

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN HCM



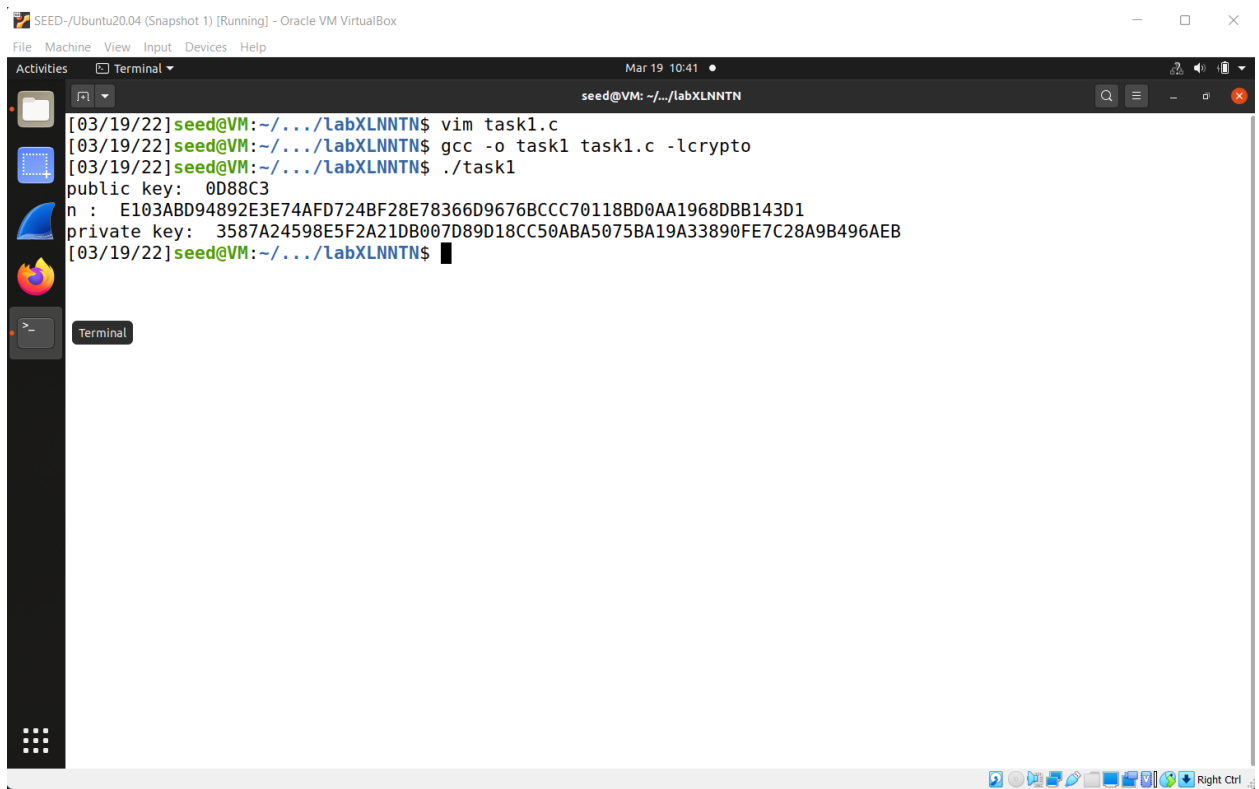
MÔN HỌC: MÃ HÓA ỨNG DỤNG – 19CNTT

REPORT

Nguyễn Quang Thuận – 19127571

Nguyễn Quang Huy – 19127161

1. Task1



The screenshot shows a terminal window titled "SEED-/Ubuntu20.04 (Snapshot 1) [Running] - Oracle VM VirtualBox". The terminal output is as follows:

