

UNIVERSITY OF INFORMATION TECHNOLOGY
FACULTY OF COMPUTER NETWORK AND COMMUNICATION



UIT
TRƯỜNG ĐẠI HỌC
CÔNG NGHỆ THÔNG TIN

REPORT

Subject: Cryptography

Report Lab 4

Lecturer: Nguyen Ngoc Tu

Report Lab 4

Student Information

Full Name: Trương Đức Hòa

Student ID Number: 22520407

Class: ATTT2022.1

Device Information

CPU: AMD Ryzen7-5800H @ 3.2 GHz

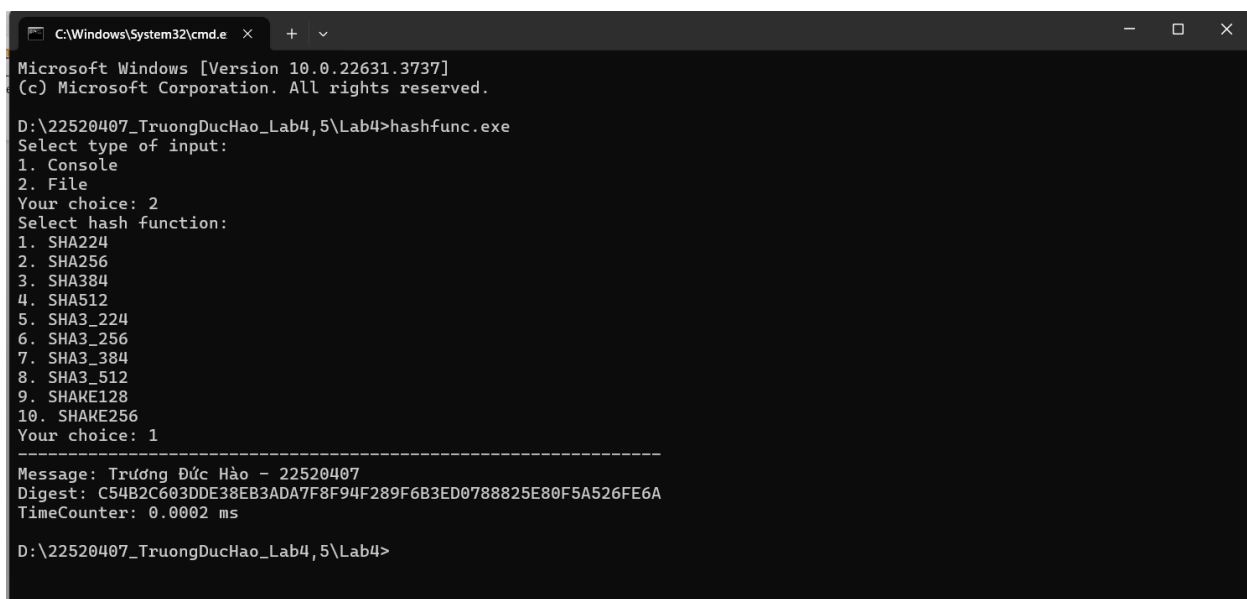
Ram: 8 GB DDR4

SSD: 500GB

Display chip name: AMD Radeon Graphics – RTX 3050 NVIDIA

LAB4: PKI & HASH FUNCTIONS

4.1 Hash functions:



```
C:\Windows\System32\cmd.e x + v
Microsoft Windows [Version 10.0.22631.3737]
(c) Microsoft Corporation. All rights reserved.

D:\22520407_TruongDucHao_Lab4,5\Lab4>hashfunc.exe
Select type of input:
1. Console
2. File
Your choice: 2
Select hash function:
1. SHA224
2. SHA256
3. SHA384
4. SHA512
5. SHA3_224
6. SHA3_256
7. SHA3_384
8. SHA3_512
9. SHAKE128
10. SHAKE256
Your choice: 1
-----
Message: Trương Đức Hòa - 22520407
Digest: C54B2C603DDE38EB3ADA7F8F94F289F6B3ED0788825E80F5A526FE6A
TimeCounter: 0.0002 ms

D:\22520407_TruongDucHao_Lab4,5\Lab4>
```

