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

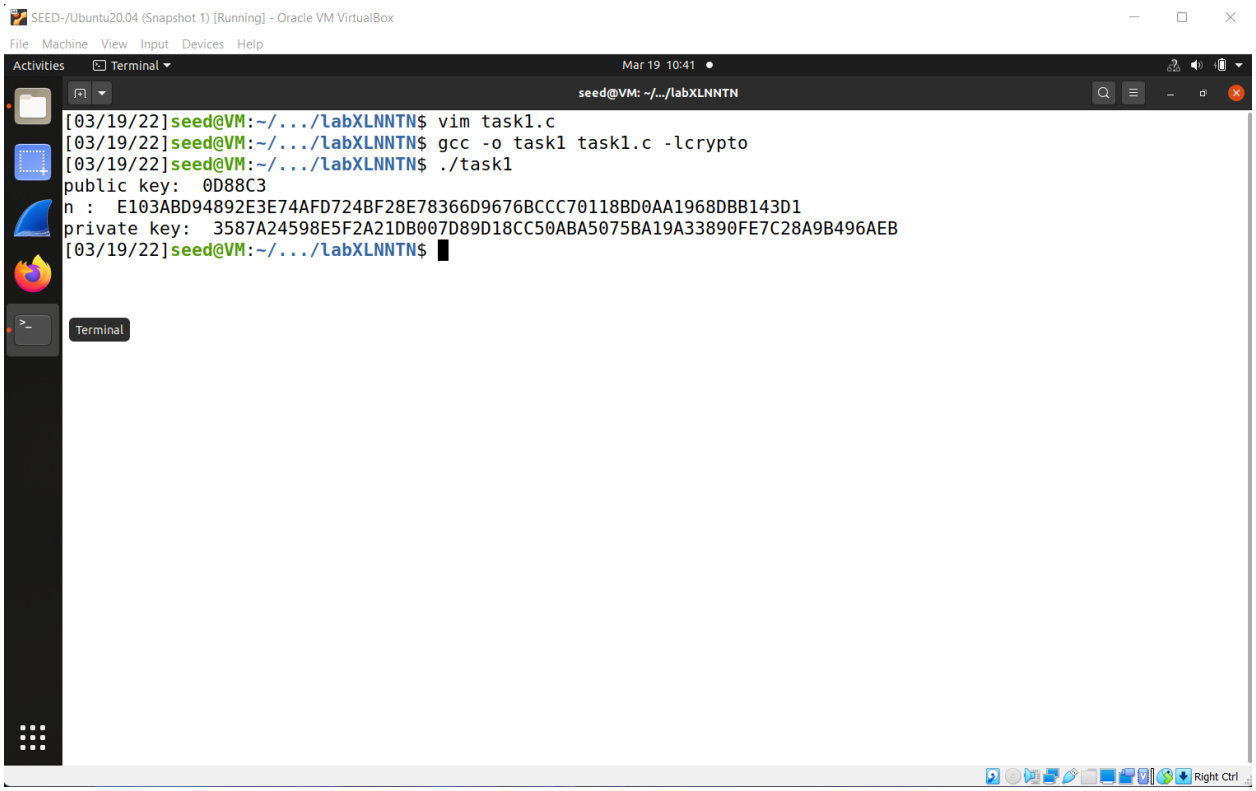
MÔN HỌC: MÃ HÓA ỨNG DỤNG – 19CNTT

REPORT

Nguyễn Quang Thuận – 19127571

Nguyễn Quang Huy – 19127161

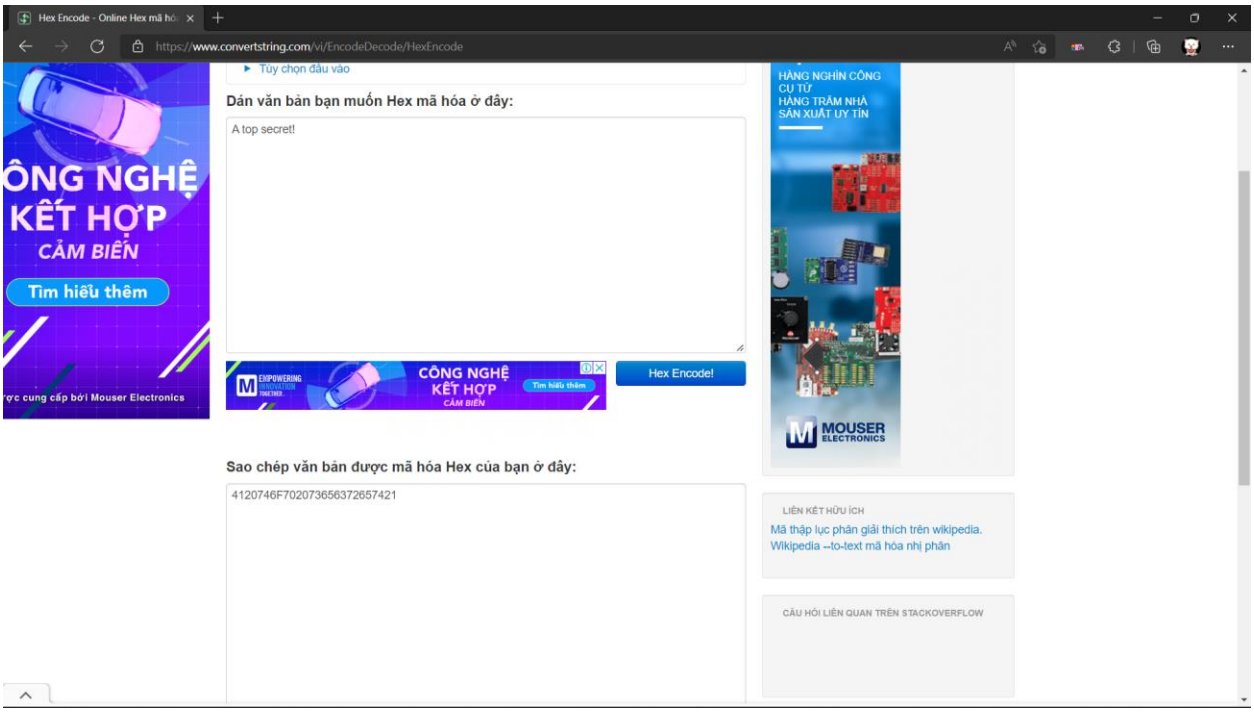
1. Task1

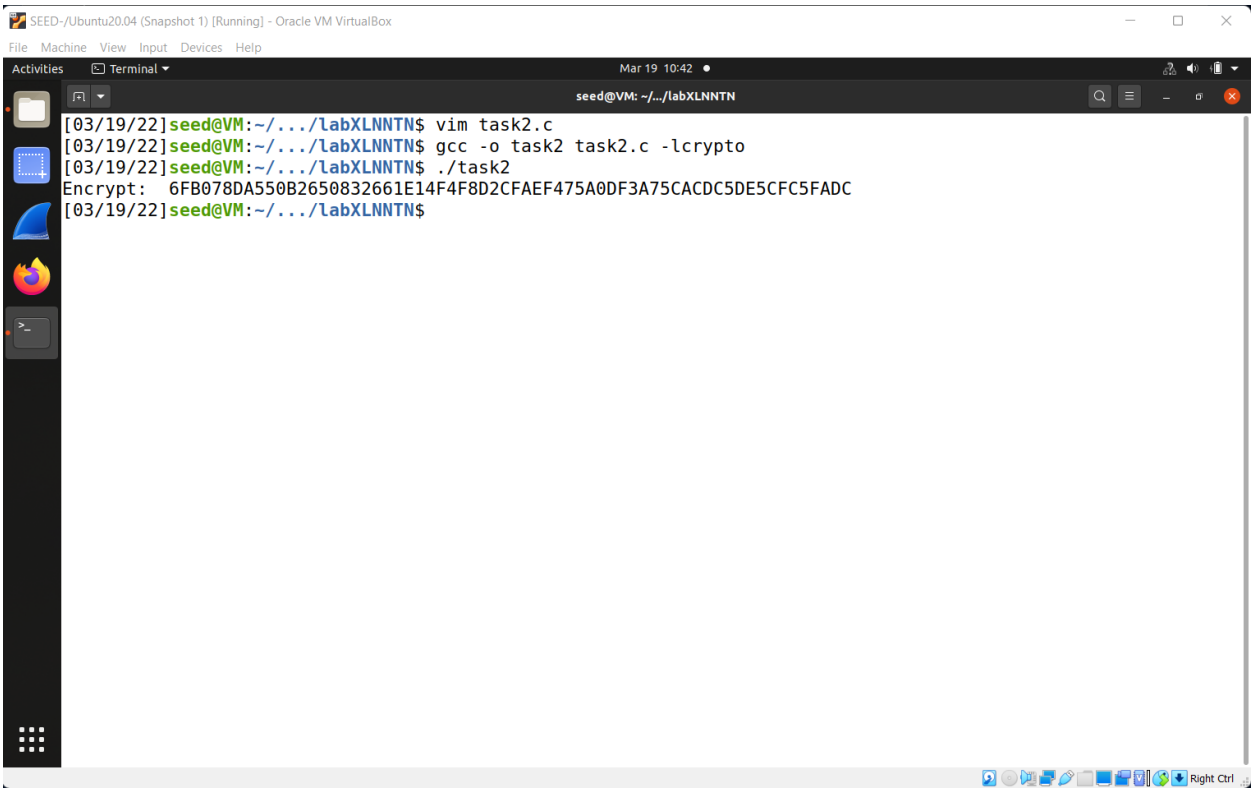

SEED-/Ubuntu20.04 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Mar 19 10:41
seed@VM: ~/.../labXLNNTN
[03/19/22]seed@VM:~/.../labXLNNTN$ vim task1.c
[03/19/22]seed@VM:~/.../labXLNNTN$ gcc -o task1 task1.c -lcrypto