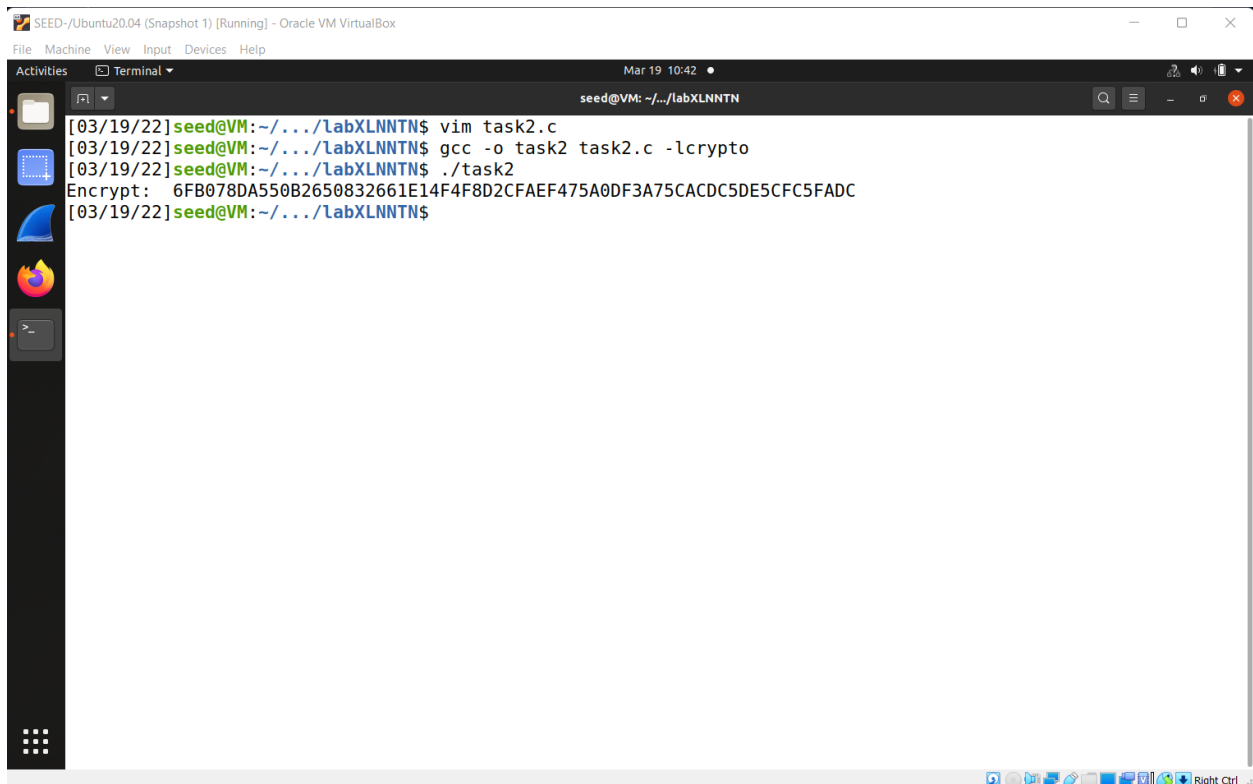
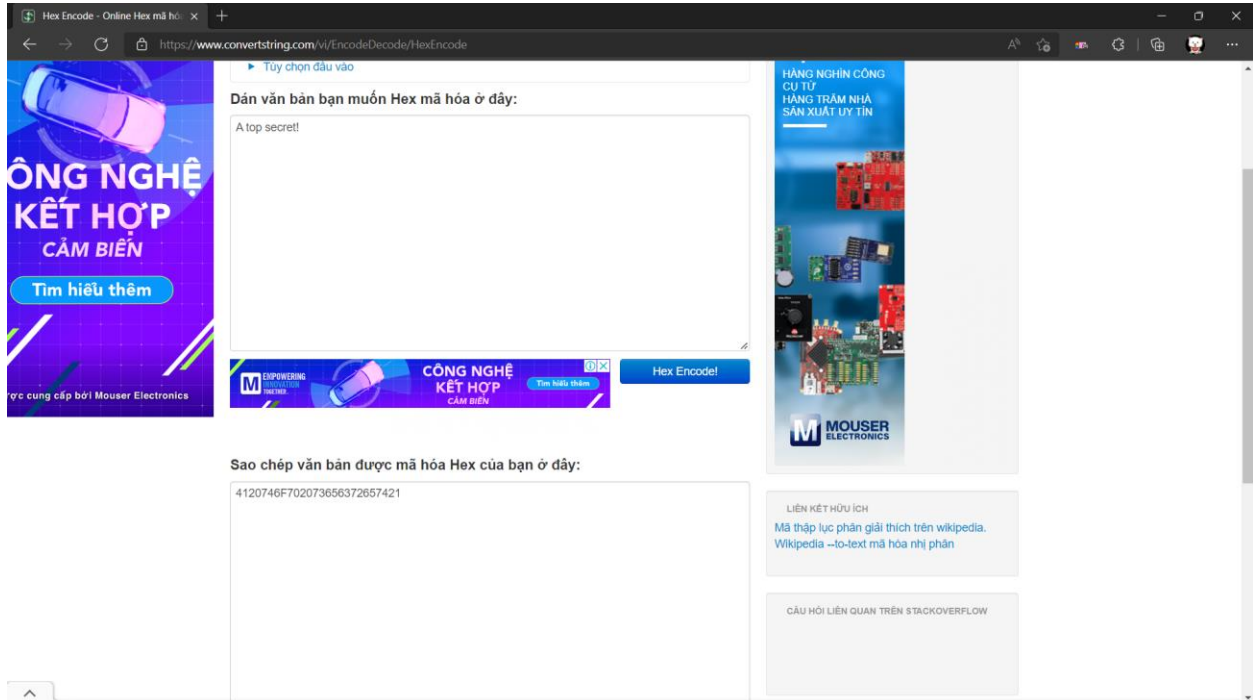
```
[03/19/22]seed@VM:~/.../labXLNNTN$ vim task1.c
[03/19/22]seed@VM:~/.../labXLNNTN$ gcc -o task1 task1.c -lcrypto
[03/19/22]seed@VM:~/.../labXLNNTN$ ./task1
public key:  0D88C3
n :  E103ABD94892E3E74AFD724BF28E78366D9676BCCC70118BD0AA1968DBB143D1
private key: 3587A24598E5F2A21DB007D89D18CC50ABA5075BA19A33890FE7C28A9B496AEB
[03/19/22]seed@VM:~/.../labXLNNTN$
```

The terminal window includes a sidebar with application icons (Files, Terminal, Firefox, etc.) and a top menu bar with options like File, Machine, View, Input, Devices, and Help. The bottom status bar shows system icons and the text "Right Ctrl".

2. Task2

Vì không thể dùng được câu lệnh: `python -c 'print("A top secret!".encode("hex"))'`
Nên em sẽ dùng cách thay thế cho câu lệnh (cho các task) là trang web:

[Hex Encode - Online Hex mã hóa \(convertstring.com\)](https://www.convertstring.com/HexEncode)



3. Task3

```
SEED-/Ubuntu20.04 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mar 19 11:22
seed@VM: ~/.../labXLNNTN
[03/19/22]seed@VM:~/.../labXLNNTN$ vim task3.c
[03/19/22]seed@VM:~/.../labXLNNTN$ gcc -o task3 task3.c -lcrypto
[03/19/22]seed@VM:~/.../labXLNNTN$ ./task3
Decrypt: 50617373776F72642069732064656573
[03/19/22]seed@VM:~/.../labXLNNTN$
```




Hex to Text - Online Hex Decoder

<https://www.convertstring.com/vi/EncodeDecode/HexDecode>

Tùy chọn đầu vào

Dán văn bản bạn muốn hex giải mã ở đây:

50617373776F72642069732064656573

Hex Decode!

