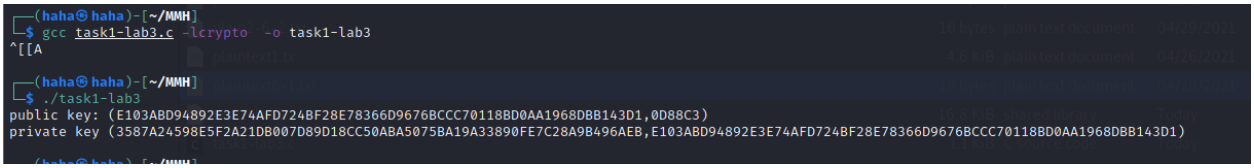
LAB 3.2

Course name: ***Cryptography*** *- Class code:* ***NT219.L21.ANTT.1***
Lecturer: ***Van Thien Luan***

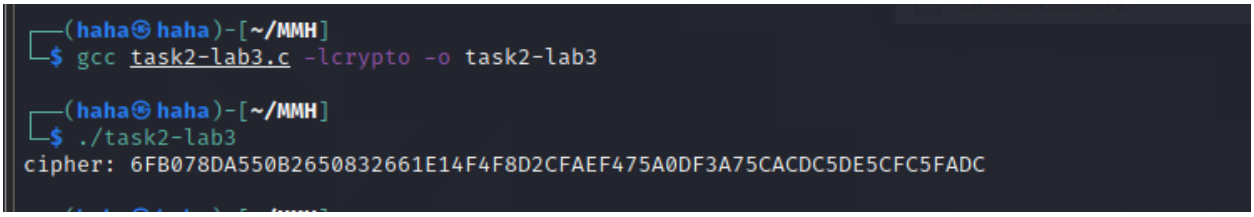
Team's info and task allocation *(actual workload per each member)*	**Team member 1** Student's ID: 19520506 Full name: Nguyễn Thị Hải Hà Task allocation: 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5, 3.2.6 **Team member 2** Student's ID: 19520499 Full name: Lê Thị Hương Giang Task allocation:

Task 1: <source code>

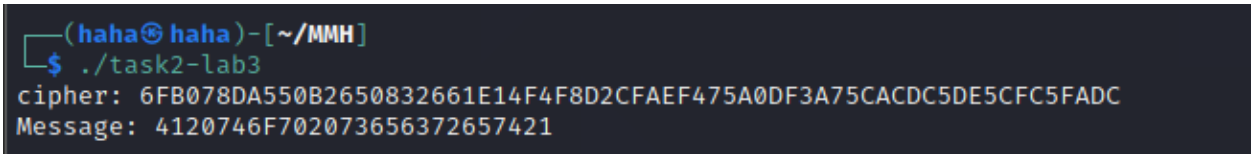
Sau khi sửa đổi một số trong file bn_sample ta có thể tìm ra được private key



