



## LAB 3.2

Course name: **Cryptography** - Class code: **NT219.L21.ANTT.1**

Lecturer: **Van Thien Luan**

Team's info and task allocation ( <i>actual workload per each member</i> )	<b>Team member 1</b> 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  <b>Team member 2</b> 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

```
(haha@haha)~[~/MMH]
$ gcc task1-lab3.c -lcrypto -o task1-lab3
^[[A
(haha@haha)~[~/MMH]
$ ./task1-lab3
public key: (E103ABD94892E3E74AFD724BF28E78366D9676BCCC70118BD0AA1968DBB143D1,0D88C3)
private key (3587A24598E5F2A21DB007D89D18CC50ABA5075BA19A33890FE7C28A9B496AEB,E103ABD94892E3E74AFD724BF28E78366D9676BCCC70118BD0AA1968DBB143D1)
```

Task 2: <source code>

```
(haha@haha)~[~/MMH]
$ gcc task2-lab3.c -lcrypto -o task2-lab3
(haha@haha)~[~/MMH]
$ ./task2-lab3
cipher: 6FB078DA550B2650832661E14F4F8D2CFAEF475A0DF3A75CACDC5DE5CFC5FADC
```

Kiểm tra lại

```
(haha@haha)~[~/MMH]
$ ./task2-lab3
cipher: 6FB078DA550B2650832661E14F4F8D2CFAEF475A0DF3A75CACDC5DE5CFC5FADC
Message: 4120746F702073656372657421
```

Task 3: <source code>



```
(haha@haha)~[~/MMH]
$ gcc task3-lab3.c -lcrypto -o task3-lab3

(haha@haha)~[~/MMH]
$ ./task3-lab3
Message: 50617373776F72642069732064656573
```

```
3
4 hex_string = '50617373776F72642069732064656573'
5 # printing the encoded string
6
7 bytes_object = bytes.fromhex(hex_string)
8 ascii_string = bytes_object.decode("ASCII")
9 print(ascii_string)
```

```
Password is dees
[Finished in 0.0s]
```

Task 4: <source code>

Chuyển msg sang dạng hex

```
>>> import codecs
>>> msg=" I owe you $2000."
>>> print(msg.encode().hex())
2049206f776520796f752024323030302e
```

Tạo chữ ký

```
(haha@haha)~[~/MMH]
$ gcc task4-lab3.c -lcrypto -o task4-lab3
(haha@haha)~[~/MMH]
$ ./task4-lab3
signature: B717A9E38AE9013ADF3B6636A1C0B190CEE5C4532B4416B0E9DD3F8841DC5935
Message: 2049206f776520796f752024323030302e
```

Thay đổi msg một tí

```
>>> msg=" I owe you $3000."
>>> print(msg.encode().hex())
2049206f776520796f752024333030302e
```

So sánh hai chữ ký



```
(haha@haha)-[~/MMH]
$ gcc task4-lab3.c -lcrypto -o task4-lab3
$ ./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())
4c61756e63682061206d697373696e6352e
```

Giải mã chữ ký và msg bằng public key

```
(haha@haha)-[~/MMH]
$ gcc task5-lab3.c -lcrypto -o task5-lab3
$ ./task5-lab3
sau khi giai ma: 4C61756E63682061206D697373696C652E
Valid Signature!
>>> print(msg.encode().hex())
```