Hex vào văn bản [Download file](#)

Sao chép văn bản giải mã hex của bạn ở đây:

Password is dees

LIÊN KẾT HỮU ÍCH

Mã thập lục phân giải thích trên wikipedia.
[Wikipedia -to-text mã hóa nhị phân](#)

CÂU HỎI LIÊN QUAN TRÊN STACKOVERFLOW

4. Task4

The image shows a web browser window with the URL <https://www.convertstring.com/vi/EncodeDecode/HexEncode>. The page has a header with a search bar and navigation links. The main content area is divided into two columns. The left column contains a form titled "Dẫn văn bản bạn muốn Hex mã hóa ở đây:" (Paste the text you want to hex encode here:). The form contains the text "I owe you \$2000" and "I owe you \$3000". Below the form is a button labeled "Hex Encode". The right column contains a section titled "Sao chép văn bản được mã hóa Hex của bạn ở đây:" (Copy the hex encoded text of your text here:). This section contains the hex encoded text "49206F776520796F75202432303030" and "49206F776520796F75202433303030". Below this is a button labeled "Hex Decode".

Below the browser window is a terminal window showing the execution of a program. The terminal output is as follows:

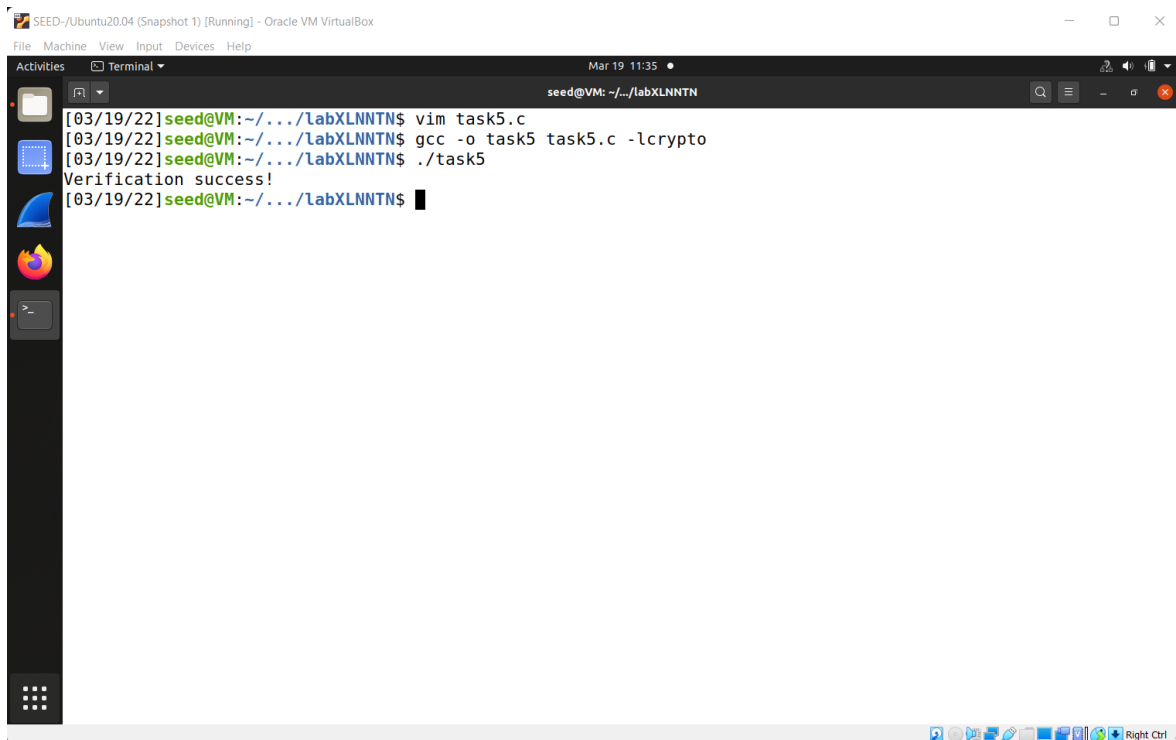
```
[03/19/22]seed@VM:~/.../LabXLNNTN$ vim task4.c
[03/19/22]seed@VM:~/.../LabXLNNTN$ gcc -o task4 task4.c -lcrypto
[03/19/22]seed@VM:~/.../LabXLNNTN$ ./task4
M: 80A55421D72345AC199836F60D51DC9594E2BDB4AE20C804823FB71660DE7B82
M1: 04FC9C53ED7BBE4ED4BE2C24B0BDF7184B96290B4ED4E3959F58E94B1ECEAE2EB
[03/19/22]seed@VM:~/.../LabXLNNTN$
```