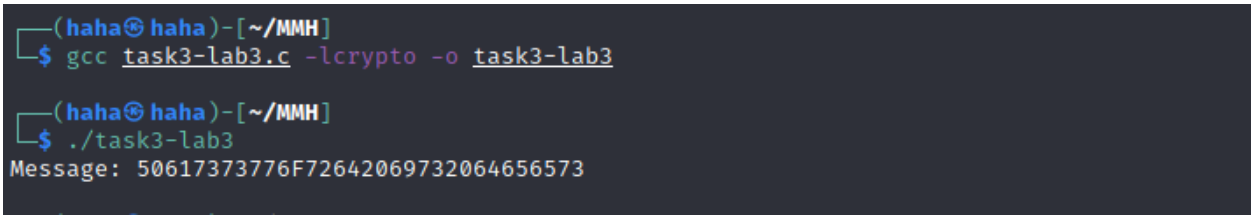
Task 2: <source code>

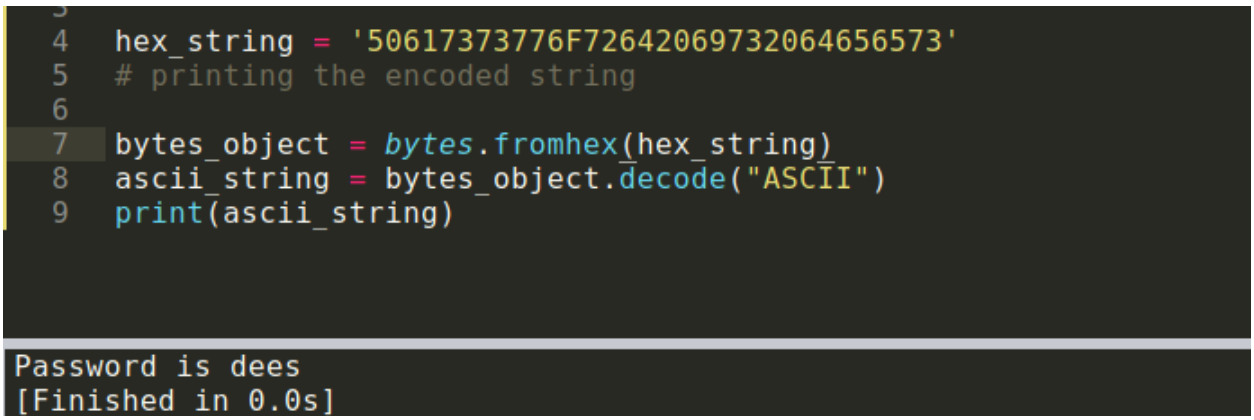


Kiểm tra lại



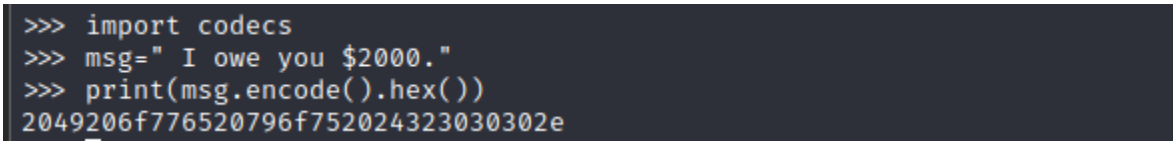
Task 3: <source code>





Task 4: <source code>

Chuyển msg sang dạng hex



Tạo chữ ký

Thay đổi msg một tí

So sánh hai chữ ký

```
┌──(haha㉿haha)-[~/MMH]
└─$ gcc task4-lab3.c -lcrypto -o task4-lab3

┌──(haha㉿haha)-[~/MMH]
└─$ ./task4-lab3
signature: B717A9E38AE9013ADF3B6636A1C0B190CEE5C4532B4416B0E9DD3F8841DC5935
Message: 2049206F776520796F752024323030302E
signature: 5BFF0BC498A5DD81322AABC8C7B3B78FBB50770758F2A2007B5A964F8D451B53
Message: 2049206F776520796F752024333030302E
```

Thì thấy tuy phần message thay đổi một ít nhưng chữ ký thay đổi hoàn toàn.

Task 5: <source code>

Chuyển msg sang dạng hex

```
>>> msg="Launch a missile."
>>> print(msg.encode().hex())
4c61756e63682061206d697373696c652e
```

Giải mã chữ ký và msg bằng public key

```
┌──(haha㉿haha)-[~/MMH]
└─$ gcc task5-lab3.c -lcrypto -o task5-lab3

┌──(haha㉿haha)-[~/MMH]
└─$ ./task5-lab3
sau khi giai ma: 4C61756E63682061206D697373696C652E
Valid Signature!
```