[03/19/22]seed@VM:~/.../labXLNNTN$ ./task1
public key: 0D88C3
n : E103ABD94892E3E74AFD724BF28E78366D9676BCCC70118BD0AA1968DBB143D1
private key: 3587A24598E5F2A21DB007D89D18CC50ABA5075BA19A33890FE7C28A9B496AEB
[03/19/22]seed@VM:~/.../labXLNNTN$
Terminal
Right Ctrl

2. Task2

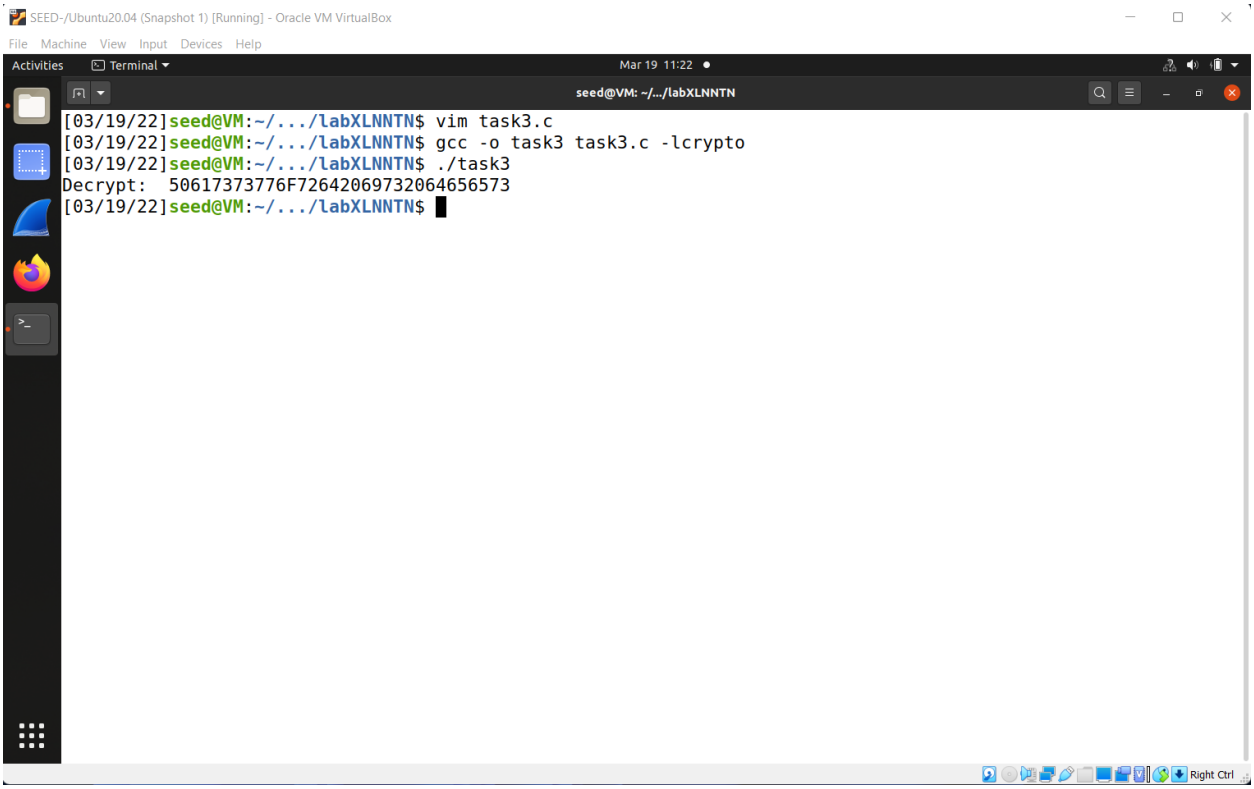
Vì không thể dùng được câu lệnh: python -c ’print("A top secret!".encode("hex"))’
Nên em sẽ dùng cách thay thế cho câu lệnh (cho các task) là trang web:

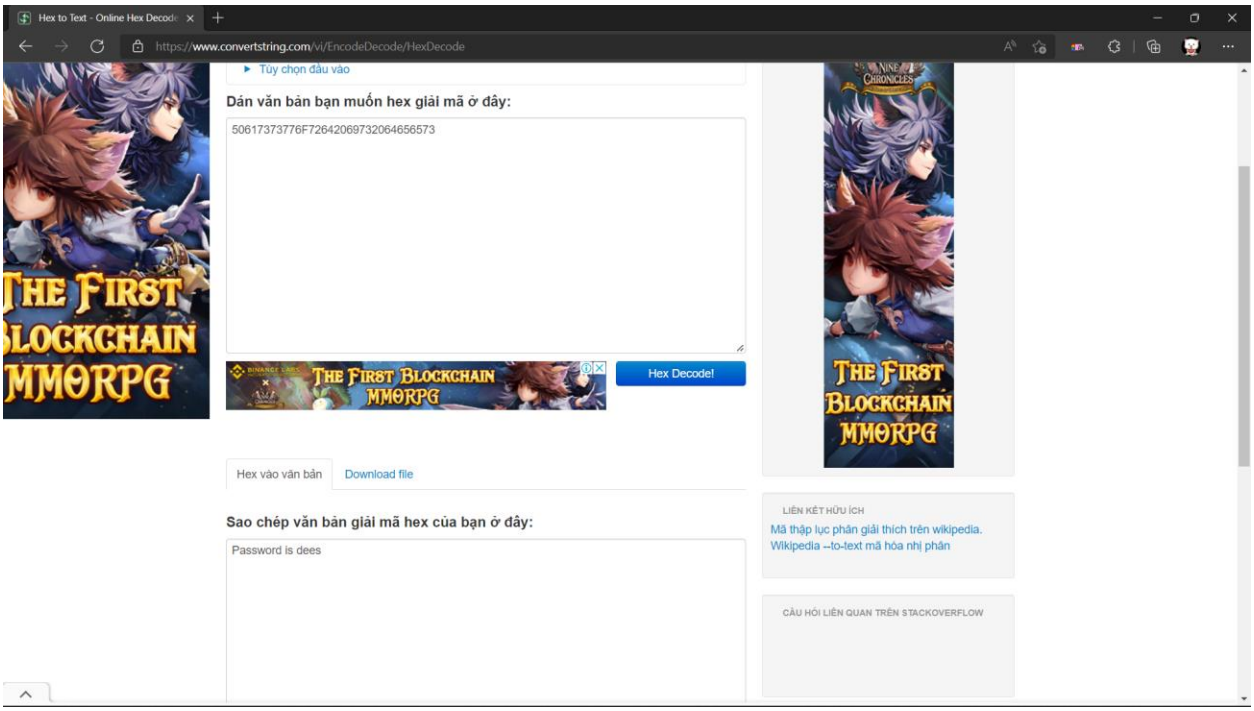
[Hex Encode - Online Hex mã hóa (convertstring.com)]