Sau khi encode 2 câu chỉ khác nhau một chữ số

Nhưng sau khi mã hóa thì M và M1 hoàn toàn khác nhau

5. Task5

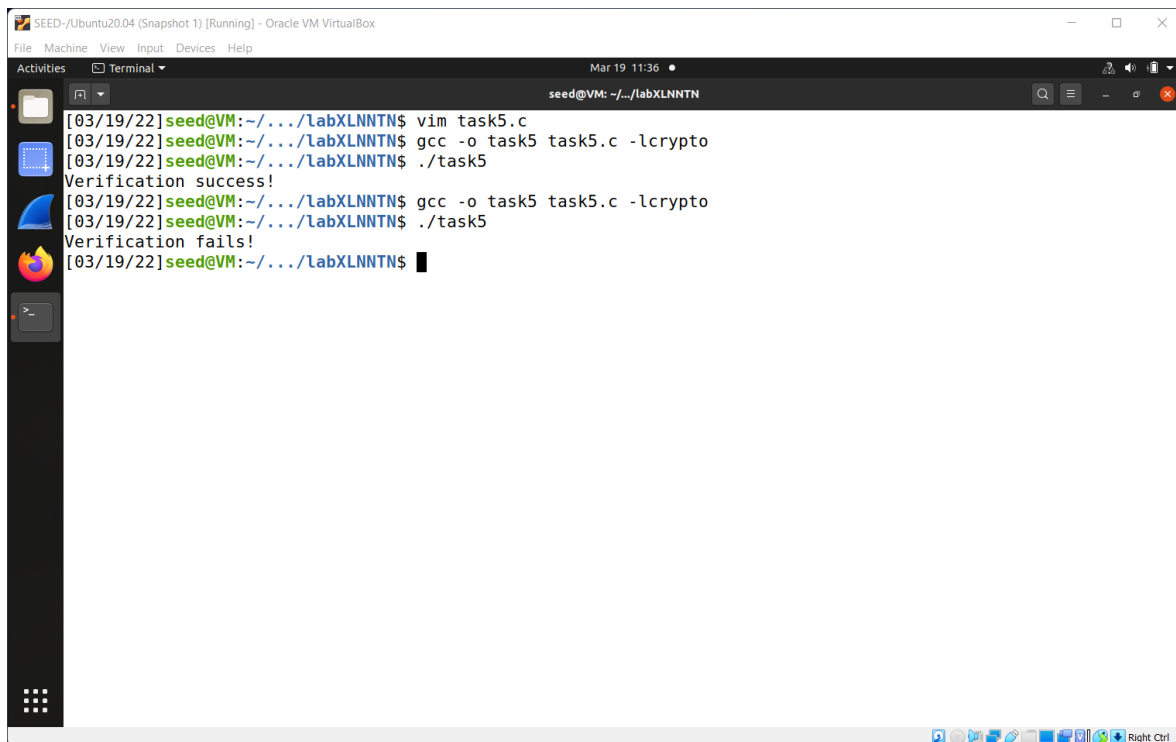
Đối với 2 bytes cuối cùng là 2F (xác nhận đúng)



The screenshot shows a terminal window titled "SEED-/Ubuntu20.04 (Snapshot 1) [Running] - Oracle VM VirtualBox". The terminal output is as follows:

```
seed@VM: ~/.../labXLNNTN
[03/19/22]seed@VM:~/.../labXLNNTN$ vim task5.c
[03/19/22]seed@VM:~/.../labXLNNTN$ gcc -o task5 task5.c -lcrypto
[03/19/22]seed@VM:~/.../labXLNNTN$ ./task5
Verification success!
[03/19/22]seed@VM:~/.../labXLNNTN$
```

Đối với 2 bytes cuối là 3F (xác nhận sai)

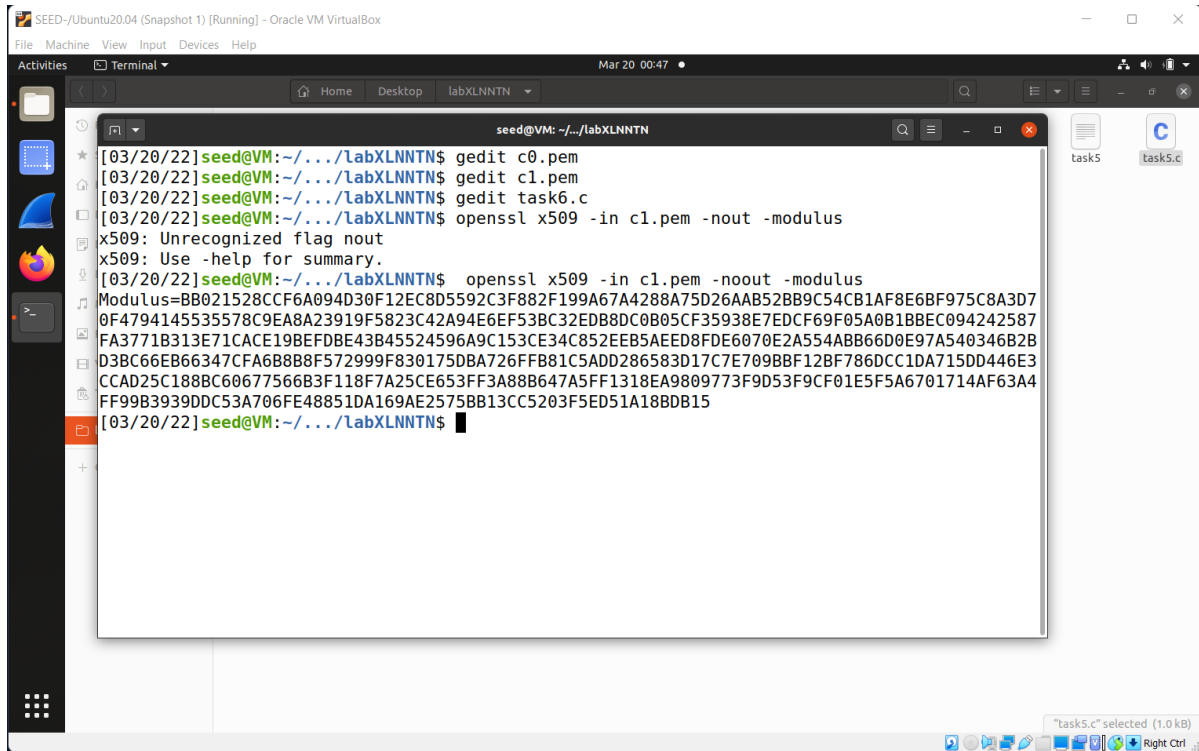


The screenshot shows a terminal window titled "SEED-/Ubuntu20.04 (Snapshot 1) [Running] - Oracle VM VirtualBox". The terminal output is as follows:

```
seed@VM: ~/.../labXLNNTN
[03/19/22]seed@VM:~/.../labXLNNTN$ vim task5.c
[03/19/22]seed@VM:~/.../labXLNNTN$ gcc -o task5 task5.c -lcrypto
[03/19/22]seed@VM:~/.../labXLNNTN$ ./task5
Verification success!
[03/19/22]seed@VM:~/.../labXLNNTN$ gcc -o task5 task5.c -lcrypto
[03/19/22]seed@VM:~/.../labXLNNTN$ ./task5
Verification fails!
[03/19/22]seed@VM:~/.../labXLNNTN$
```

