3.1 Task 1: Deriving the Private Key

P = F7E75FDC469067FFDC4E847C51F452DF =
329520679814142392965336341297134588639

Q = E85CED54AF57E53E092113E62F436F4F =
308863399973593539130925275387286220623

E = 0D88C3 = 886979

Private Key =
3587A24598E5F2A21DB007D89D18CC50ABA5075BA19A33890FE7C28A9B496AEB

=
24212225287904763939160097464943268930139828978795606022583874367720623008491

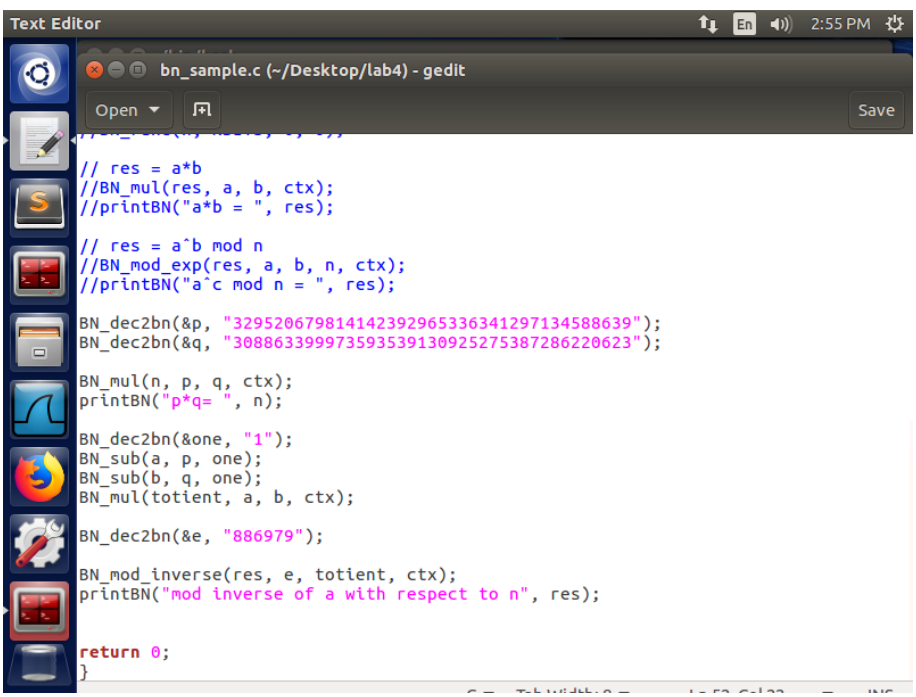
In the program I plugged in p, q, and e using BN_hex2bn. Then I calculated n using BN_mul(n, p, q, ctx); Next I calculated the totient using (p-1)(q-1). BN_dec2bn(&one, "1");

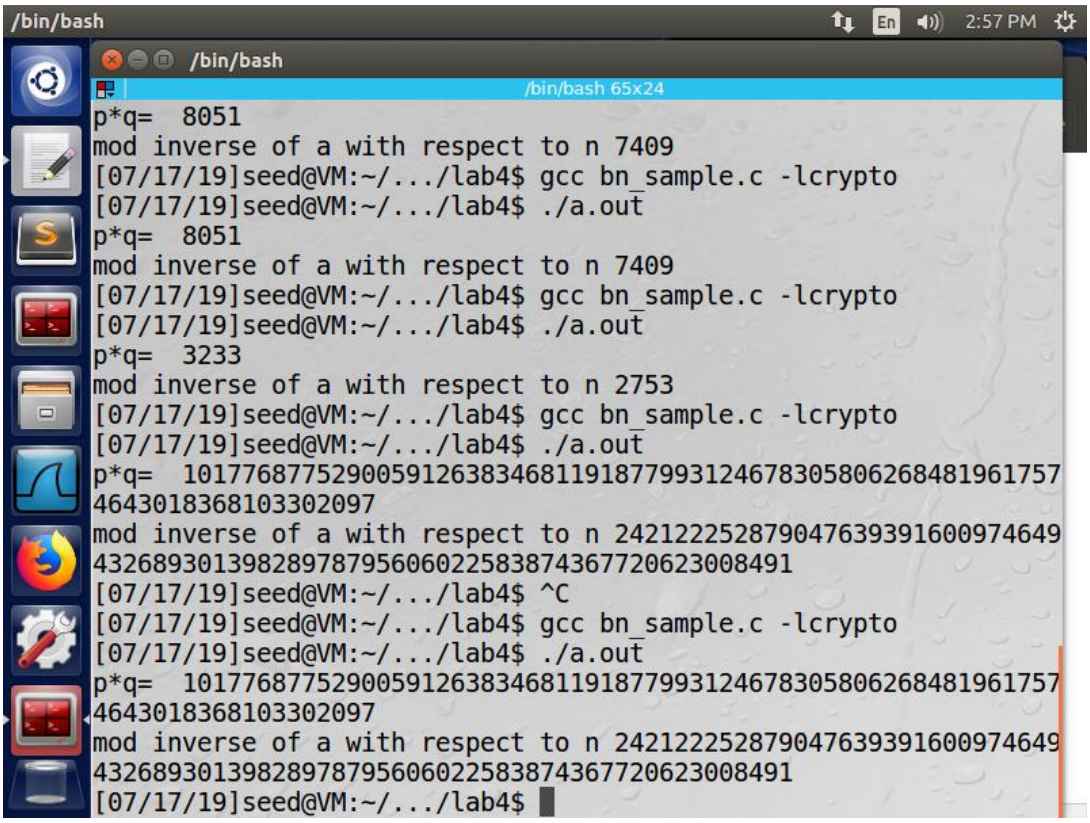
BN_sub(a, p, one);