Window

Hash function	1KB	100KB	1MB	10MB	100MB
SHA224	0.0002	0.0512	0.5302	5.3828	51.4601
SHA256	0.0001	0.0513	0.53	5.3244	51.3711
SHA384	0.0005	0.2038	2.1484	22.2451	212.402
SHA512	0.0004	0.203	2.1594	22.1494	209.913
SHA3-224	0.0004	0.2061	2.2594	22.4874	211.325
SHA3-256	0.0004	0.2182	2.3824	23.5598	212.235
SHA3-384	0.0004	0.2938	3.1129	31.0414	301.322
SHA3-512	0.0005	0.4224	4.6603	44.753	415.326
SHAKE128 (Digest size: 64 bytes)	0.0004	0.1815	1.9834	19.4342	189.632
SHAKE256 (Digest size: 64 bytes)	0.0004	0.2281	2.6836	23.6849	222.652

Linux

Hash function	1KB	100KB	1MB	10MB	100MB
SHA224	0.0011023	0.0437	0.5103	5.3236	50.3204
SHA256	0.0010611	0.0548	0.5	5.3012	51.2387
SHA384	0.0011874	0.2009	2.1156	22.1265	212.321
SHA512	0.0012427	0.2	2.1236	22.0235	209.796
SHA3-224	0.0014128	0.2103	2.2256	22.532	211.125
SHA3-256	0.0014235	0.2098	2.4865	23.3625	212.04
SHA3-384	0.0015383	0.2876	3.0036	31.0298	301.213
SHA3-512	0.0018721	0.4115	4.5324	44.520	415.205
SHAKE128 (Digest size: 64 bytes)	0.0014478	0.1812	1.9256	19.4261	189.476
SHAKE256 (Digest size: 64 bytes)	0.0013604	0.2126	2.5149	23.53	222.364

So sánh và nhận xét:

- Kích thước đầu vào càng lớn sẽ càng mất thời gian thực thi (điều này khá hiển nhiên).
- Thời gian thực thi trên Linux nhanh hơn Windows, điều này có lẽ đến từ quản lý tài nguyên và cài đặt hệ thống giữa hai hệ điều hành này.

4.2: PKI & Digital certificate:

Tạo cert:

```
D:\22520407_TruongDucHao_Lab4,5\Lab4>openssl x509 -in cert.pem -pubkey -noout
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAr4qCfZwhNqNdHMFVNxWU
BtmdbhIbL4QsQssrxqq6sqkwwsKlaEFLDz5VizDmWE6SQf+TwmQN8o1RK3REXYWnw
qy5lh+PPLeIuQTsHL6t+goSLHznzmXPrRKBYHE3ZNxwN1n116hM8KeVdmu37oea0
jv228958BZ6FE1uHzDuTimn8xw+vB0c6FDQLBUyduYe5oHgw8dZwDN00hm7FNJF6/
01Ts+Y3AqFxSy0d7pN+HPQrVU3zKljn960yemSirsTYQjohPn0iIx36AiYXubk6
PI+tOMT2jAYx/OEVHoiEf4dT4TCW09d9FWzleM89A1WkT3QqLxSeVe9c3IYdQ6ai
VwIDAQAB
-----END PUBLIC KEY-----

D:\22520407_TruongDucHao_Lab4,5\Lab4>openssl x509 -in cert.pem -pubkey -noout > publickey.pem
```

```

Verified certificate
The information of the certificate is as follows:

Version: 2

Serial Number: 1270998701932642547726494228958552298332406447124.

Not Before: 240706073124Z

Not After: 250706073124Z

Subject Identities:
DN: C=VN; ST=HCM; L=HCM; O=UIT; OU=HCMUIT; CN=TruongDucHao; EMAIL=22520407@gm.uit.edu.vn
CN: TruongDucHao
EMAIL: 22520407@gm.uit.edu.vn
SPKI: 6C79D62F52C3A775A74CBB1DCAFAF4331EEAC51E

Issuer Identities: C=VN; ST=HCM; L=HCM; O=UIT; OU=HCMUIT; CN=TruongDucHao; EMAIL=22520407@gm.uit.edu.vn

Subject Key Identities: hash: 6C79D62F52C3A775A74CBB1DCAFAF4331EEAC51E

Authority Key Identities: hash: 6C79D62F52C3A775A74CBB1DCAFAF4331EEAC51E

Sign Algorithm: 1.2.840.113549.1.1.11

Subject Public Key Algorithm: 1.2.840.113549.1.1.11

Signature: 509FF7567FFE6EF419118590391A7FBC15CEBD78DE0DCA0DE333F6185AB93AACBCBDCB589ED0DE2BA0A277E6E2E667D0030FC559E33E5F
49201D12CF9B5114756C8FBDDEF8AB9D1D67F9477D8BC5DB2D3473BB16E33C348F487C54138BF81246A53908832AD60689822082B877FE383AC2D901F
D8F755B26196EBF6ED140A92B95EE2551D324B4CCE03D684DA1495A87419A94FABA53737DC8607B114EF46132CE4C4D4DB074D23CFC0B7451EEB9578
74115999AF5DD7A792019AFAEECF46D1312E23B18F3B93C4A64333124C51B706B5790A6E6DECEE22BEE5B8D3876E4D68DF052C1C237CC274393035
379B2B4C23C616570F60AEAFAD2FB9373A32BF273C92

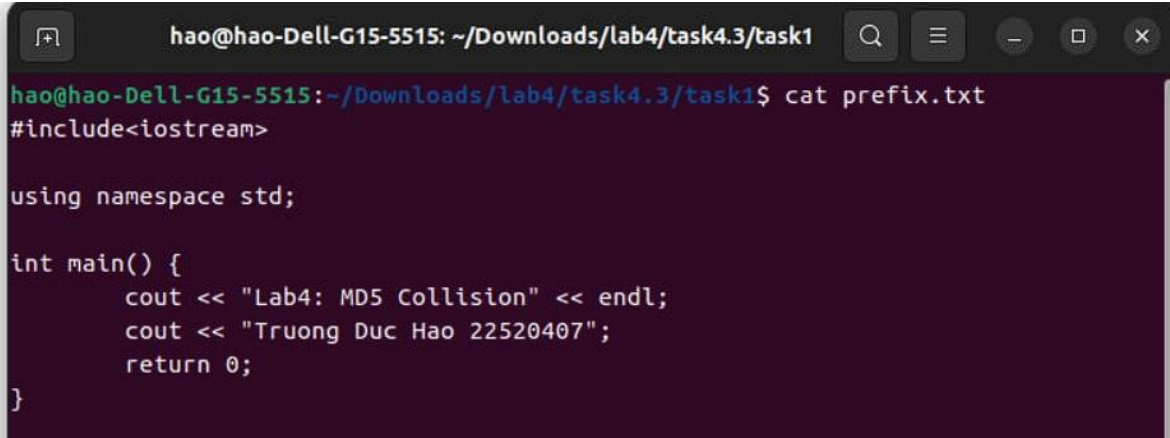
To Be Signed: 308202D7A003020102021416435AF4818DD50B3FF2DD095C30C7F8CD1A7C14300D06092A864886F70D01010B0500308186310B3009
06035504061302564E310C300A06035504080C0348434D310C300A06035504070C0348434D310C300A060355040A0C03554954310F300D060355040B

```

4.3 Collision and length extension attacks on Hash functions:

- Two collision messages have the same prefix string:

Prefix:

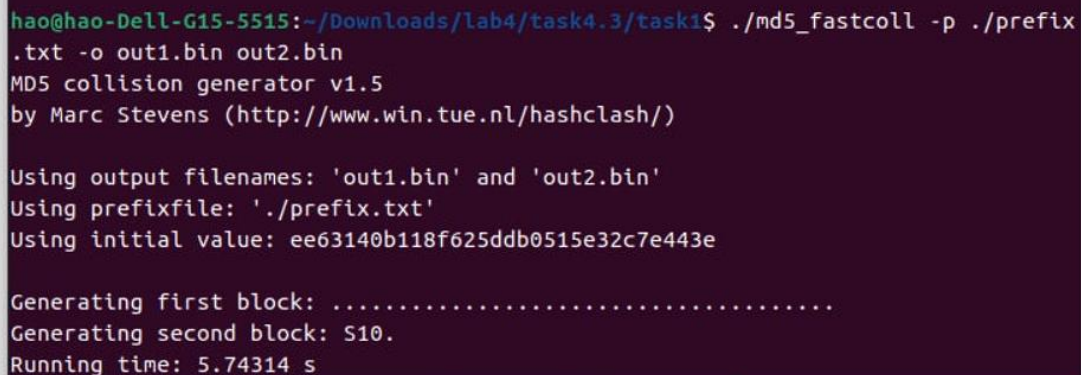


```
hao@hao-Dell-G15-5515: ~/Downloads/lab4/task4.3/task1
hao@hao-Dell-G15-5515:~/Downloads/lab4/task4.3/task1$ cat prefix.txt
#include<iostream>

using namespace std;

int main() {
    cout << "Lab4: MD5 Collision" << endl;
    cout << "Truong Duc Hao 22520407";
    return 0;
}
```

Run `md5_fastcoll` để tạo hai file khác nhau có chung prefix và MD5 Hash digest.