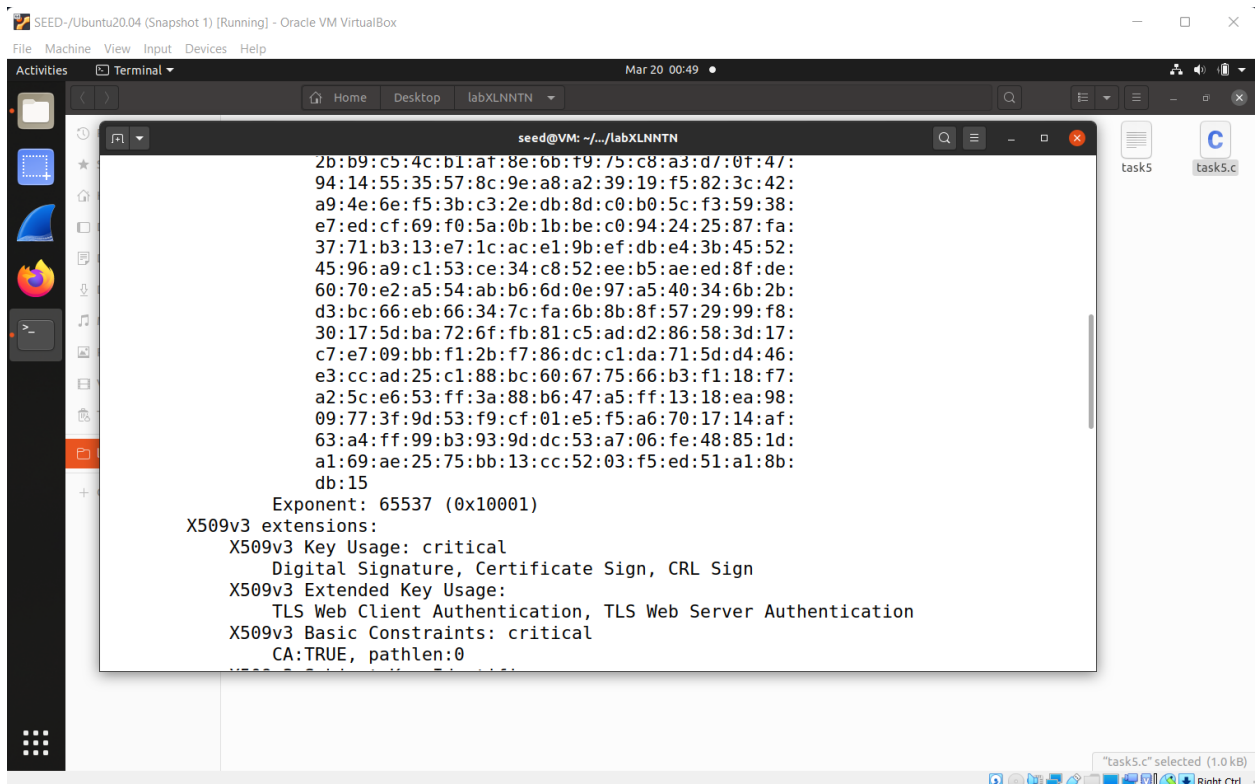
6. Task6

Tim Modulus n:



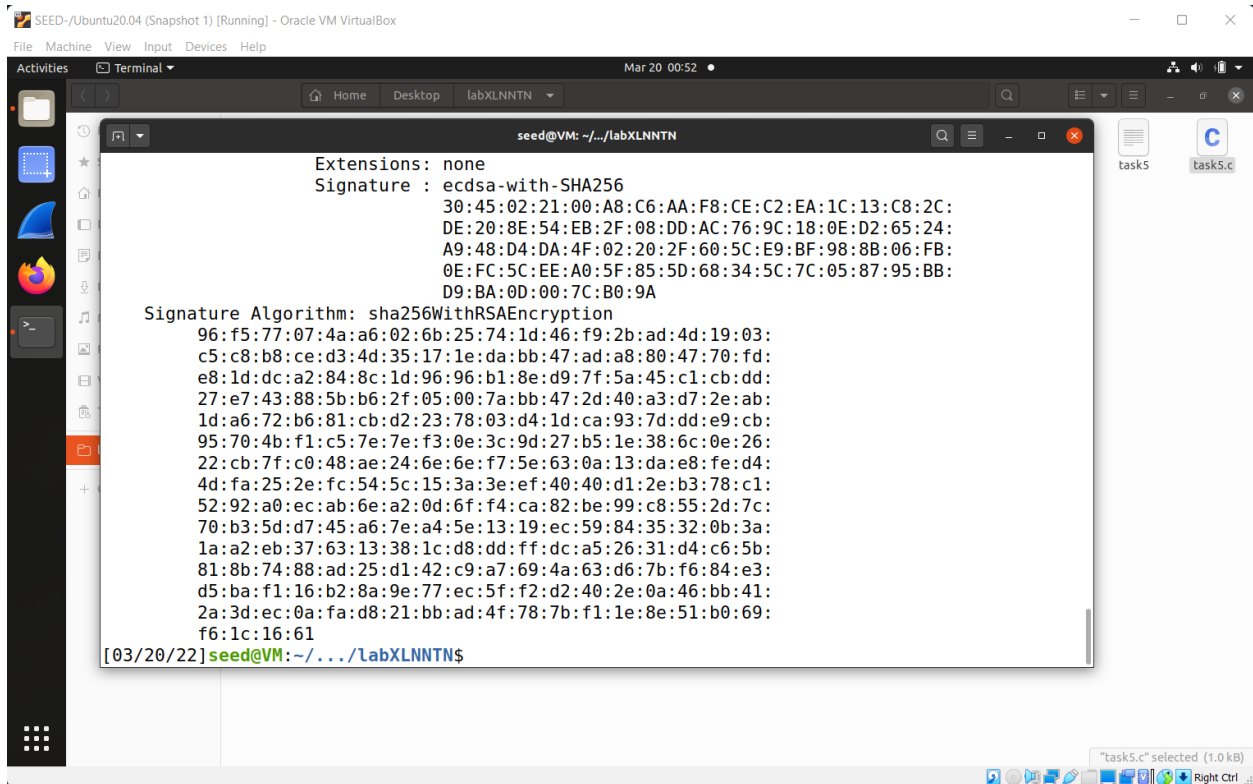
```
seed@VM: ~/.../labXLNNTN
[03/20/22]seed@VM:~/.../labXLNNTN$ gedit c0.pem
[03/20/22]seed@VM:~/.../labXLNNTN$ gedit c1.pem
[03/20/22]seed@VM:~/.../labXLNNTN$ gedit task6.c
[03/20/22]seed@VM:~/.../labXLNNTN$ openssl x509 -in c1.pem -nout -modulus
x509: Unrecognized flag nout
x509: Use -help for summary.
[03/20/22]seed@VM:~/.../labXLNNTN$ openssl x509 -in c1.pem -noout -modulus
Modulus=BB021528CCF6A094D30F12EC8D5592C3F882F199A67A4288A75D26AAB52BB9C54CB1AF8E6BF975C8A3D7
0F4794145535578C9EA8A23919F5823C42A94E6EF53BC32EDB8DC0B05CF35938E7EDCF69F05A0B1BBEC094242587
FA3771B313E71CACE19BEFDBE43B45524596A9C153CE34C852EEB5AEED8FDE6070E2A554ABB66D0E97A540346B2B
D3BC66EB66347CFA6B8B8F572999F830175DBA726FFB81C5ADD286583D17C7E709BBF12BF786DCC1DA715DD446E3
CCAD25C188BC60677566B3F118F7A25CE653FF3A88B647A5FF1318EA9809773F9D53F9CF01E5F5A6701714AF63A4
FF99B3939DDC53A706FE48851DA169AE2575BB13CC5203F5ED51A18BD15
[03/20/22]seed@VM:~/.../labXLNNTN$
```