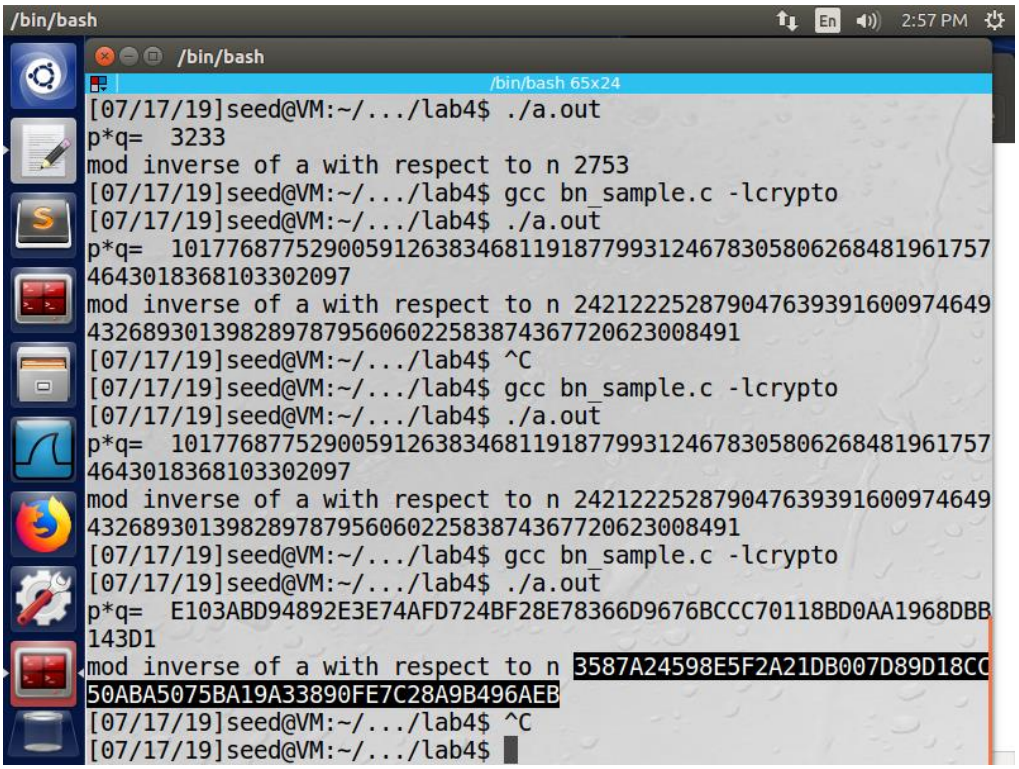
BN_sub(b, q, one);

BN_mul(totient, a, b, ctx);

Finally I calculated d using the mod inverse, BN_mod_inverse(res, e, totient, ctx);

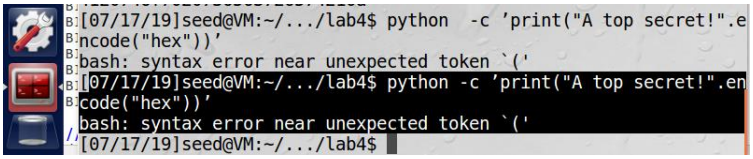






Both output the private key. One in decimal, one in hexadecimal.

