

LAB 5, 6

Nguyễn Bùi Kim Ngân - 20520648

Task 5.1

Hardware

CPU: Intel(R) Core(TM) i7-8550U CPU @ 1.80GHz

RAM: 16GB

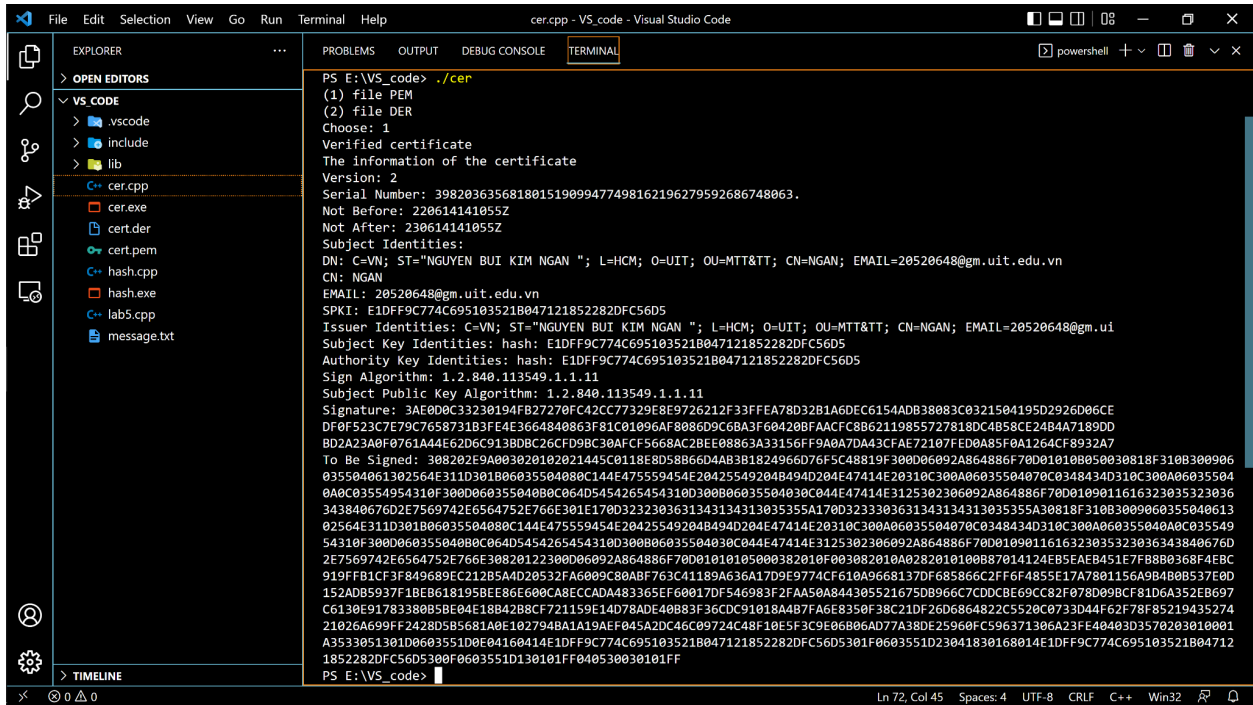
Ổ cứng: SSD 512GB

File input: 44 bytes

Hash functions	Window	Linux
SHA224	0.0002ms	0.00310903ms
SHA256	0.0008ms	0.00125109ms
SHA384	0.0013ms	0.00120856ms
SHA512	0.0005ms	0.00186676ms
SHA3-224	0.0005ms	0.0020182ms
SHA3-256	0.0008ms	0.00161945ms
SHA3-384	0.0006ms	0.00213349ms
SHA3-512	0.0007ms	0.00208186ms
SHAKE128 (512 bytes)	0.0037ms	0.00400049ms
SHAKE256 (512 bytes)	0.0035ms	0.00435937ms

Task 5.2

- Kết quả chạy:

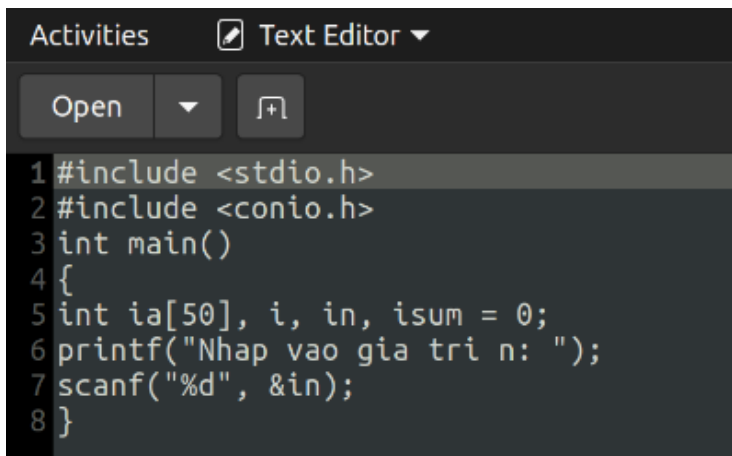


```
PS E:\VS_code> ./cer
(1) file PEM
(2) file DER
Choose: 1
Verified certificate
The information of the certificate
Version: 2
Serial Number: 398203635681801519099477498162196279592686748063.
Not Before: 220614141055Z
Not After: 230614141055Z
Subject Identities:
DN: C=VN; ST="NGUYEN BUI KIM NGAN "; L=HCM; O=UIT; OU=MTT&TT; CN=NGAN; EMAIL=20520648@gm.uit.edu.vn
CN: NGAN
EMAIL: 20520648@gm.uit.edu.vn
SPKI: E1DFF9C774C695103521B047121852282DFC56D5
Issuer Identities: C=VN; ST="NGUYEN BUI KIM NGAN "; L=HCM; O=UIT; OU=MTT&TT; CN=NGAN; EMAIL=20520648@gm.uit.edu.vn
Subject Key Identities: hash: E1DFF9C774C695103521B047121852282DFC56D5
Authority Key Identities: hash: E1DFF9C774C695103521B047121852282DFC56D5
Sign Algorithm: 1.2.840.113549.1.1.11
Subject Public Key Algorithm: 1.2.840.113549.1.1.11
Signature: 3AE0D0C33230194FB27270FC42CC77329E8E9726212F33FEEA78D32B1A6DEC6154ADB38083C0321504195D2926D06CE
DF0F523C7E79C7658731B3FE4E3664840863F81C01096AF8086D9C6BA3F60420BFAACFC8B62119855727818DC4B58CE24B4A7189D0
BD2A23A0F0761A44E62D6C913B0BC26CFD9BC30AFC5668AC2BEE08863A33156FF9A8A7DA43CFAE72107FED0A8F50A1264CF8932A7
To Be Signed: 308202E9A003020102021445C0118E8D58866D4A8381824966D76F5C48819F300D06092A864886F70D010108050030818F310B300906
035504061302564E311D301B06035504080C144E475559454E204255492048494D204E47414E20310C300A06035504070C0348434D310C300A06035504
0A0C03554954310F300D06035504080C064D5454265454310D300B06035504030C044E47414E3125302306092A864886F70D0109011616323035323036
343840676D2E7569742E6564752E766E301E170D2232303631343134313035355A170D2232303631343134313035355A30818F310B3009060355040613
02564E311D301B06035504080C144E475559454E204255492048494D204E47414E20310C300A06035504070C0348434D310C300A060355040A0C035549
54310F300D06035504080C064D5454265454310D300B06035504030C044E47414E3125302306092A864886F70D0109011616323035323036343840676D
2E7569742E6564752E766E30820122300D06092A864886F70D0101010500302010F003082010A02020101008B7014124E85EAEB451E7F880368F4EBC
919FFB1CF3F849689EC212B5A4D20532FA6009C80ABF763C41189A636A17D9E9774CF610A9668137DF685866C2FF6F4855E17A7801156A98480B537E0D
152AD85937F1BE86181958EE86E608CABECCADA483365EF60017DF546983F2FAA50A8443055216750B966C7CDDCBE69CC82F078D098CF81D6A352EB697
C6130E91783380B58E04E1884288CF721159E14D78ADE40B83F36DC91018A4B7FA6E8350F38C21DF2606864822C5520C073D044F62F78F85219435274
21026A699FF2428D5B5681A0E1027948A1A19AEF045A2DC46C09724C48F10E5F3C9E06B06AD77A38DE25960FC596371306423FE48403D3570203010001
A3533051301D0603551D0E04160414E1DFF9C774C695103521B047121852282DFC56D5301F0603551D23041830168014E1DFF9C774C695103521B04712
1852282DFC56D5300F0603551D130101FF040530030101FF
```