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



```
-----BEGIN CERTIFICATE-----
MIIGkTCCBxmGAWIBAgIQAAkY7znITYiNLSf1xQAxhTANBgkqhkiG9w0BAQsFADBw
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLEwB3
d3cuZGlnaWlnalcnQuY29tMS8wLQYDVQQDEyZEaWdpQ2VydCBTSEEyIEhpZ2ggQXNz
dXJhbmNlIFNlcnZlcjBDQTAeFw0yMTA0MDYwMDAwMDBaFw0yMTA3MDMyMzU5NTla
MGkxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwplDYWxpZm9ybmlhMRMwEQYDVQQHEwplN
ZW5sbyBQYXJrMRcwFQYDVQQKEw5GYWNlYm9vaywSW5jLjEXMBUGA1UEAwOKi5m
YWNlYm9vay5jb20wWTATBgqhkiOPQIBBgqhkiOPQMBBwNCAATfgrmdpt+F6X1f
PokqpA/8GnRI303GMZDR8UXfLviJbeYf1j0P4+g1R3AF5SNr/mIVopbVOA/0bwtX
qPUEKx8Qo4ID9zCCA/MwHwYDVR0jBBgwFoAUUWj/kK8CB3U8zNllZGKiErhZcjsW
HQYDVR00BBYEFpJxnXNFSDHKkvXA+PLYl2+AWMoMIG1BgNVHREEga0wgaqCDiou
ZmFjZWJvb2suY29tgg4qLmZhY2Vib29rLm5ldIILKi5mYmNkbi5uZXSCCyouZmJz
YnguY29tghAqLm0uZmFjZWJvb2suY29tgg4qLm1lc3Nlbmdlci5jb22CDiouEHgu
ZmJjZG4ubmV0gg4qLnh5LmZiY2RuLm5ldIIOKi54ei5mYmNkbi5uZXSCDGZhY2Vi
b29rLmNvbYINbWVzc2VuZ2VyLmNvbTAOBgNVHQ8BAf8EBAMCB4AwHQYDVR0lBBYw
FAYIKwYBBQUHAwEGCCsGAQUFBwMCMHUGA1UdHwRUMGwwNKAyoDCGLmh0dHA6Ly9j
cmwzLmRpZ2ljZXJ0LmNvbS9zaGEyLWhhLXNlcnZlc1N15jcmwwNKAyoDCGLmh0
dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9zaGEyLWhhLXNlcnZlc1N15jcmwwPgYD
VR0gBDcwNTAzBgZngQwBAgIwKTAnBggrBgEFBQcCARYbaHR0cDovL3d3dy5kaWdp
Y2VydC5jb20vQ1BTMIGDBggrBgEFBQcCBAQR3MHUwJAYIKwYBBQUHMAGGGGh0dHA6
Ly9vY3NwLmRpZ2ljZXJ0LmNvbTBnBggrBgEFBQcwAoZBaHR0cDovL2NhY2VydHMu
ZGlnaWlnalcnQuY29tL0RpZ2lDZXJ0U0hBMkhpZ2hBc3N1cmFuY2VtZXJ2ZXJ0S5j
cnQwDAYDVR0TAAQH/BAIwADCCAX0GCisGAQQB1nkCBAIEggFtBIIBaQFnAHYA9lyU
L9F3MCIUVBgIMJRWjuNNEExkzv98MLyALzE7xZOMAAAF4qSrjbgAABAMARzBFAiEA
wF4NIb9QhAoN5DVJWF2LnFUH2NAoR5w0cfcKeTMsA2ACIDN7qFDNmOLWYys8Fm1B
fqNX/nfV3bzi78neQvt0vmZgAHUAXNxDkv7mq0VEsV6a1FbmEDf71fpH3KFzLLJe
5vbHDsoAAAF4qSrjgQAABAMARjBEAiBAMhP018gD7JYBwUC9AUFMIbX2MSdfX6GN
WBKJgubfLgIgUSiUN0fhW4k60QD+H6XMIQJWbyG1d3RQ48M0gbGJgcUAdgDuwJXu
jXJkD5Ljw7kbxxKjaWoJe0tqGhQ45keyy+3F+QAAAXipKuPUAAAEAwBHMEUCIced
3Y6zt3H78XdNc3jHDKibS8YCIhkQ3PBgVXRguVoeAiEAXB0b8KHxUzZft3WoNNV2
kO6De5ADlxnUZyis+hVT10kwDQYJKoZIhvcNAQELBQADggEBABETweyZ90oG4mnz
K9FjKnrm+v5R0xTIWL2pKH65NBXYhDXZdVQwTMZ/KCmjI+Sv7z00/Uh2TLq2cg/o
b8ZNAbuA/mIczDjJ1h/o+cPjdlG0/kvaFOAXsEZUp8+GM0d86WiXi+/7AAf2SZBO
jb8dNPsj/2EBz+CSLLZfXRnSutd9aoIsN5kqcDy6CcwrlRySpW606QSWg8dPEWCu
B7xEOMVXXX3PNMhC/lmj6XoBAEIWGCAGSKP7uXHM8EsRn2XgTm0KMpML/XREXoYd
Za9cWbP+Tdgjo49kl0Jd2YyWSBYhq+S/XSLrwWvlklBdRaRLNL17YAFQbmaOUsa
tqIWZUo=
-----END CERTIFICATE-----
```