3.2 Task 2:

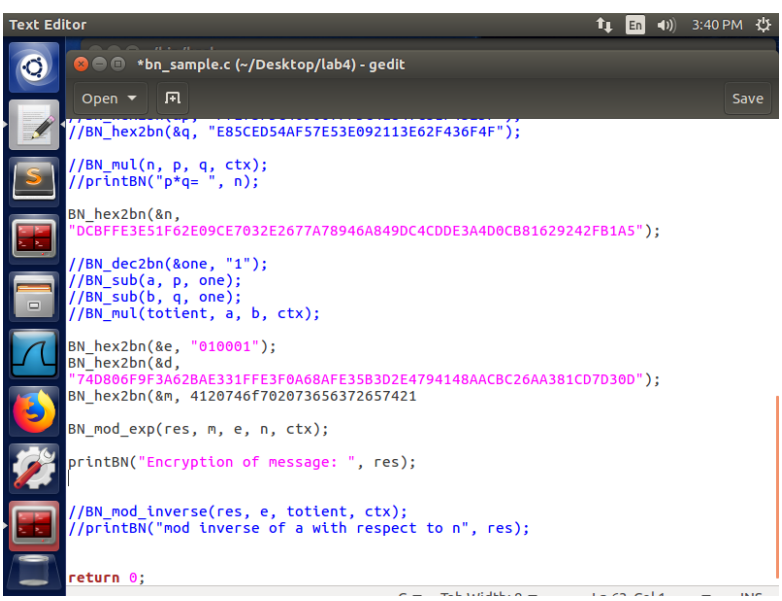


The method of using python in the command line to find the hex value of an ASCII string outlined in the PDF lab manual doesn't work. From google, it appears that method depreciated when python 2 updated to python 3. I used an ASCII text to hex converter.

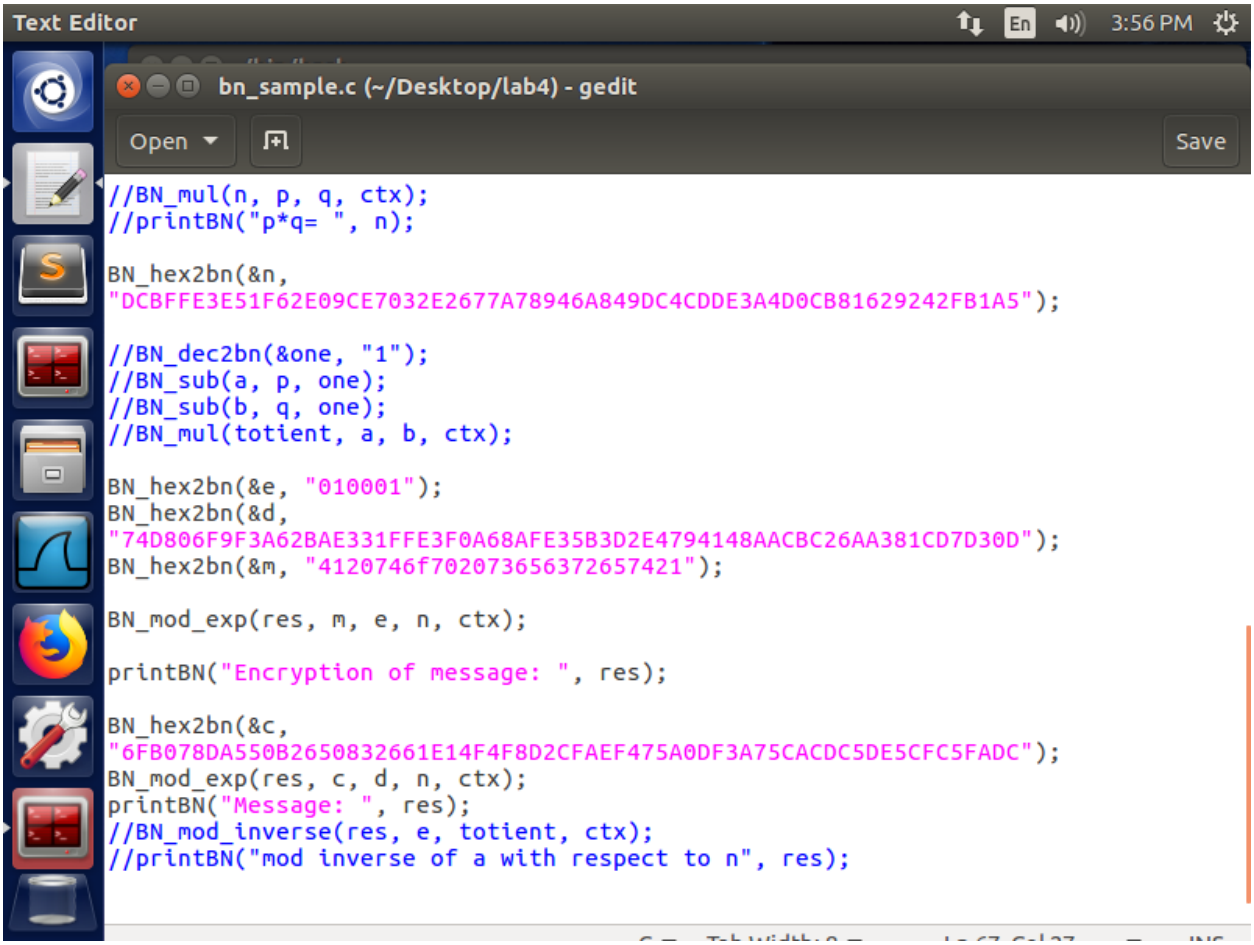
I used BN_hex2bn to plug in values for n, e, and message (hex value).