Tim khóa công khai e: 65537



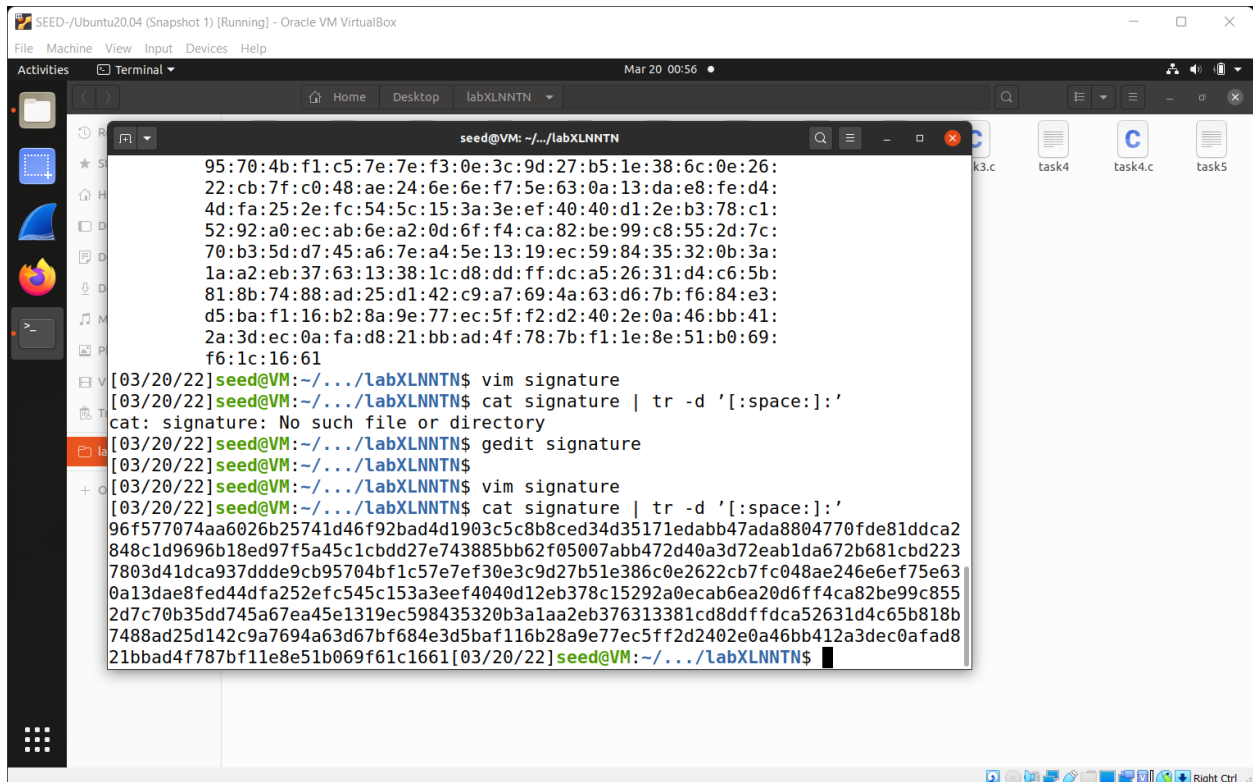
```
seed@VM: ~/.../labXLNNTN
2b:b9:c5:4c:b1:af:8e:bb:f9:75:c8:a3:d7:0f:47:
94:14:55:35:57:8c:9e:a8:a2:39:19:f5:82:3c:42:
a9:4e:6e:f5:3b:c3:2e:db:8d:c0:b0:5c:f3:59:38:
e7:ed:cf:69:f0:5a:0b:1b:be:c0:94:24:25:87:fa:
37:71:b3:13:e7:1c:ac:e1:9b:ef:db:e4:3b:45:52:
45:96:a9:c1:53:ce:34:c8:52:ee:b5:ae:ed:8f:de:
60:70:e2:a5:54:ab:b6:6d:0e:97:a5:40:34:6b:2b:
d3:bc:66:eb:66:34:7c:fa:6b:8b:8f:57:29:99:f8:
30:17:5d:ba:72:6f:fb:81:c5:ad:d2:86:58:3d:17:
c7:e7:09:bb:f1:2b:f7:86:dc:c1:da:71:5d:d4:46:
e3:cc:ad:25:c1:88:bc:60:67:75:66:b3:f1:18:f7:
a2:5c:e6:53:ff:3a:88:b6:47:a5:ff:13:18:ea:98:
09:77:3f:9d:53:f9:cf:01:e5:f5:a6:70:17:14:af:
63:a4:ff:99:b3:93:9d:dc:53:a7:06:fe:48:85:1d:
a1:69:ae:25:75:bb:13:cc:52:03:f5:ed:51:a1:8b:
db:15
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Key Usage: critical
Digital Signature, Certificate Sign, CRL Sign
X509v3 Extended Key Usage:
TLS Web Client Authentication, TLS Web Server Authentication
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:0
```