Task 6.1

+

code c:



```
#include <stdio.h>
#include <conio.h>
int main()
{
    int ia[50], i, in, isum = 0;
    printf("Nhap vao gia tri n: ");
    scanf("%d", &in);
}
```

so sánh input

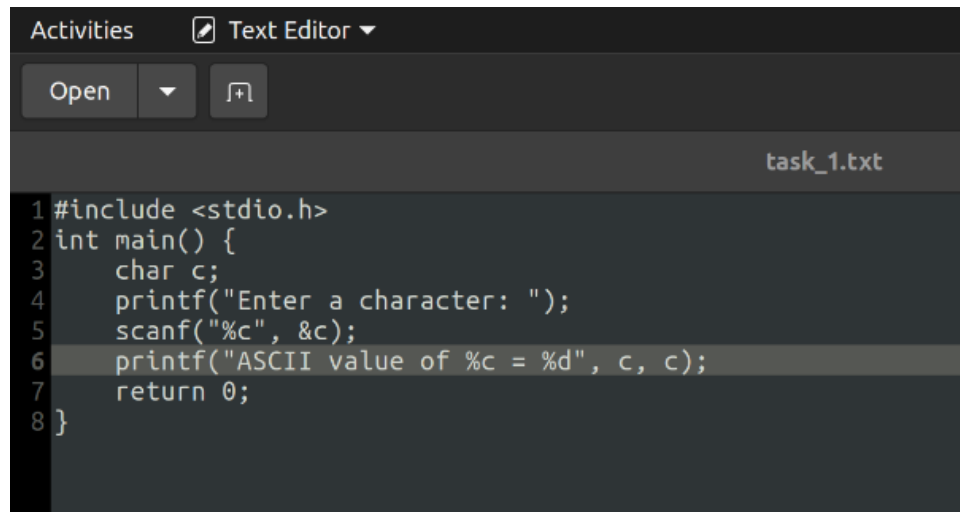


same MD5 digest

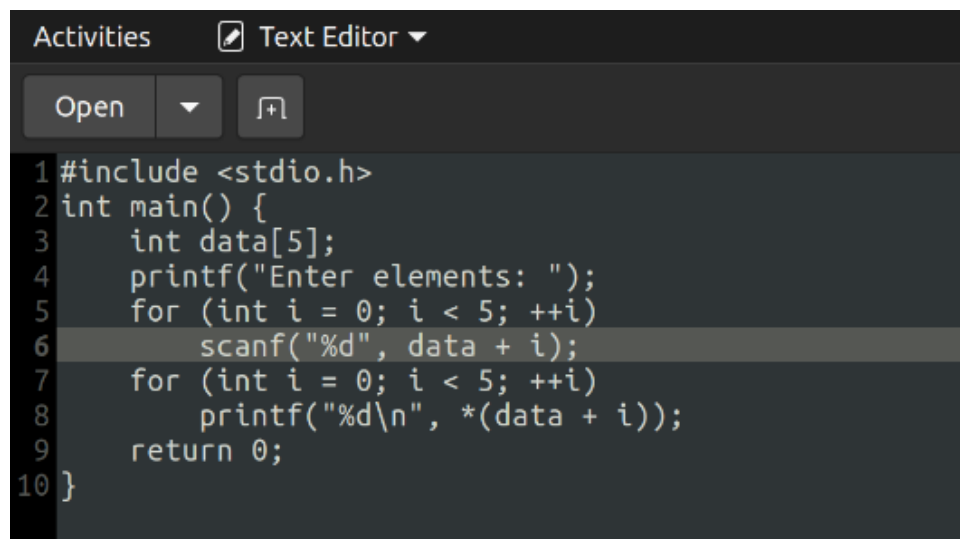
```
ngan@ngan-XPS-13-9370:~/Documents/hashclash-master/lab-6$ md5sum collision1.bin
305437cffe093790f60e70ac6b3fb770 collision1.bin
ngan@ngan-XPS-13-9370:~/Documents/hashclash-master/lab-6$ md5sum collision2.bin
305437cffe093790f60e70ac6b3fb770 collision2.bin
ngan@ngan-XPS-13-9370:~/Documents/hashclash-master/lab-6$
```