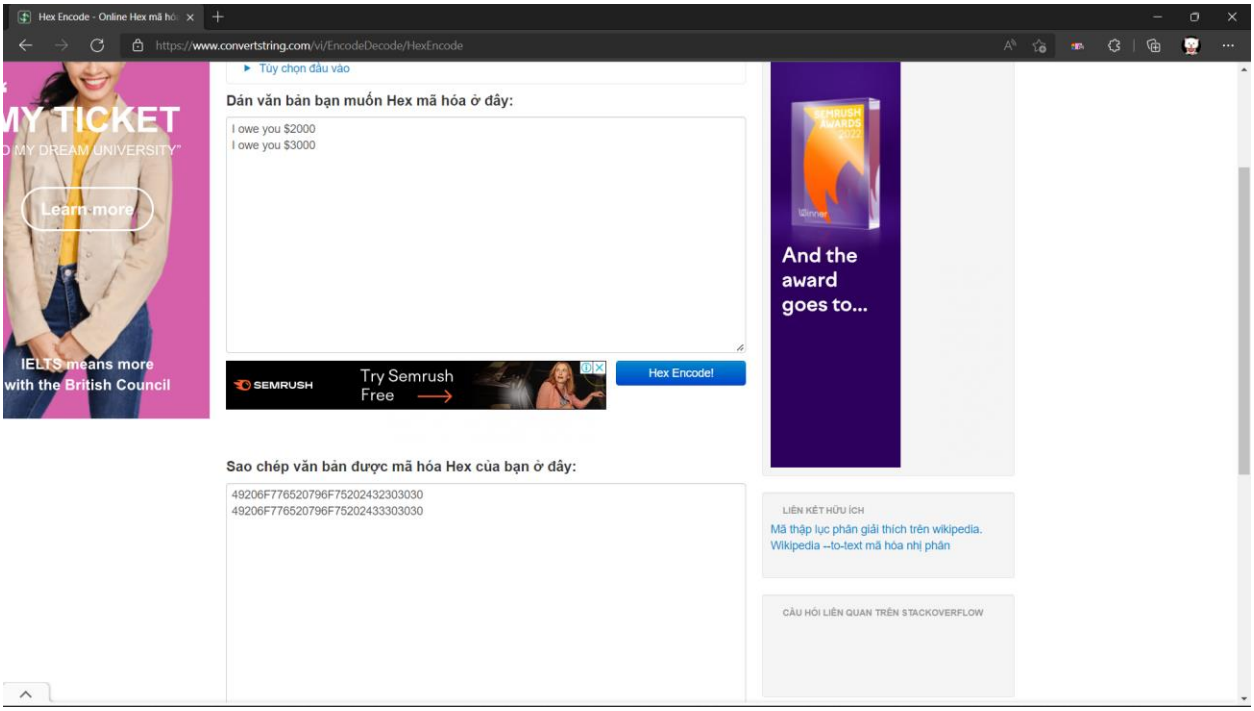


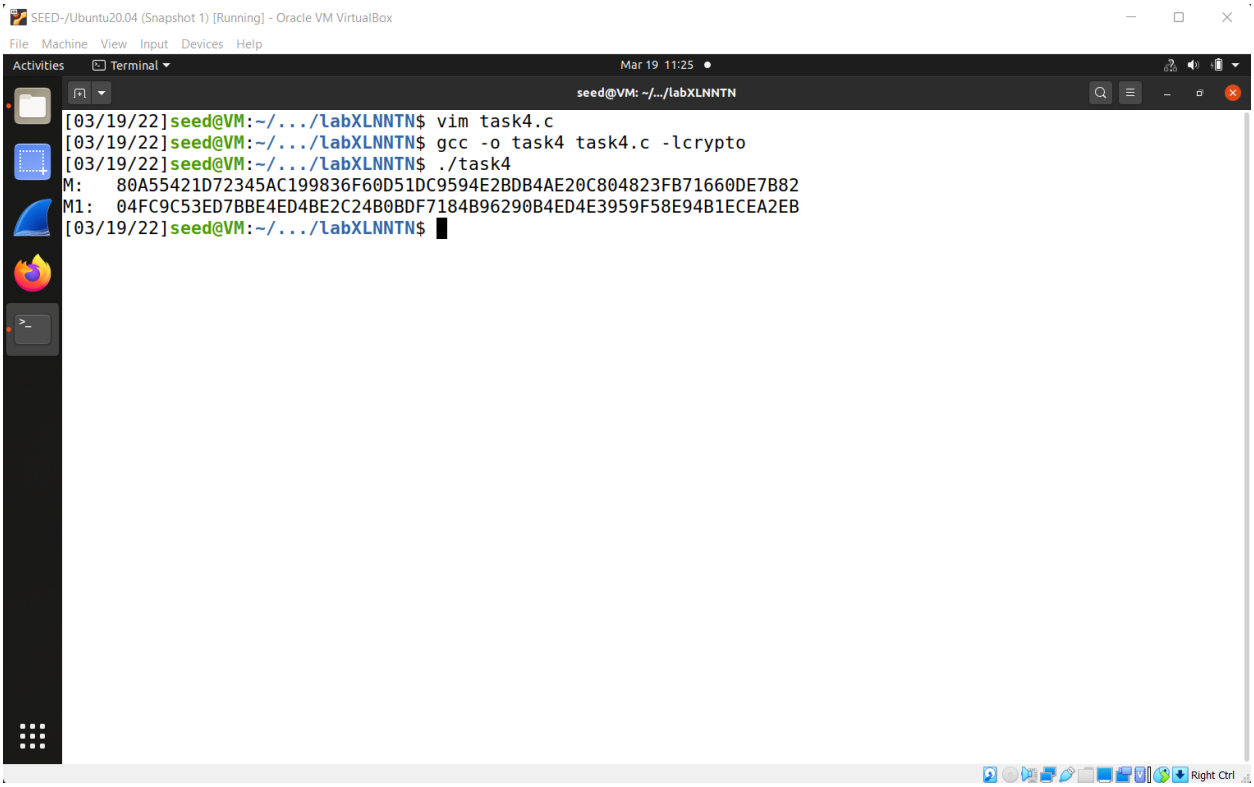
3. Task3


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$
Right Ctrl


Hex to Text - Online Hex Decode
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



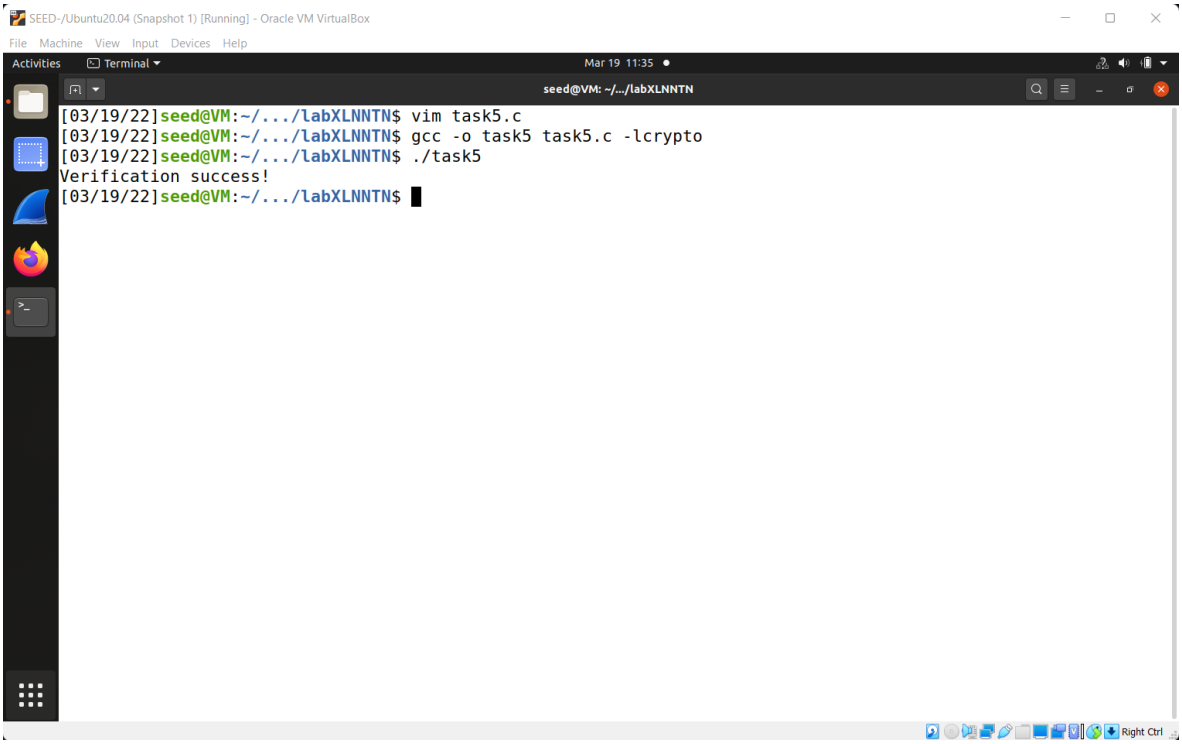


Sau khi encode 2 câu chỉ khác nhau một chữ số

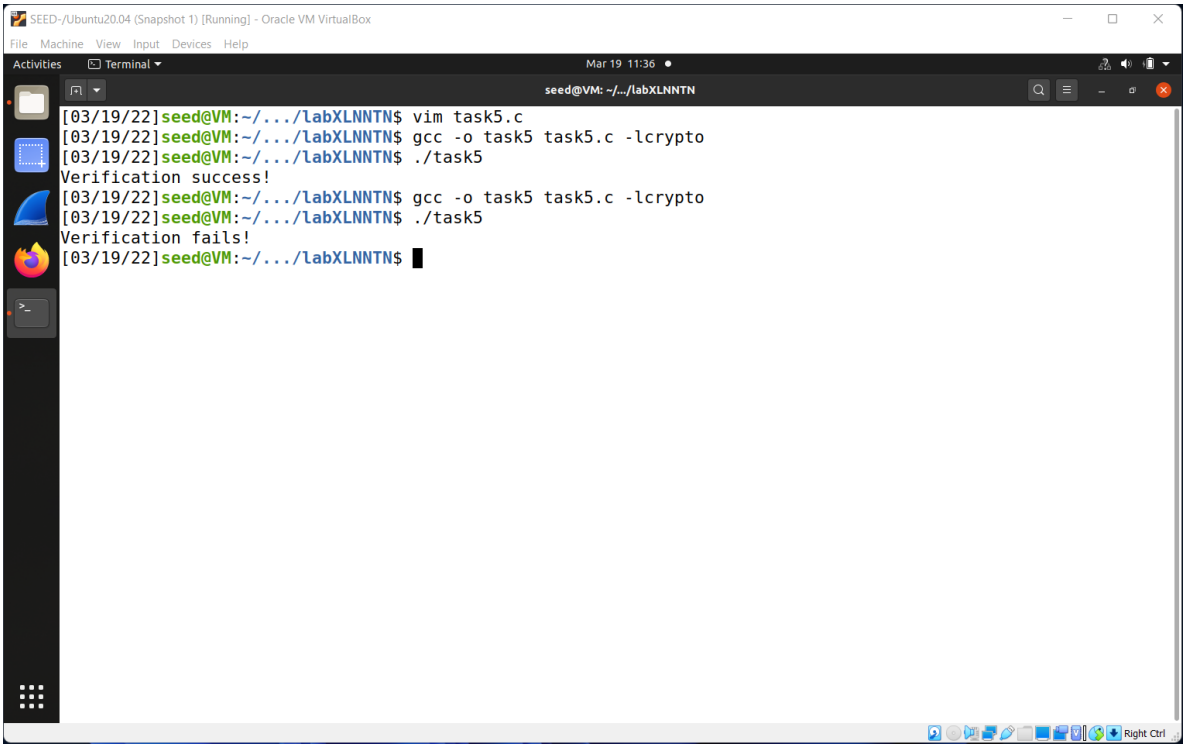
Nhưng sau khi mã hóa thì M và M1 hoàn toàn khác nhau