Thay đổi S một chút thì nhận thấy rằng không giống với chuỗi nhận được

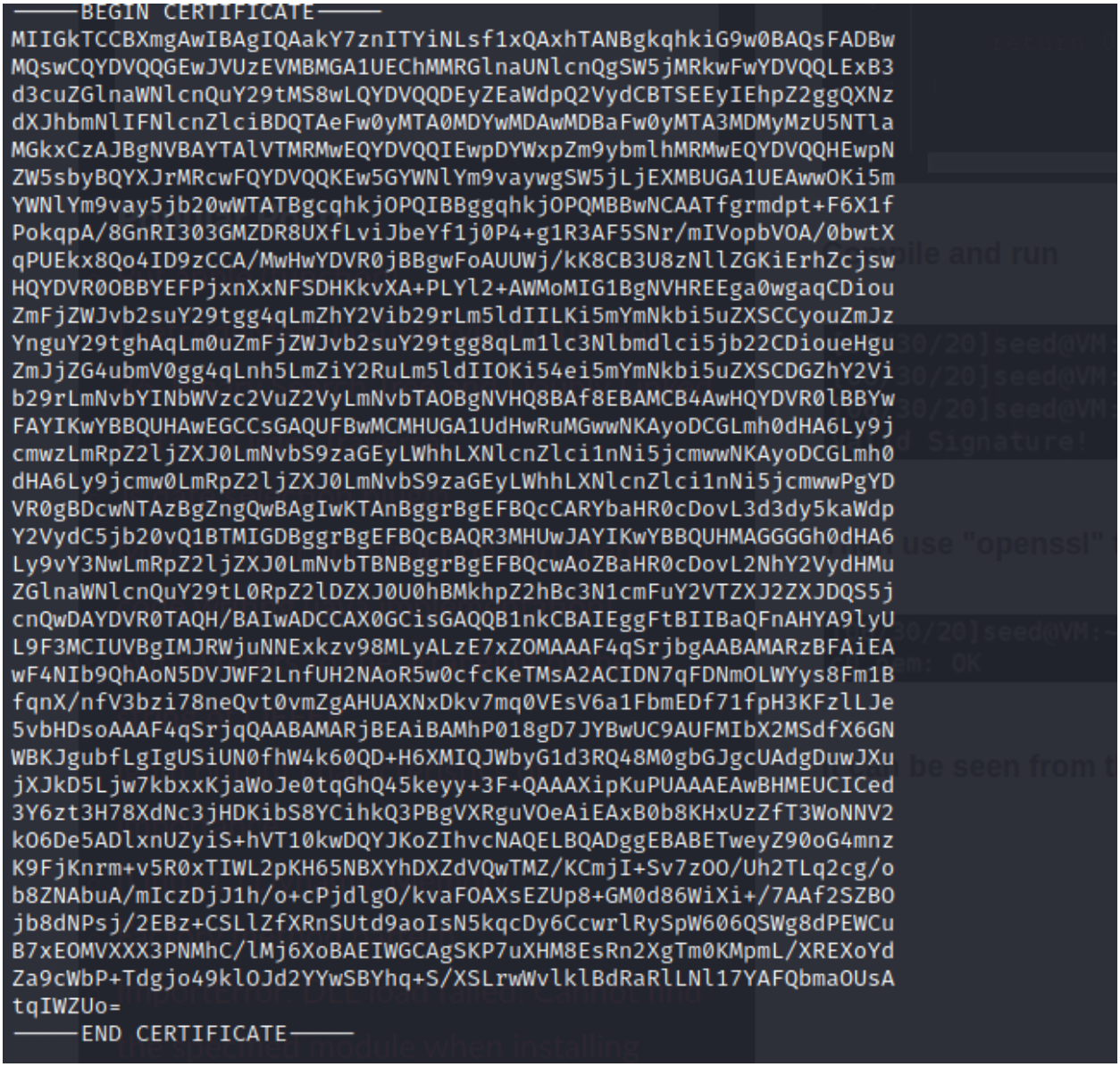
```
┌──(haha㉿haha)-[~/MMH]
└─$ ./task5-lab3
sau khi giai ma: 91471927C80DF1E42C154FB4638CE8BC726D3D66C83A4EB6B7BE0203B41AC294
Verification fails!
```

Task 6: <source code>

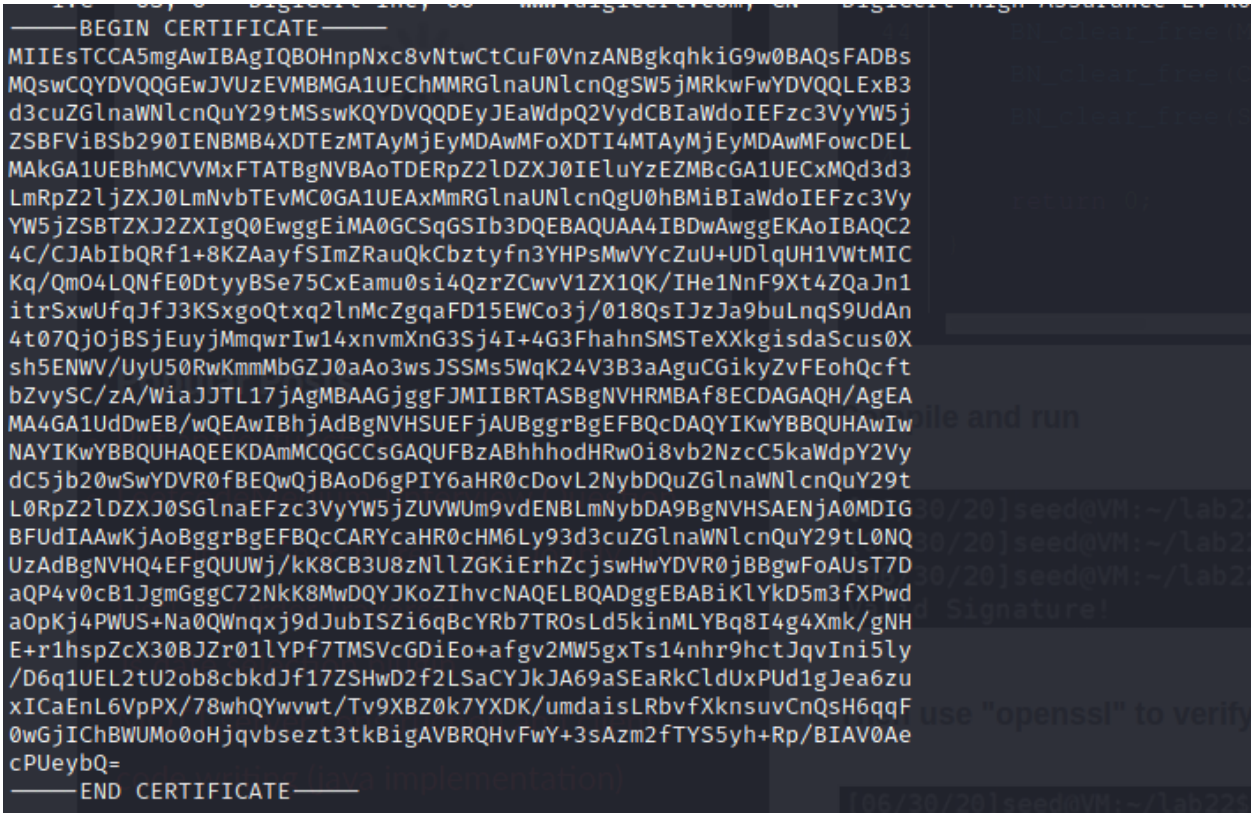
Dùng câu lệnh đã cho tải certificate về task6.txt.

```
┌──(haha㉿haha)-[~/MMH]
└─$ openssl s_client -connect www.facebook.com:443 -showcerts
CONNECTED(00000003)
```