+

code c:



```
Activities Text Editor
Open task_1.txt
1 #include <stdio.h>
2 int main() {
3     char c;
4     printf("Enter a character: ");
5     scanf("%c", &c);
6     printf("ASCII value of %c = %d", c, c);
7     return 0;
8 }
```



```
Activities Text Editor
Open
1 #include <stdio.h>
2 int main() {
3     int data[5];
4     printf("Enter elements: ");
5     for (int i = 0; i < 5; ++i)
6         scanf("%d", data + i);
7     for (int i = 0; i < 5; ++i)
8         printf("%d\n", *(data + i));
9     return 0;
10 }
```

kết quả chạy:

```
Activities Terminal Thg 6 5 15:02
ngan@ngan-XPS-13-9370: ~/Documents/hashclash-master/lab-6/task2

25: Q14Q3n14tunnel = 1
.1 0
2 0
4 0
8 0
16 0
32 0
64 0
128 0
256 0
512 0
1024 0
2048 0
4096 0
8192 0
16384 0
32768 0
37892 1
65536 1
[*] Time before backtrack: 5710 s
131072 1
135080 2
262144 2
Block 1: workdir6/coll1_1410490260
90 10 48 2a b2 7e d2 d5 07 fe 29 5e 68 90 bb c6
7b e3 f4 ad b1 46 05 bd 39 20 4c 83 f1 b8 a7 8a
f2 7d 85 39 06 44 00 e2 f9 3b 5e 70 3b 03 9f 40
24 92 22 8a ec a0 cd 6a d4 2b e4 a5 af 9a 0d 73
Block 2: workdir6/coll2_1410490260
90 10 48 2a b2 7e d2 d5 07 fe 29 5e 68 90 bb c6
7b e3 f4 ad b1 46 05 bd 39 20 4c 83 f1 b8 a7 8a
f2 7d 85 39 06 44 00 e2 f9 3b 5e 70 3b 03 9f 3c
24 92 22 8a ec a0 cd 6a d4 2b e4 a5 af 9a 0d 73
Found collision!
[*] Step 6 completed
[*] Number of backtracks until now: 0
[*] Collision generated: task2a.txt.coll task2b.txt.coll
a85e4924730f1c32d8d9b62c7c4435f6 task2a.txt.coll
a85e4924730f1c32d8d9b62c7c4435f6 task2b.txt.coll
[*] Process completed in 298 minutes (0 backtracks).
ngan@ngan-XPS-13-9370:~/Documents/hashclash-master/lab-6/task2$
ngan@ngan-XPS-13-9370:~/Documents/hashclash-master/lab-6/task2$
```

so sánh input

Activities Firefox Web Browser Thg 6 5 15:06

Computed Diff - Diff Ch... +

https://www.diffchecker.com/diff

Diffchecker Text Images PDF Excel Folders Features Desktop Pricing Sign in Create an account Download Diffchecker Desktop

Saved Diffs You haven't saved any diffs yet.

Diff history

- now

Clear

Diff history is cleared on refresh

Real-time Regular Collapsed Expanded Split Unified Word Character Tools

4 lines -1 Removal Copy all

```
1 90 10 48 2a b2 7e d2 d5 07 fe 29 5e 68 90 bb c6
2 7b e3 f4 ad b1 46 05 bd 39 20 4c 83 f1 b8 a7 8a
3 f2 7d 85 39 06 44 00 e2 f9 3b 5e 70 3b 03 9f 40
4 24 92 22 8a ec a0 cd 6a d4 2b e4 a5 af 9a 0d 73
```