5. Task5

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

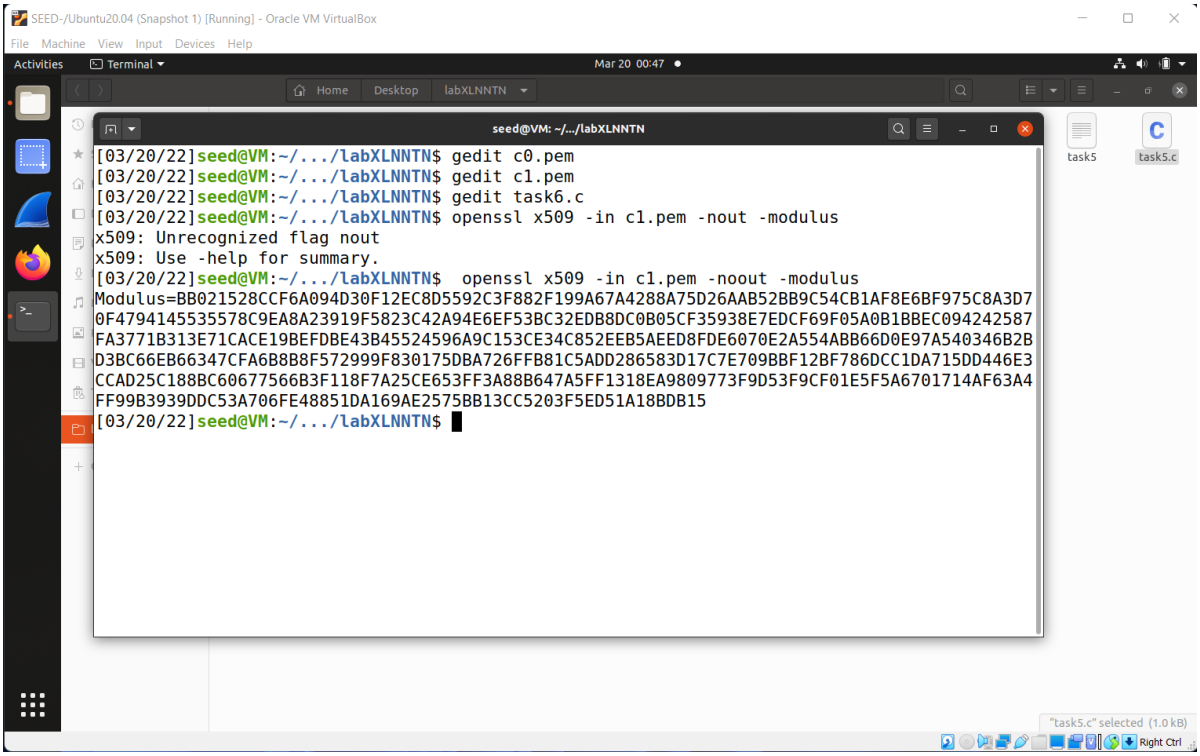


Đối với 2 bytes cuối là 3F (xác nhận sai)