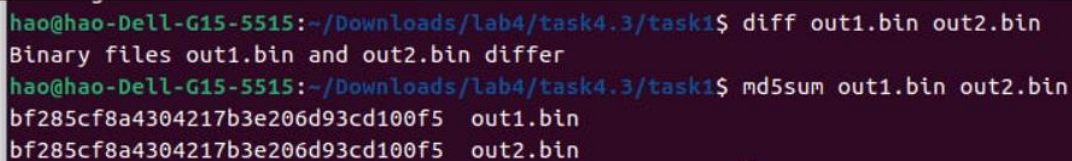


```
hao@hao-Dell-G15-5515:~/Downloads/lab4/task4.3/task1$ ./md5_fastcoll -p ./prefix
.txt -o out1.bin out2.bin
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'out1.bin' and 'out2.bin'
Using prefixfile: './prefix.txt'
Using initial value: ee63140b118f625ddb0515e32c7e443e

Generating first block: .....
Generating second block: S10.
Running time: 5.74314 s
```

So sánh hai outfile:



```
hao@hao-Dell-G15-5515:~/Downloads/lab4/task4.3/task1$ diff out1.bin out2.bin
Binary files out1.bin and out2.bin differ
hao@hao-Dell-G15-5515:~/Downloads/lab4/task4.3/task1$ md5sum out1.bin out2.bin
bf285cf8a4304217b3e206d93cd100f5  out1.bin
bf285cf8a4304217b3e206d93cd100f5  out2.bin
```

Sử dụng md5 và so sánh hash.

Trên đây là collision.

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

Build file .o từ file code:

```

C task2.c x
C task2.c
1  #include <stdio.h>
2
3  int main()
4  {
5      int i = 0;
6      for (i = 0; i < 200; i++)
7      {
8          printf("%x", i);
9      }
10     printf("\n");
11     printf("Lab4: MD5 Collision\n");
12     printf("Truong Duc Hao 22520407");
13 }

```

MD5(prefix || variant1 || suffix) = MD5(prefix || variant2 || suffix). Prefix được chọn là bội 64, offset là 4224. Suffix được giữ bằng 10FF.

```

hao@hao-Dell-G15-5515:~/Downloads/lab4/task4.3/task2$ head -c 4224 task2.o > prefix
hao@hao-Dell-G15-5515:~/Downloads/lab4/task4.3/task2$ tail -c 4352 task2.o > suffix

```

Sử dụng MD5_fastcoll để chuyển đổi hash từ file1 file2

```

hao@hao-Dell-G15-5515:~/Downloads/lab4/task4.3/task2$ ./md5_fastcoll -p prefix -o file1 file2
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'file1' and 'file2'
Using prefixfile: 'prefix'
Using initial value: cceaba80b3aabb3211a657316671eead

Generating first block: .....
Generating second block: S10.....
Running time: 3.218 s
hao@hao-Dell-G15-5515:~/Downloads/lab4/task4.3/task2$

```

Tạo 2 binaries transfer (code1, code2)

```
hao@hao-Dell-G15-5515:~/Downloads/lab4/task4.3/task2$ cat file1 suffix > code1
hao@hao-Dell-G15-5515:~/Downloads/lab4/task4.3/task2$ cat file2 suffix > code2
```

Check binary và sử dụng md5 để so sánh hash.

```
hao@hao-Dell-G15-5515:~/Downloads/lab4/task4.3/task2$ diff code1 code2
Binary files code1 and code2 differ
hao@hao-Dell-G15-5515:~/Downloads/lab4/task4.3/task2$ md5sum code1 code2
069d3425a3a834ded4f104ba89f18a20  code1
069d3425a3a834ded4f104ba89f18a20  code2
```

Trên đây là collision.

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

[illegible]