Tim S



```
seed@VM: ~/.../labXLNNTN
Extensions: none
Signature : ecdsa-with-SHA256
30:45:02:21:00:A8:C6:AA:F8:CE:C2:EA:1C:13:C8:2C:
DE:20:8E:54:EB:2F:08:DD:AC:76:9C:18:0E:D2:65:24:
A9:48:D4:DA:4F:02:20:2F:60:5C:E9:BF:98:8B:06:FB:
0E:FC:5C:EE:A0:5F:85:5D:68:34:5C:7C:05:87:95:BB:
D9:BA:0D:00:7C:B0:9A
Signature Algorithm: sha256WithRSAEncryption
96:f5:77:07:4a:a6:02:6b:25:74:1d:46:f9:2b:ad:4d:19:03:
c5:c8:b8:ce:d3:4d:35:17:1e:da:bb:47:ad:a8:80:47:70:fd:
e8:1d:dc:a2:84:8c:1d:96:96:b1:8e:d9:7f:5a:45:c1:cb:dd:
27:e7:43:88:5b:b6:2f:05:00:7a:bb:47:2d:40:a3:d7:2e:ab:
1d:a6:72:b6:81:cb:d2:23:78:03:d4:1d:ca:93:7d:dd:e9:cb:
95:70:4b:f1:c5:7e:7e:f3:0e:3c:9d:27:b5:1e:38:6c:0e:26:
22:cb:7f:c0:48:ae:24:6e:6e:f7:5e:63:0a:13:da:e8:fe:d4:
4d:fa:25:2e:fc:54:5c:15:3a:3e:ef:40:40:d1:2e:b3:78:c1:
52:92:a0:ec:ab:6e:a2:0d:6f:f4:ca:82:be:99:c8:55:2d:7c:
70:b3:5d:d7:45:a6:7e:a4:5e:13:19:ec:59:84:35:32:0b:3a:
1a:a2:eb:37:63:13:38:1c:d8:dd:ff:dc:a5:26:31:d4:c6:5b:
81:8b:74:88:ad:25:d1:42:c9:a7:69:4a:63:d6:7b:f6:84:e3:
d5:ba:f1:16:b2:8a:9e:77:ec:5f:f2:d2:40:2e:0a:46:bb:41:
2a:3d:ec:0a:fa:d8:21:bb:ad:4f:78:7b:f1:1e:8e:51:b0:69:
f6:1c:16:61
[03/20/22] seed@VM: ~/.../LabXLNNTN$
```

Cắt signature sau đó cắt dấu “:” và khoảng trắng ta được S



```
seed@VM: ~/.../labXLNNTN
95:70:4b:f1:c5:7e:7e:f3:0e:3c:9d:27:b5:1e:38:6c:0e:26:
22:cb:7f:c0:48:ae:24:6e:6e:f7:5e:63:0a:13:da:e8:fe:d4:
4d:fa:25:2e:fc:54:5c:15:3a:3e:ef:40:40:d1:2e:b3:78:c1:
52:92:a0:ec:ab:6e:a2:0d:6f:f4:ca:82:be:99:c8:55:2d:7c:
70:b3:5d:d7:45:a6:7e:a4:5e:13:19:ec:59:84:35:32:0b:3a:
1a:a2:eb:37:63:13:38:1c:d8:dd:ff:dc:a5:26:31:d4:c6:5b:
81:8b:74:88:ad:25:d1:42:c9:a7:69:4a:63:d6:7b:f6:84:e3:
d5:ba:f1:16:b2:8a:9e:77:ec:5f:f2:d2:40:2e:0a:46:bb:41:
2a:3d:ec:0a:fa:d8:21:bb:ad:4f:78:7b:f1:1e:8e:51:b0:69:
f6:1c:16:61
[03/20/22] seed@VM: ~/.../LabXLNNTN$ vim signature
[03/20/22] seed@VM: ~/.../LabXLNNTN$ cat signature | tr -d '[:space:]'
cat: signature: No such file or directory
[03/20/22] seed@VM: ~/.../LabXLNNTN$ gedit signature
[03/20/22] seed@VM: ~/.../LabXLNNTN$ vim signature
[03/20/22] seed@VM: ~/.../LabXLNNTN$ cat signature | tr -d '[:space:]'
96f577074aa026b25741d46f92bad4d1903c5c8b8ced34d35171edabb47ada8804770fde81ddca2
848c1d9696b18ed97f5a45c1cbdd27e743885bb62f05007abb472d40a3d72eab1da672b681cbd223
7803d41dca937ddde9cb95704bf1c57e7ef30e3c9d27b51e386c0e2622cb7fc048ae246e6ef75e63
0a13dae8fed44dfa252efc545c153a3eef4040d12eb378c15292a0ecab6ea20d6ff4ca82be99c855
2d7c70b35dd745a67ea45e1319ec598435320b3a1aa2eb376313381cd8ddffdc52631d4c65b818b
7488ad25d142c9a7694a63d67bf684e3d5baf116b28a9e77ec5ff2d2402e0a46bb412a3dec0afad8
21bbad4f787bf11e8e51b069f61c1661[03/20/22] seed@VM: ~/.../LabXLNNTN$
```