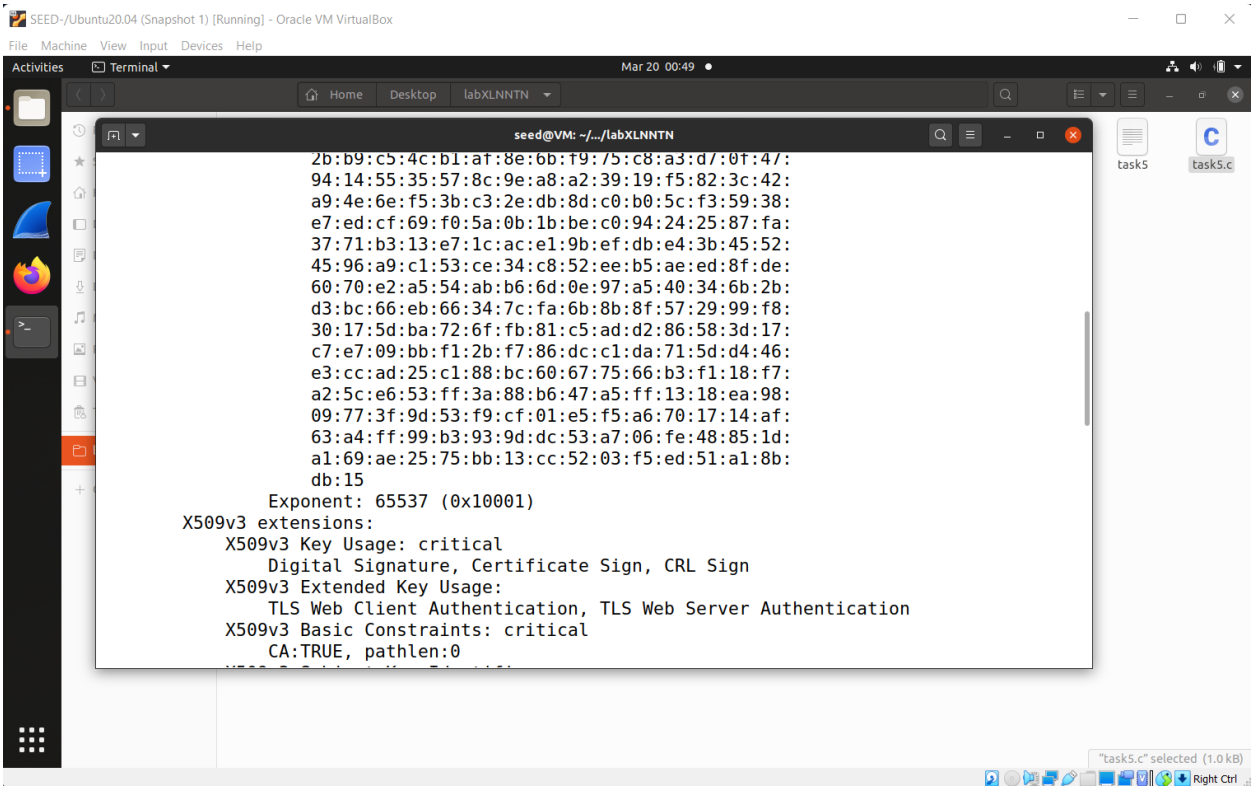


6. Task6

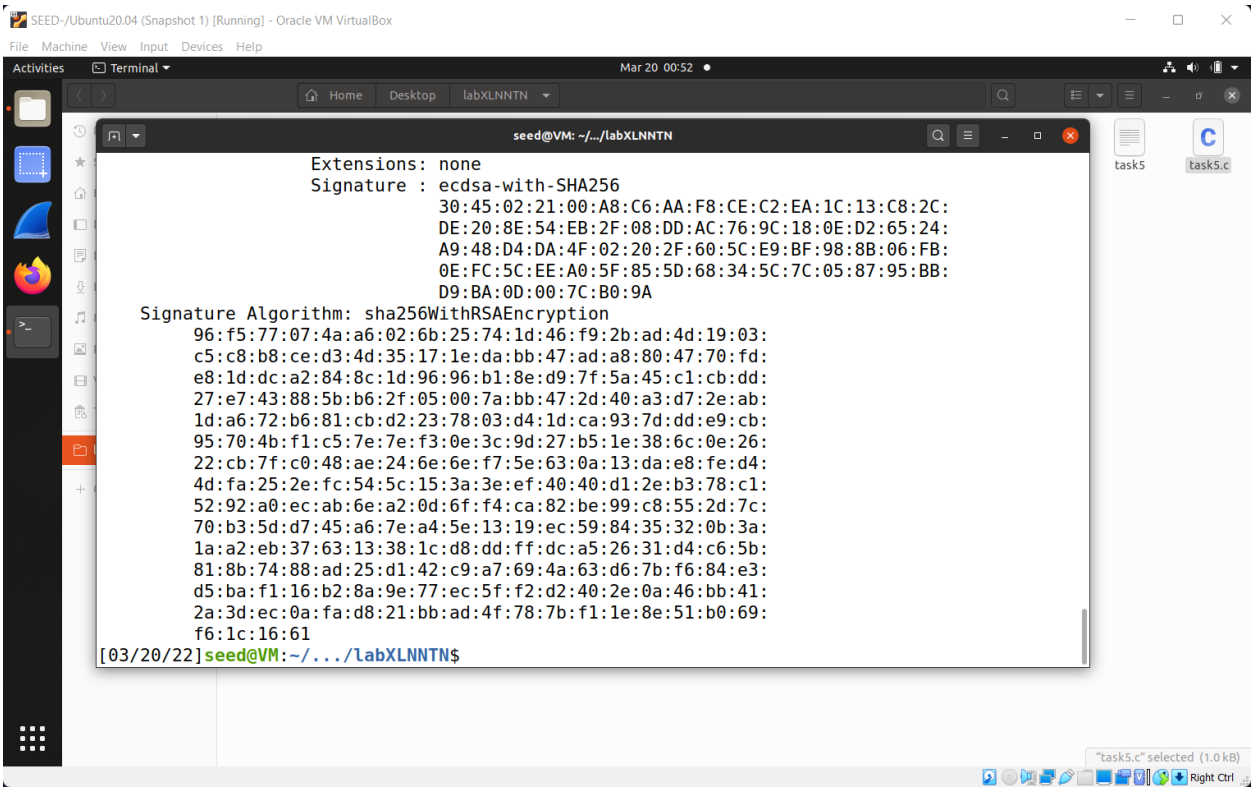
Tìm Modulus n:



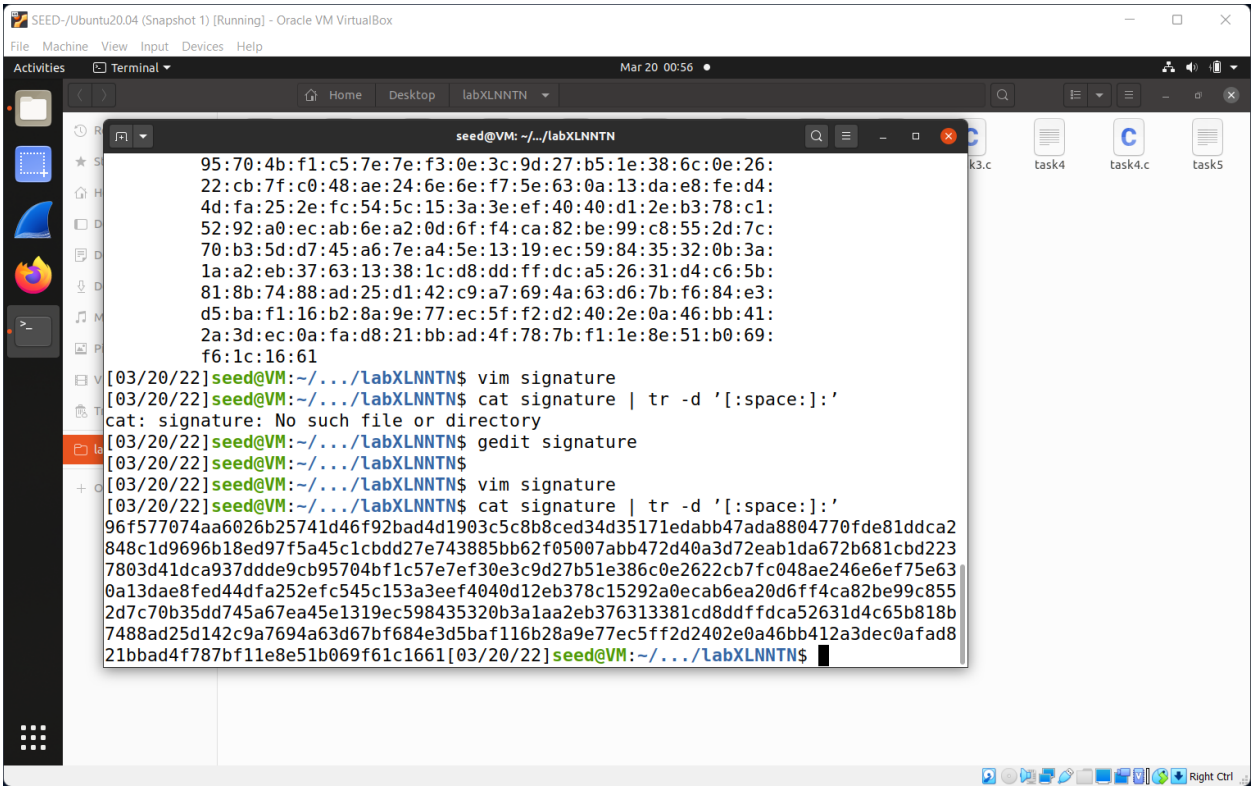
Tìm khóa công khai e: 65537



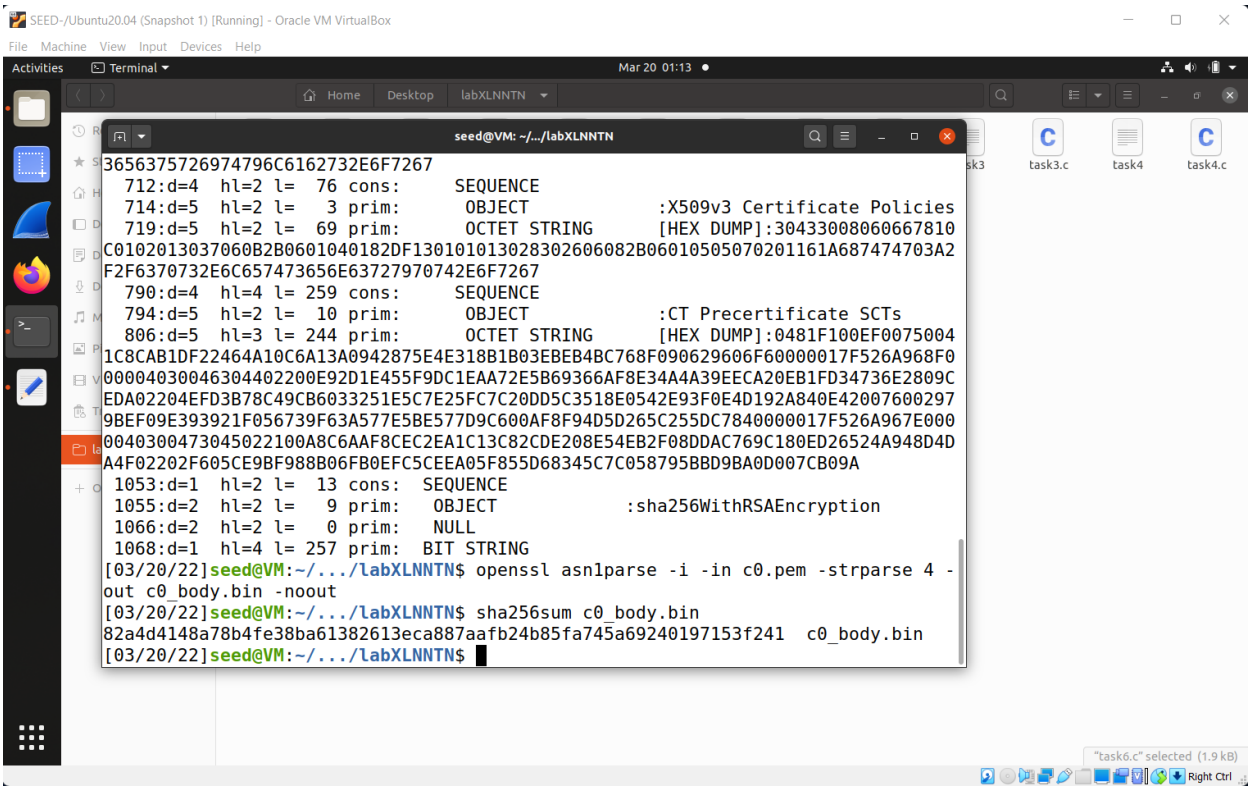
Tìm S



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

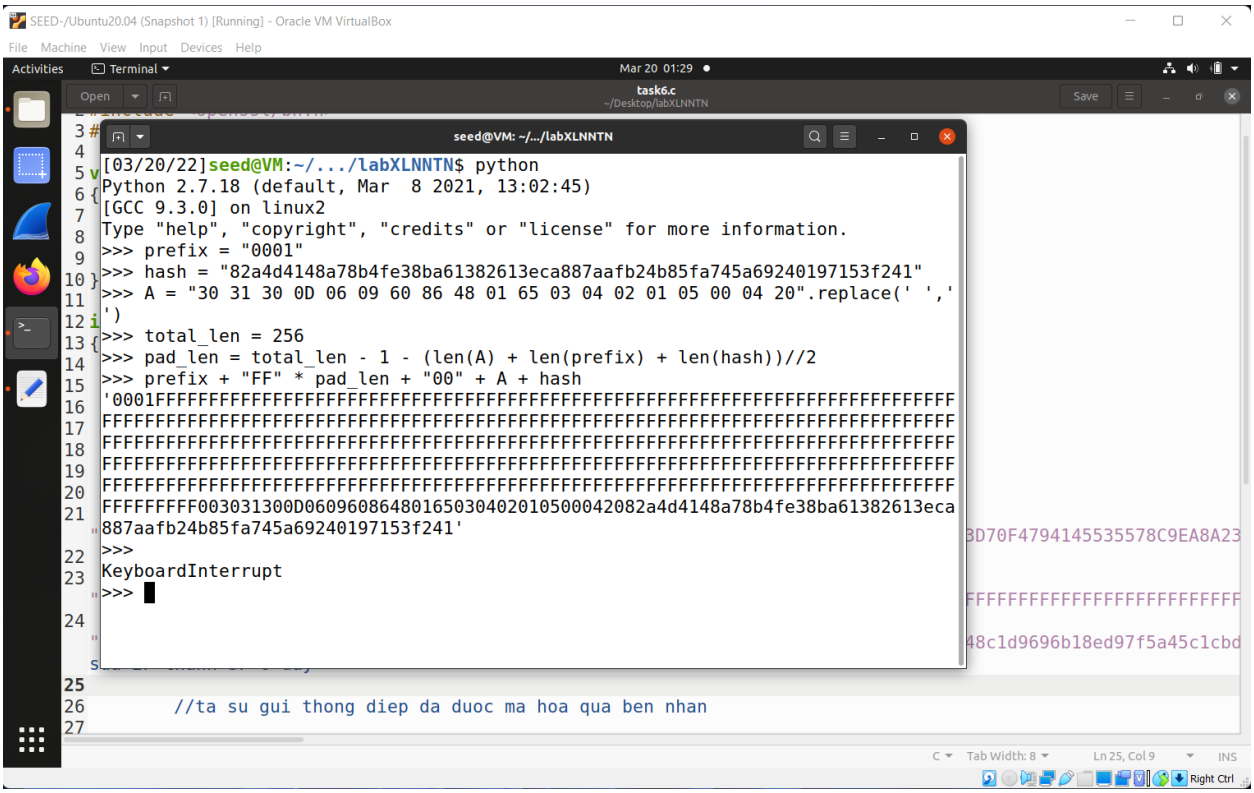


Body của chứng chỉ



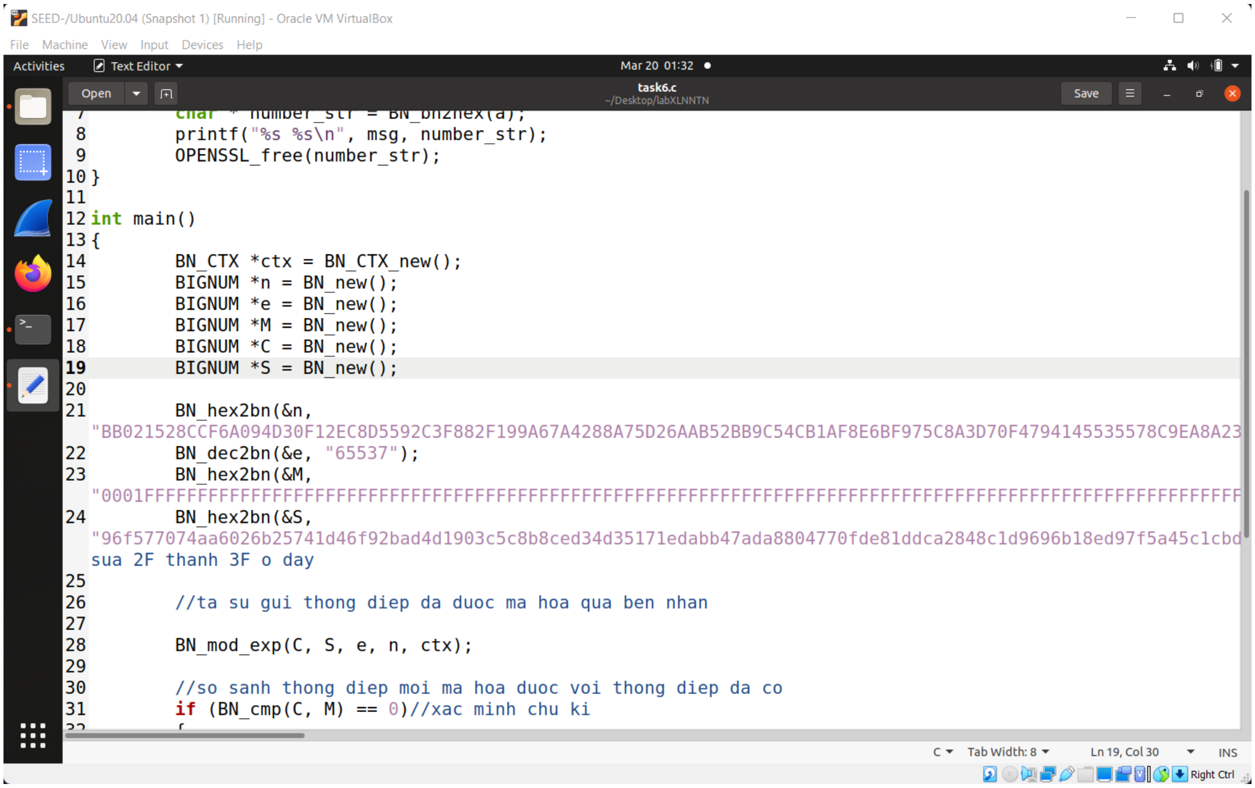
```
3656375726974796C6162732E6F7267
  712:d=4  hl=2 l=  76 cons:     SEQUENCE
  714:d=5  hl=2 l=   3 prim:      OBJECT            :X509v3 Certificate Policies
  719:d=5  hl=2 l=  69 prim:      OCTET STRING      [HEX DUMP]:304330080606667810
C0102013037060B2B0601040182DF130101013028302606082B06010505070201161A687474703A2
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
1C8CAB1DF22464A10C6A13A0942875E4E318B1B03EBEB4BC768F090629606F60000017F526A968F0
000004030046304402200E92D1E455F9DC1EAA72E5B69366AF8E34A4A39EECA20EB1FD34736E2809C
EDA02204EFD3B78C49CB6033251E5C7E25FC7C20DD5C3518E0542E93F0E4D192A840E42007600297
9BEF09E393921F056739F63A577E5BE577D9C600AF8F94D5D265C255DC7840000017F526A967E000
00403004730450221 00A8C6AAF8CEC2EA1C13C82CDE208E54EB2F08DDAC769C180ED26524A948D4D
A4F02202F605CE9BF988B06FB0EFC5CEEA05F855D68345C7C058795BBD9BA0D007CB09A
 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)



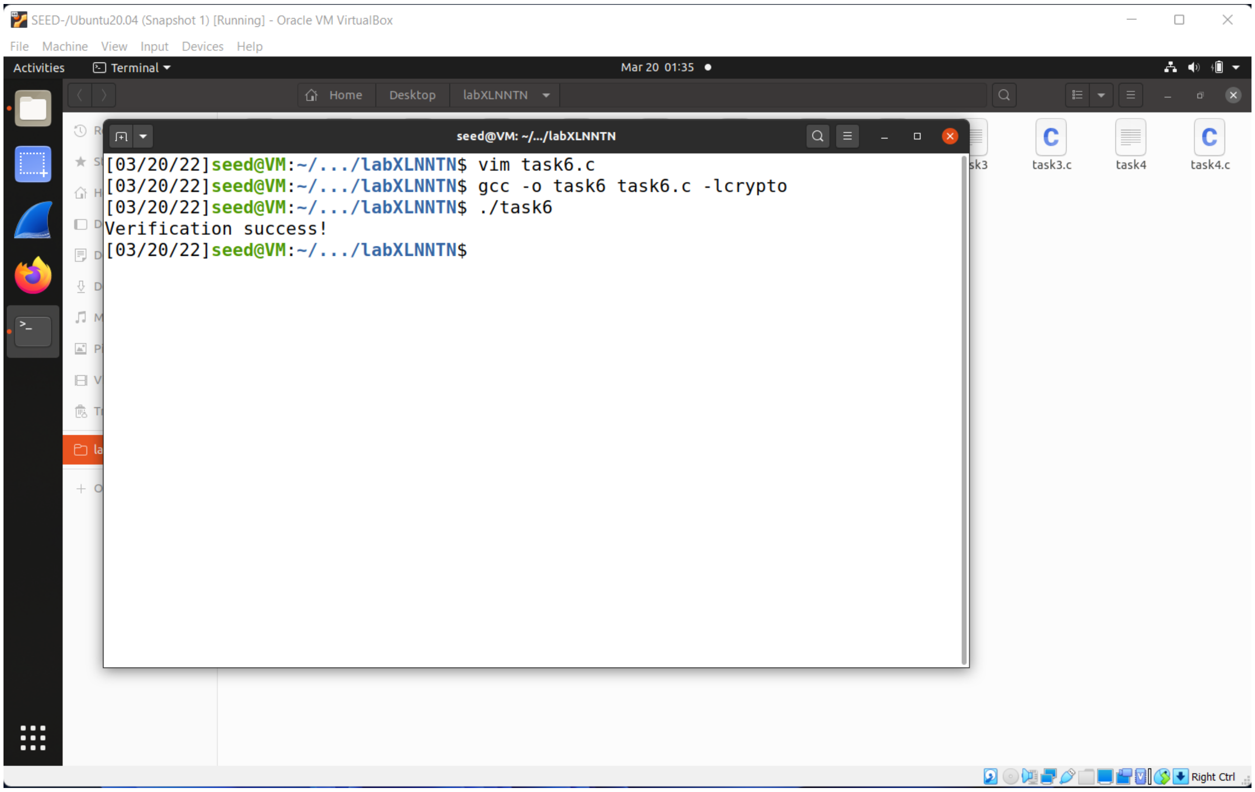
```
[03/20/22]seed@VM:~/.../labXLNNTN$ python
Python 2.7.18 (default, Mar  8 2021, 13:02:45)
[GCC 9.3.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> prefix = "0001"
>>> hash = "82a4d4148a78b4fe38ba61382613eca887aafb24b85fa745a69240197153f241"