Cipher text = M^e mod n. Then BN_mod_exp(res, m, e, n, ctx); was used to get encrypted message.

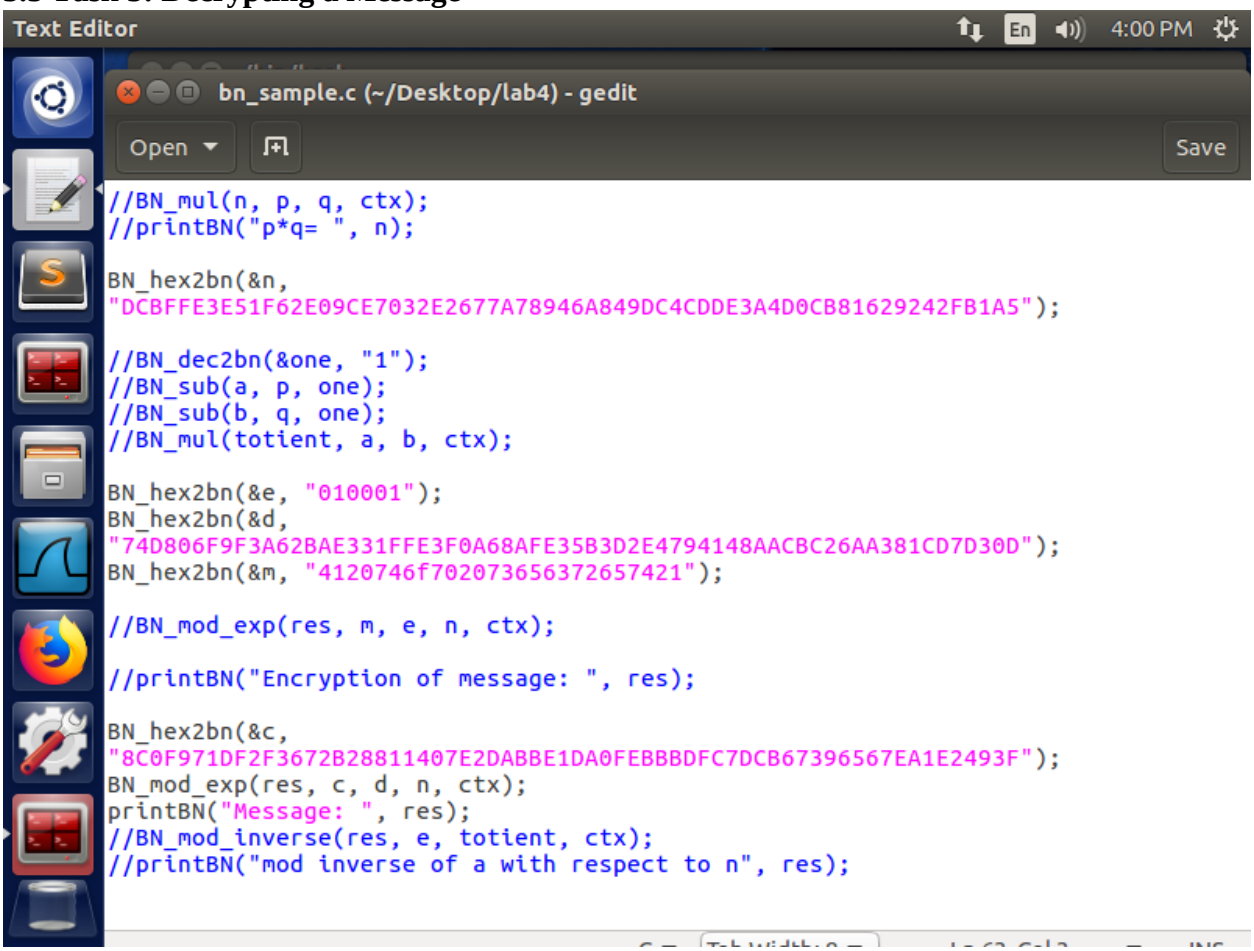
Encryption of message:
6FB078DA550B2650832661E14F4F8D2CFAEF475A0DF3A75CACDC5DE5CFC5FADC



I also used the private key provided to check results.