Lưu chứng chỉ này vào c0.pem



Lưu chứng chỉ này vào c1.pem



Sau đó tìm n và e trong c1.pem

Sau đó tìm signatrue trong c0.pem

Lưu đoạn signature vào signature0

```
        28:92:FA:15:53:D7:49
    Signature Algorithm: sha256WithRSAEncryption
         11:13:c1:ec:99:f7:4a:06:e2:69:f3:2b:d1:63:2a:7a:e6:fa:
         fe:51:d3:14:c8:58:bd:a9:28:7e:b9:34:15:d8:84:35:d9:75:
         54:30:4c:c6:7f:28:29:a3:23:e4:af:ef:33:8e:fd:48:76:4c:
         ba:b6:72:0f:e8:6f:c6:4d:01:bb:80:fe:62:1c:cc:38:c9:d6:
         1f:e8:f9:c3:e3:76:58:0e:fe:4b:da:14:e0:17:b0:46:54:a7:
         cf:86:33:47:7c:e9:68:97:8b:ef:fb:00:07:f6:49:90:4e:8d:
         bf:1d:34:fb:23:ff:61:01:cf:e0:92:2e:56:5f:5d:19:d2:52:
         d7:7d:6a:82:2c:37:99:2a:70:3c:ba:09:cc:2b:95:1c:92:a5:
         6e:b4:e9:04:96:83:c7:4f:11:60:ae:07:bc:44:38:c5:57:5d:
         7d:cf:34:c8:42:fe:53:23:e9:7a:01:00:42:16:18:20:20:48:
         a3:fb:b9:71:cc:f0:4b:11:9f:65:e0:4e:6d:0a:32:99:8b:fd:
         74:44:5e:86:1d:65:af:5c:59:b3:fe:4d:d8:23:a3:8f:64:94:
         e2:5d:d9:86:30:48:16:21:ab:e4:bf:5d:22:eb:c1:6b:e5:92:
         50:5d:45:a4:65:2c:d9:75:ed:80:05:41:b9:9a:39:4b:00:b6:
         a2:16:65:4a
```

Tìm đoạn hash

```
┌──(haha㉿haha)-[~/MMH]
└─$ openssl asn1parse -i -in c0.pem -strparse 4 -out c0_body.bin -noout        1 ⚙

┌──(haha㉿haha)-[~/MMH]
└─$ sha256sum c0_body.bin                                                      1 ⚙
5e0b13fcd057cff040c202642733523978b8103bc8b41be72cf68f88aa76e93d  c0_body.bin
```

Kiểm tra thử

```
e=65537
module=   0xB6E02FC22406C86D045FD7EF0A6406B27D22266516AE42409BCEDC9F9F76073EC330558719B94F940E5A941F5556B4C2022/
signature=0x1113c1ec99f74a06e269f32bd1632a7ae6fafe51d314c858bda9287eb93415d88435d97554304cc67f2829a323e4afef338
print(hex(pow(signature,e,module)))
# hash="5e0b13fcd057cff040c202642733523978b8103bc8b41be72cf68f88aa76e93d"
```

```
0x1fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffff003031300d0609608648016503040201050004205e0b13fcd057cff040c202642733523978b8103bc8b41be72cf68f88a
a76e93d
```

```
┌──(haha㉿haha)-[~/MMH]
└─$ openssl verify -untrusted c1.pem c0.pem
c0.pem: OK
```