>>> A = "30 31 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00 04 20".replace(' ','
')
>>> total_len = 256
>>> pad_len = total_len - 1 - (len(A) + len(prefix) + len(hash))//2
>>> prefix + "FF" * pad_len + "00" + A + hash
'0001FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFF003031300D06096086480165030402010500042082a4d4148a78b4fe38ba61382613eca
887aafb24b85fa745a69240197153f241'
>>>
KeyboardInterrupt
>>> 
```

Copy task5 thành task6 và chỉnh lại dữ liệu của task6



```
        char * number_str = BN_bn2hex(a);
        printf("%s %s\n", msg, number_str);
        OPENSSL_free(number_str);
}

int main()
{
        BN_CTX *ctx = BN_CTX_new();
        BIGNUM *n = BN_new();
        BIGNUM *e = BN_new();
        BIGNUM *M = BN_new();
        BIGNUM *C = BN_new();
        BIGNUM *S = BN_new();

        BN_hex2bn(&n,
"BB021528CCF6A094D30F12EC8D5592C3F882F199A67A4288A75D26AAB52BB9C54CB1AF8E6BF975C8A3D70F4794145535578C9EA8A23
        BN_dec2bn(&e, "65537");
        BN_hex2bn(&M,
"0001FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
        BN_hex2bn(&S,
"96f577074aa6026b25741d46f92bad4d1903c5c8b8ced34d35171edabb47ada8804770fde81ddca2848c1d9696b18ed97f5a45c1cbd
sua 2F thanh 3F o day

        //ta su gui thong diep da duoc ma hoa qua ben nhan

        BN_mod_exp(C, S, e, n, ctx);

        //so sanh thong diep moi ma hoa duoc voi thong diep da co
        if (BN_cmp(C, M) == 0)//xac minh chu ki
        {
```

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$
```