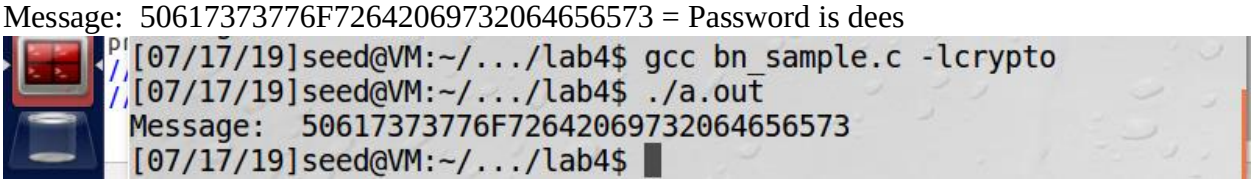
3.3 Task 3: Decrypting a Message




```
//BN_mul(n, p, q, ctx);
//printBN("p*q= ", n);

BN_hex2bn(&n,
"DCBFFE3E51F62E09CE7032E2677A78946A849DC4CDDE3A4D0CB81629242FB1A5");

//BN_dec2bn(&one, "1");
//BN_sub(a, p, one);
//BN_sub(b, q, one);
//BN_mul(totient, a, b, ctx);

BN_hex2bn(&e, "010001");
BN_hex2bn(&d,
"74D806F9F3A62BAE331FFE3F0A68AFE35B3D2E4794148AACBC26AA381CD7D30D");
BN_hex2bn(&m, "4120746f702073656372657421");

//BN_mod_exp(res, m, e, n, ctx);

//printBN("Encryption of message: ", res);

BN_hex2bn(&c,
"8C0F971DF2F3672B28811407E2DABBE1DA0FEBBBDFC7DCB67396567EA1E2493F");
BN_mod_exp(res, c, d, n, ctx);
printBN("Message: ", res);
//BN_mod_inverse(res, e, totient, ctx);
//printBN("mod inverse of a with respect to n", res);
```

Using the same values for n, d, and e from task 2, I decrypted the cipher text C to get message m.

Message: 50617373776F72642069732064656573 = Password is dees

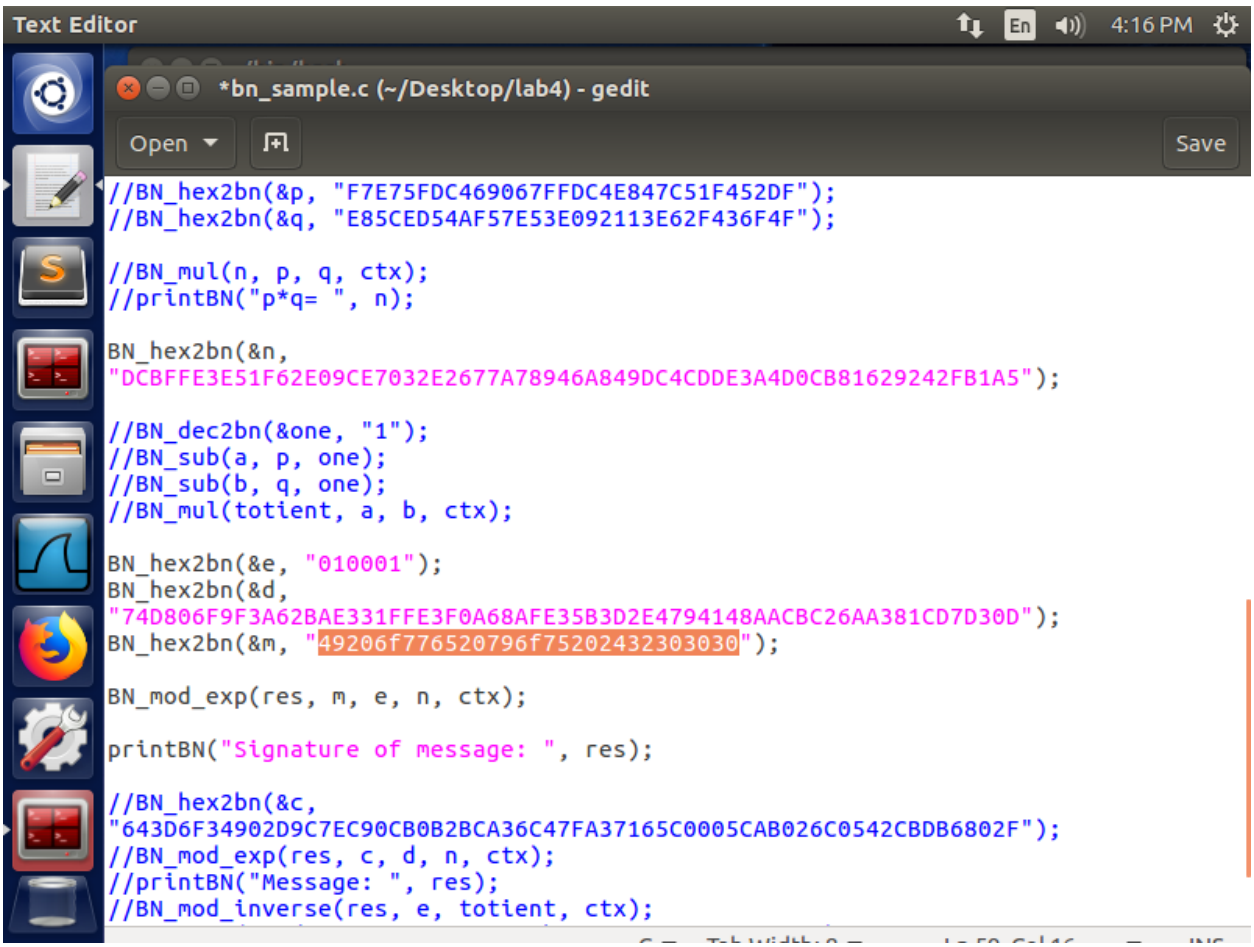


```
[07/17/19]seed@VM:~/.../lab4$ gcc bn_sample.c -lcrypto
[07/17/19]seed@VM:~/.../lab4$ ./a.out
Message:  50617373776F72642069732064656573
[07/17/19]seed@VM:~/.../lab4$
```