Body của chứng chỉ

```
SEED-/Ubuntu20.04 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mar 20 01:13
Home Desktop labXLNNTN
seed@VM: ~/labXLNNTN
3656375726974796C6162732E6F7267
712:d=4 hl=2 l= 76 cons: SEQUENCE
714:d=5 hl=2 l= 3 prim: OBJECT :X509v3 Certificate Policies
719:d=5 hl=2 l= 69 prim: OCTET STRING [HEX DUMP]:30433008060667810
C0102013037060B2B0601040182DF130101013028302606082B06010505070201161A687474703A2
F2F6370732E6C657473656E63727970742E6F7267
790:d=4 hl=4 l= 259 cons: SEQUENCE
794:d=5 hl=2 l= 10 prim: OBJECT :CT Precertificate SCTs
806:d=5 hl=3 l= 244 prim: OCTET STRING [HEX DUMP]:0481F100EF0075004
1C8CAB1DF22464A10C6A13A0942875E4E318B1B03EBE84BC768F090629606F60000017F526A968F0
00004030046304402200E92D1E455F9DC1EAA72E5B69366AF8E34A4A39ECA20EB1FD34736E2809C
EDA02204EFD3B78C49CB6033251E5C7E25FC7C20DD5C3518E0542E93F0E4D192A840E42007600297
9BEF09E393921F056739F63A577E5BE577D9C600AF8F94D5D265C255DC7840000017F526A967E000
0040300473045022100A8C6AAF8CEC2EA1C13C82CDE208E54EB2F08DDAC769C180ED26524A948D4D
A4F02202F605CE9BF988B06FB0EFC5CEE0A5F855D68345C7C058795BBD9BA0D007CB09A
1053:d=1 hl=2 l= 13 cons: SEQUENCE
1055:d=2 hl=2 l= 9 prim: OBJECT :sha256WithRSAEncryption
1066:d=2 hl=2 l= 0 prim: NULL
1068:d=1 hl=4 l= 257 prim: BIT STRING
[03/20/22]seed@VM:~/labXLNNTN$ openssl asn1parse -i -in c0.pem -strparse 4 -
out c0_body.bin -noout
[03/20/22]seed@VM:~/labXLNNTN$ sha256sum c0_body.bin
82a4d4148a78b4fe38ba61382613eca887aafb24b85fa745a69240197153f241 c0_body.bin
[03/20/22]seed@VM:~/labXLNNTN$
```

Tìm M để làm step 5 trong đó A là định danh của SHA-256 [RSA Algorithm \(di-mgt.com.au\)](https://di-mgt.com.au)

```
SEED-/Ubuntu20.04 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mar 20 01:29
task6.c
~/Desktop/labXLNNTN
Save
seed@VM: ~/labXLNNTN
3#
4
5 [03/20/22]seed@VM:~/labXLNNTN$ python
6 Python 2.7.18 (default, Mar 8 2021, 13:02:45)
7 [GCC 9.3.0] on linux2
8 Type "help", "copyright", "credits" or "license" for more information.
9 >>> prefix = "0001"
10 >>> hash = "82a4d4148a78b4fe38ba61382613eca887aafb24b85fa745a69240197153f241"
11 >>> A = "30 31 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00 04 20".replace(' ', '')
12 >>>
13 >>> total_len = 256
14 >>> pad_len = total_len - 1 - (len(A) + len(prefix) + len(hash))//2
15 >>> prefix + "FF" * pad_len + "00" + A + hash
16 '0001FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
17 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
18 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
19 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
20 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
21 FFFFFFFFFF003031300D06096086480165030402010500042082a4d4148a78b4fe38ba61382613eca
22 887aafb24b85fa745a69240197153f241'
23 >>>
24 KeyboardInterrupt
25 >>>
26 //ta su gui thong diep da duoc ma hoa qua ben nhan
27
```

Copy task5 thành task6 và chỉnh lại dữ liệu của task6

```
7 char * number_str = BN_bn2hex(a);
8 printf("%s %s\\n", msg, number_str);
9 OPENSSL_free(number_str);
10 }
11
12 int main()
13 {
14     BN_CTX *ctx = BN_CTX_new();
15     BIGNUM *n = BN_new();
16     BIGNUM *e = BN_new();
17     BIGNUM *M = BN_new();
18     BIGNUM *C = BN_new();
19     BIGNUM *S = BN_new();
20
21     BN_hex2bn(&n,
22     "BB021528CF6A094D30F12EC8D5592C3F882F199A67A4288A75D26AAB52BB9C54CB1AF8E6BF975C8A3D70F4794145535578C9EA8A23
23     BN_dec2bn(&e, "65537");
24     BN_hex2bn(&M,
25     "0001FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
26     BN_hex2bn(&S,
27     "96f577074aa6026b25741d46f92bad4d1903c5c8b8ced34d35171edabb47ada8804770fde81ddca2848c1d9696b18ed97f5a45c1cbd
28     sua 2F thành 3F o day
29
30     //ta su gui thong diep da duoc ma hoa qua ben nhan
31     BN_mod_exp(C, S, e, n, ctx);
32
33     //so sanh thong diep moi ma hoa duoc voi thong diep da co
34     if (BN_cmp(C, M) == 0)//xac minh chu ki
35     {
36         printf("Verification success!\\n");
37     }
38     return 0;
39 }
```

Kết quả

```
[03/20/22] seed@VM: ~/.../labXLNNTN$ vim task6.c
[03/20/22] seed@VM: ~/.../labXLNNTN$ gcc -o task6 task6.c -lcrypto
[03/20/22] seed@VM: ~/.../labXLNNTN$ ./task6
Verification success!
[03/20/22] seed@VM: ~/.../labXLNNTN$
```