -p  prefix.txt -o output1 output2
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'output1' and 'output2'
Using prefixfile: 'prefix.txt'
Using initial value: 4a69336d1e30f01f65e1c6bdec31cfb1

Generating first block: ................................................
Generating second block: S11.....................................
Running time: 26.7329 s
sei@TrinhThiBichThao-22521376:~/22521376/Labsetup$ diff output1 output2
Binary files output1 and output2 differ
sei@TrinhThiBichThao-22521376:~/22521376/Labsetup$ md5sum output1 output2
c1317ffddcfbf0aeef86a307410de0c5  output1
c1317ffddcfbf0aeef86a307410de0c5  output2
```

Collision attack về 2 file cpp đã compiler

```
sei@TrinhThiBichThao-22521376:~/22521376/HashPump-partialhash-master$ cat test.txt
k = 22521376

m = Trinh Thi Bich Thao

padding = ok fine

signature
md5:
s = 0da5bda836e1f2980bc46c6463a973af

sha1:
s = a2211bc15078d6e7f28d64932065445231510018

sha256:
s = 5b8188c400a058d256d356aa0ddb4642f64d5fa1ec826bbc78d203a725690a17

sha512
s = d898ad2d04fb31e356474cca0825960ffcd2778187f37186e01277d63c00850e243a19db373d34ec773345143913fc6fa102ea987d39ace9243ebbbbdff48195
```



```
sei@TrinhThiBichThao-22521376:~/22521376/hashclash-master/scripts$ ./test1
1sei@TrinhThiBichThao-22521376:~/22521376/hashclash-master/scripts$ ./test2
2sei@TrinhThiBichThao-22521376:~/22521376/hashclash-master/scripts$ ./test1.coll
sei@TrinhThiBichThao-22521376:~/22521376/hashclash-master/scripts$ ./test2.coll
sei@TrinhThiBichThao-22521376:~/22521376/hashclash-master/scripts$ md5sum test1 test2
425f4a9e6b4802714760089b4161e8b5  test1
1a87f05d9471a5f581b07bc41ea8192c  test2
sei@TrinhThiBichThao-22521376:~/22521376/hashclash-master/scripts$ md5sum test1.coll test2.coll
25bae4b2baaf4fad5ea83d02954bb49f  test1.coll
25bae4b2baaf4fad5ea83d02954bb49f  test2.coll
sei@TrinhThiBichThao-22521376:~/22521376/hashclash-master/scripts$ diff test1.coll test2.coll
Binary files test1.coll and test2.coll differ
```

TASK4.4

Length Extension Attack: Sử dụng private key và hàm Hmac (online) để tạo ra signature rồi sử dụng công cụ hashpump để thực hiện attack

```
sei@TrinhThiBichThao-22521376:~/22521376/HashPump-partialhash-master$ cat test.txt
k = 22521376

m = Trinh Thi Bich Thao

padding = ok fine

signature
md5:
s = 0da5bda836e1f2980bc46c6463a973af

sha1:
s = a2211bc15078d6e7f28d64932065445231510018

sha256:
s = 5b8188c400a058d256d356aa0ddb4642f64d5fa1ec826bbc78d203a725690a17

sha512
s = d898ad2d04fb31e356474cca0825960ffcd2778187f37186e01277d63c00850e243a19db373d34ec773345143913fc6fa102ea987d39ace9243ebbbbdff48195
```

```
sei@TrinhThiBichThao-22521376:~/22521376/HashPump-partialhash-master$ ./hashpump -s '0da5bda836e1f2980bc46c6463a973af' -d 'Trinh Thi Bich Thao' -a 'ok fine ' -k 8
mask: ffffffff
predicted sig: c88b61387a810f846f7252481a9f663e
Trinh Thi Bich Thao\x80\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xd8\x00\x00\x00\x00\x00\x00\x00ok fine
sei@TrinhThiBichThao-22521376:~/22521376/HashPump-partialhash-master$ ^C
sei@TrinhThiBichThao-22521376:~/22521376/HashPump-partialhash-master$ ./hashpump -s 'a2211bc15078d6e7f28d64932065445231510018' -d 'Trinh Thi Bich Thao' -a 'ok fine ' -k 8
mask: ffffffff
predicted sig: 2d32da97b3c8e426113716472a9aa19c43cafe83
Trinh Thi Bich Thao\x80\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xd8ok fine
sei@TrinhThiBichThao-22521376:~/22521376/HashPump-partialhash-master$
sei@TrinhThiBichThao-22521376:~/22521376/HashPump-partialhash-master$ ./hashpump -s '5b8188c400a058d256d356aa0ddb4642f64d5fa1ec826bbc78d203a725690a17' -d 'Trinh Thi Bich Thao' -a 'ok
fine ' -k 8
mask: ffffffff
predicted sig: 49c6cf77e218b10423019e0f3e726105d18941f00438d69d16a0838fad64d507
Trinh Thi Bich Thao\x80\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xd8ok fine
sei@TrinhThiBichThao-22521376:~/22521376/HashPump-partialhash-master$ ./hashpump -s 'd898ad2d04fb31e356474cca0825960ffcd2778187f37186e01277d63c00850e243a19db373d34ec773345143913fc6fa1
02ea987d39ace9243ebbbbdff48195' -d 'Trinh Thi Bich Thao' -a 'ok fine ' -k 8
mask: ffffffff
predicted sig: 70d5a78c8df27c1f3acfe763b11f28158d69086bd9114b50eadf0924ebefbece1f46debb47624158bfe777982a667f155c453f06721bf3153aca510c4e6c480e
Trinh Thi Bich Thao\x80\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xd8ok fine
sei@TrinhThiBichThao-22521376:~/22521376/HashPump-partialhash-master$ ./hashpump -s 'd898ad2d04fb31e356474cca0825960ffcd2778187f37186e01277d63c00850e243a19db373d34ec773345143913fc6fa1
02ea987d39ace9243ebbbbdff48195' -d 'Trinh Thi Bich Thao' -a 'ok fine ' -k 8
mask: ffffffff
predicted sig: 70d5a78c8df27c1f3acfe763b11f28158d69086bd9114b50eadf0924ebefbece1f46debb47624158bfe777982a667f155c453f06721bf3153aca510c4e6c480e
Trinh Thi Bich Thao\x80\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xd8ok fine
```