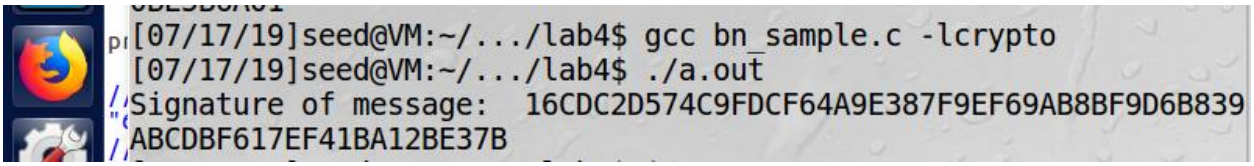
3.4 Task 4: Signing a Message

Using the same values for n, d, and e from task 2 and 3.

M = I owe you $2000 = 49206f776520796f75202432303030



S = 16CDC2D574C9FDCF64A9E387F9EF69AB8BF9D6B839ABCDBF617EF41BA12BE37B



M = I owe you $3000 = 49206f776520796f75202433303030

S = 686126E57A64A817BF54D768ABD615B33ECE1C4D7C8160D3E6645250F3B1C98E

```
[07/17/19]seed@VM:~/.../lab4$ gcc bn_sample.c -lcrypto
[07/17/19]seed@VM:~/.../lab4$ ./a.out
Signature of message:  686126E57A64A817BF54D768ABD615B33ECE1C4D7C
8160D3E6645250F3B1C98E
```

The signatures are very different. Even different in length.