Lưu chứng chỉ này vào c1.pem



```
-----BEGIN CERTIFICATE-----
MIIEsTCCA5mgAwIBAgIQB0HnpNxc8vNtwCtCuF0VnzANBgkqhkiG9w0BAQsFADBs
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSswKQYDVQQDEyJEaWdpQ2VydCBiawdoIEFzc3VyYW5j
ZSBFViBSb290IENBMb4XDTEzMAYmJyMDAwMmFoXDTI4MTAyMjE5MDAwMmFowcDEL
MAkGA1UEBhMCVVMxFTATBgNVBAoTDERpZ2ZlZDZlZDZlZDZlZDZlZDZlZDZlZDZl
LmRpZ2ZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZl
YW5jZSBTZXJ2ZXIgc0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC2
4C/CJAbIbQRf1+8KZAayfSimZRauQkCbztyfn3YHPsMwVYcZuU+UDlqUH1VWtMIC
Kq/Qm04LQNF0DtyyBSe75CxEamu0si4QzrZCwvV1ZX1QK/IHe1NnF9Xt4ZQaJn1
itrSxwUfQJfJ3KSxgoQtqx2lnMcZgqaFD15EWCo3j/018QsIJzJa9buLnqS9UdAn
4t07Qj0jBSjEuyjMmqwrIw14xnmvXnG3Sj4I+4G3FhahnSMStEXXkgisdaScus0X
sh5ENWV/UyU50RwKmmMbGZJ0aAo3wsJSSMs5WqK24V3B3aAguCGikyZvFEohQcft
bZvySC/zA/WiaJJTL17jAgMBAAGjggFJMIIBRTASBgNVHRMBAf8ECDAGAQH/AgEA
MA4GA1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAWIw
NAYIKwYBBQUHAQEEDAMcQGCGCsGAQUFBzABhhhodHRw0i8vb2NzcC5kaWdpY2Vy
dC5jb20wSwYDVDR0fBEQwQjBAoD6gPIY6aHR0cDovL2NybdDQUGlnaWNlcnQuY29t
L0RpZ2ZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZl
BFUdIAAwKjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cuZGlnaWNlcnQuY29tL0NQ
UzAdBgNVHQ4EFgQUUWj/kK8CB3U8zNLLZGKiErhZcjsWwYDVR0jBBgwFoAUsT7D
aQP4v0cB1JgmGggC72NkK8MwDQYJKoZIhvcNAQELBQADggEBABiKlYkd5m3fXPwd
aOpKj4PWUS+Na0QWnqxj9dJubISZi6qBcYRb7TROsLd5kinMLYBq8I4g4Xmk/gNH
E+r1hspZcX30BJZr01LYPf7TMSVcGDIEo+afgv2MW5gxTs14nhr9hctJqvInisly
/D6q1UEL2tU2ob8cbkdJf17ZSHwD2f2LSaCYJkJA69aSEaRkClDUXpUD1gJea6zu
xICaEnL6VpPX/78whQYwvwt/Tv9XBZ0k7YXDK/umdaSLRbvfxKnsuvCnQsH6qqf
0wGjIChBWUMo0oHjqvbsezt3tkBigAVBRQHvFwY+3sAzM2fTYS5yh+Rp/BIAV0Ae
cPUeybQ=
-----END CERTIFICATE-----
```

Sau đó tìm n và e trong c1.pem

```
(haha@haha)-[~/MMH]
$ openssl x509 -in c1.pem -noout -modulus
Modulus=B6E02FC22406C86D045FD7EF0A6406B27D22266516AE42409BCEDC9F9F76073EC330558719B94F940E5A941F5556B4
C2022AAFD098EE0B40D7C4D03B72C8149EEF90B111A9AED2C8B8433AD90B0BD5D595F540AFC81DED4D9C5F57B786506899F58A
DAD2C7051FA897C9DCA4B182842DC6ADA59CC71982A6850F5E44582A378FFD35F10B0827325AF5B88B9EA4BD51D027E2D03B42
33A30528C4BB28CC9AAC2B230D78C67BE65E71B74A3E08F8B1B71616A19D23124DE5D79208AC75A49CBACD17B21E4435657F53
2539D11C0A9A631B199274680A37C2C25248CB395AA2B6E15DC1DDA020B821A293266F144A2141C7ED6D9BF2482FF303F5A268
92532F5EE3

(haha@haha)-[~/MMH]
$ openssl x509 -in c1.pem -text -noout | grep Exponent
Exponent: 65537 (0x10001)
```

Sau đó tìm signature trong c0.pem

```
(haha@haha)-[~/MMH]
$ openssl x509 -in c0.pem -text -noout
Certificate:
```

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
(haha@haha)-[~/MMH]
$ sha256sum c0_body.bin
5e0b13fcd057cff040c202642733523978b8103bc8b41be72cf68f88aa76e93d  c0_body.bin
```

Kiểm tra thử

```
7 e=65537
8 module= 0xB6E02FC22406C86D045FD7EF0A6406B27D22266516AE42409BCEDC9F9F76073EC330558719B94F940E5A941F5556B4C2022/
9 signature=0x1113c1ec99f74a06e269f32bd1632a7ae6afe51d314c858bda9287eb93415d88435d97554304cc67f2829a323e4afef338e
10 print(hex(pow(signature,e,module)))
11 # hash="5e0b13fcd057cff040c202642733523978b8103bc8b41be72cf68f88aa76e93d"
12
13

0x1ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffff003031300d0609608648016503040201050004205e0b13fcd057cff040c202642733523978b8103bc8b41be72cf68f88a
a76e93d

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