4 lines +1 Addition Copy all

```
1 90 10 48 2a b2 7e d2 d5 07 fe 29 5e 68 90 bb c6
2 7b e3 f4 ad b1 46 05 bd 39 20 4c 83 f1 b8 a7 8a
3 f2 7d 85 39 06 44 00 e2 f9 3b 5e 70 3b 03 9f 3c
4 24 92 22 8a ec a0 cd 6a d4 2b e4 a5 af 9a 0d 73
```

Editor Compare & merge Clear Export as PDF Save Diff Share

Original Text Changed Text

```
1 90 10 48 2a b2 7e d2 d5 07 fe 29 5e 68 90 bb c6
2 7b e3 f4 ad b1 46 05 bd 39 20 4c 83 f1 b8 a7 8a
3 f2 7d 85 39 06 44 00 e2 f9 3b 5e 70 3b 03 9f 40
4 24 92 22 8a ec a0 cd 6a d4 2b e4 a5 af 9a 0d 73
```

```
1 90 10 48 2a b2 7e d2 d5 07 fe 29 5e 68 90 bb c6
2 7b e3 f4 ad b1 46 05 bd 39 20 4c 83 f1 b8 a7 8a
3 f2 7d 85 39 06 44 00 e2 f9 3b 5e 70 3b 03 9f 3c
4 24 92 22 8a ec a0 cd 6a d4 2b e4 a5 af 9a 0d 73
```

same md5 digest

```
Activities Terminal Thg 6 14 22:03
ngan@ngan-XPS-13-9370: ~/Documents/hashclash-master/lab-6/task2$ md5sum task2a.txt.coll
a85e4924730f1c32d8d9b62c7c4435f6 task2a.txt.coll
ngan@ngan-XPS-13-9370:~/Documents/hashclash-master/lab-6/task2$ md5sum task2b.txt.coll
a85e4924730f1c32d8d9b62c7c4435f6 task2b.txt.coll
ngan@ngan-XPS-13-9370:~/Documents/hashclash-master/lab-6/task2$
```

Task 6.2

SHA1

```
Activities Text Editor Thg 6 14 22:03
*Untitled Document 1
1 secret key
2 k =cncwncowc2039fnc
3
4 m =nguyen bui kim ngan 20520648 attn
5
6 signature
7 h(cncwncowc2039fncnguyen bui kim ngan 20520648 attn)
8 h = sha1
9 s =01786a2458440f0b9c91f732ecbb5744b5c08aa2
10
11 padding = thuc hanh lab 6
12
13 ./hashpump -s '01786a2458440f0b9c91f732ecbb5744b5c08aa2' -d 'nguyen bui kim ngan 20520648 attn' -a 'thuc hanh lab 6' -k 16

Activities Terminal Thg 6 14 22:04
ngan@ngan-XPS-13-9370:~/Documents/HashPump-master/hashpump_h$ ./hashpump -s '01786a2458440f0b9c91f732ecbb5744b5c08aa2' -d 'nguyen bui kim ngan 20520648 attn' -a 'thuc hanh lab 6' -k 16
87081fb0c58e7d79b6cb4b2004599e316c8a8f12
nguyen bui kim ngan 20520648 attn\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x01\x88thuc hanh lab 6
ngan@ngan-XPS-13-9370:~/Documents/HashPump-master/hashpump_h$
```

SHA256

```
Activities Text Editor Thg 6 14 22:09
*Untitled Document 1
1 secret key
2 k =cncwncowc2039fnc
3
4 m =nguyen bui kim ngan 20520648 attn
5
6 signature
7 h(cncwncowc2039fncnguyen bui kim ngan 20520648 attn)
8 h = sha256
9 s =31757ba09e6b4da943de0a2f063bd9e9f5edd6af822cbf83e682b5524f0e4084
10
11 padding = thuc hanh lab 6
12
13 ./hashpump -s '31757ba09e6b4da943de0a2f063bd9e9f5edd6af822cbf83e682b5524f0e4084' -d 'nguyen bui kim ngan 20520648 attn' -a 'thuc hanh lab 6' -k 16
426527b33c4514eac79bdca167d1dbfb28175c76e93050b28c09ca2fc7732eb0
nguyen bui kim ngan 20520648 attn\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x01\x88thuc hanh lab 6
ngan@ngan-XPS-13-9370:~/Documents/HashPump-master/hashpump_h$
```

SHA512