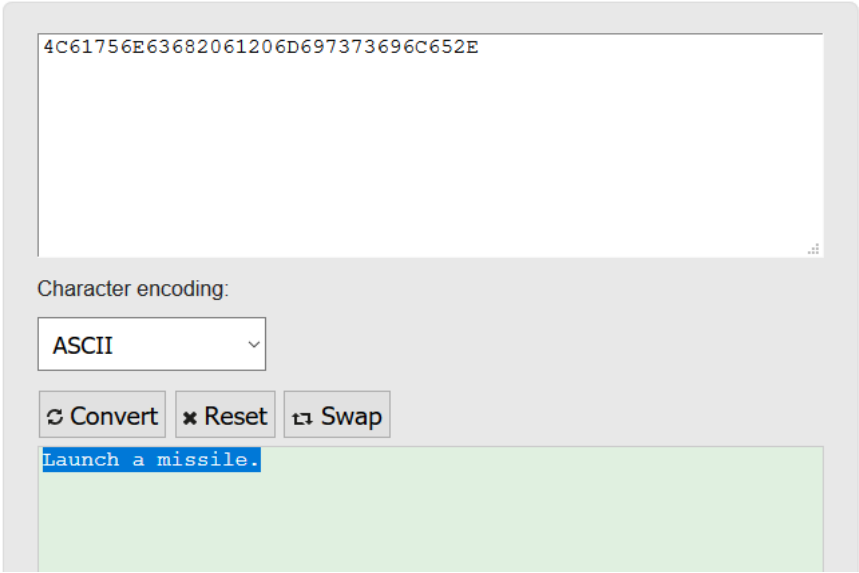
3.5 Task 5: Verifying a Signature

We know Alice's public key is (e, n), the message, and the signature which are given in the lab manual. If the signature was generated using Alice's private key then we should be able to decrypt using Alice's public key, thus verifying Alice is the sender. Using BN_mod_exp(res, s, e, n, ctx); where s is the signature, and (e, n) are Alice's public key we get the message (in hexadecimal)

```
BN_hex2bn(&n,
"AE1CD4DC432798D933779FBD46C6E1247F0CF1233595113AA51B450F18116115");

//BN_dec2bn(&one, "1");
//BN_sub(a, p, one);
//BN_sub(b, q, one);
//BN_mul(totient, a, b, ctx);

BN_hex2bn(&e, "010001");
BN_hex2bn(&d,
"74D806F9F3A62BAE331FFE3F0A68AFE35B3D2E4794148AACBC26AA381CD7D30D");
//BN_hex2bn(&m, "49206f776520796f75202432303030");

//BN_mod_exp(res, m, e, n, ctx);

//printBN("Signature of message: ", res);

BN_hex2bn(&c,
"643D6F34902D9C7EC90CB0B2BCA36C47FA37165C0005CAB026C0542CBDB6802F");
BN_mod_exp(res, c, e, n, ctx);
printBN("Message: ", res);

//BN_mod_inverse(res, e, totient, ctx);
//printBN("mod inverse of a with respect to n", res);


return 0;
}
```

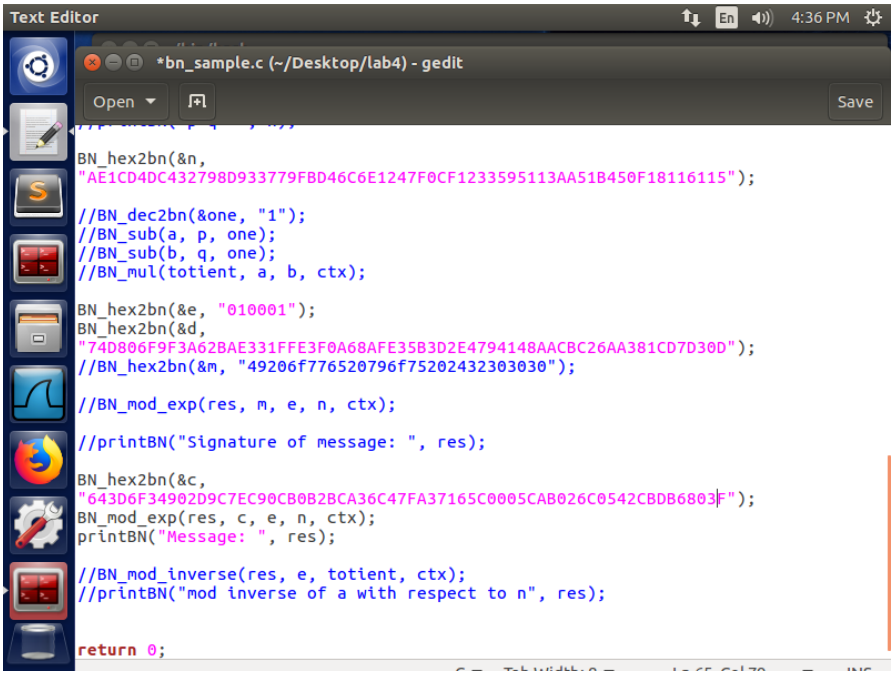
Message: 4C61756E63682061206D697373696C652E = Launch a missile.

```
[07/17/19]seed@VM:~/.../lab4$ gcc bn_sample.c -lcrypto
[07/17/19]seed@VM:~/.../lab4$ ./a.out
Message:  4C61756E63682061206D697373696C652E
[07/17/19]seed@VM:~/.../lab4$
```



Therefore signed by Alice’s private key.

The signature was corrupted by one bit, resulting in 2f to become 3f. Performing the same operation, we get the message.



Message:
91471927C80DF1E42C154FB4638CE8BC726D3D66C83A4EB6B7BE0203B41AC294

= ‘ G'È

ñä,O´cŒè¼rm=fÈ:N¶·¾————————————————´Â”

The corrupted signature resulted in Alice not being verified as the sender. We can conclude the message was corrupted, or Alice was not the sender of this message.

3.6 Task 6: Manually Verifying an X.509 Certificate

Step 1: I used www.utdallas.edu

[07/17/19]seed@VM:~/.../lab4$ openssl s_client -connect www.utdallas.edu:443 -showcerts

CONNECTED(00000003)

depth=3 C = SE, O = AddTrust AB, OU = AddTrust External TTP Network, CN = AddTrust External CA Root

verify return:1

depth=2 C = US, ST = New Jersey, L = Jersey City, O = The USERTRUST Network, CN = USERTrust RSA Certification Authority

verify return:1

depth=1 C = US, ST = MI, L = Ann Arbor, O = Internet2, OU = InCommon, CN = InCommon RSA Server CA

verify return:1

depth=0 C = US, postalCode = 75080, ST = TX, L = Richardson, street = 800 West Campbell Road, O = The University of Texas at Dallas, OU = General, CN = www.utdallas.edu

verify return:1

Certificate chain

0 s:/C=US/postalCode=75080/ST=TX/L=Richardson/street=800 West Campbell Road/O=The University of Texas at Dallas/OU=General/CN=www.utdallas.edu

i:/C=US/ST=MI/L=Ann Arbor/O=Internet2/OU=InCommon/CN=InCommon RSA Server CA

-----BEGIN CERTIFICATE-----

MIIFpDCCBIygAwIBAgIQZqaSOKoqvWJ/7OD/DDhKdzANBgkqhkiG9w0BAQsFADB2

MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUkxEjAQBgNVBAcTCUFubiBBcmJvcjES

MBAGA1UEChMJSW50ZXJuZXQyMREwDwYDVQQLEwhJbkNvbW1vbjEfMB0GA1UEAxMW

SW5Db21tb24gUlNBIFNlcnZlciBDQTAeFw0xODAzMDUwMDAwMDBaFw0yMDAzMDQy

MzU5NTlaMIG5MQswCQYDVQQGEwJVUzEOMAwGA1UEERMFNzUwODAxCzAJBgNV
BAgT

AlRYMRMwEQYDVQQHEwpSaWNoYXJkc29uMR8wHQYDVQQJExY4MDAgV2VzdCBD
YW1w

YmVsbCBSb2FkMSowKAYDVQQKEyFUaGUgVW5pdmVyc2l0eSBvZiBUZXhhcyBhdCBE

YWxsYXMxEDAOBgNVBAsTB0dlbmVyYWwxGTAXBgNVBAMTEHd3dy51dGRhbGxhcy
5l

ZHUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCiybDR9oz0lIMbZ871

uaKPw7y6ux4zJVyEXNK1lS6GJ1leBJ1zeX9hL7z9OJbFQ3v0kFHfdlbu8dRb2W7v

ODOlO4qiABKpWEbYINRNjO5KCS0gIGs1YVi9TXl8Y0sI89baIkIRqJuofxduV0h0

1ay2xs+hQCb4M7VwHDQPUVZNUsCPc50J/16PPwtzzkZHvel+OD7GiCcejiAeiTlu

HgP8civeINNrtAImoMhg1H4bDSHCMfIaPRf6ytZDfzvSnB1Phvj5vfARBHStJk/7

O/hjkKl1Zcv8X2iR2iHsB36SqwC9D1tPonLdqsvvttlMUe0XoFVJUAp7/l7wz4TK

gqYJAgMBAAGjggHoMIIB5DAfBgNVHSMEGDAWgBQeBaN3j2yW4luHS6a0hqxxAAzn

ODAdBgNVHQ4EFgQUaywqKOdSTD2knrccq5cKltgk0dQwDgYDVR0PAQH/BAQDAgWg

MAwGA1UdEwEB/wQCMAAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBw
MCMGcG

A1UdIARgMF4wUgYMKwYBBAGuIwEEAwEBMEIwQAYIKwYBBQUHAgEWNGh0dHBz
Oi8v

d3d3LmluY29tbW9uLm9yZy9jZXJ0L3JlcG9zaXRvcnkvY3BzX3NzbC5wZGYwCAYG

Z4EMAQICMEQGA1UdHwQ9MDswOaA3oDWGM2h0dHA6Ly9jcmwuaW5jb21tb24tcnNh

Lm9yZy9JbkNvbW1vblJTQVNlcnZlckNBLmNybDB1BggrBgEFBQcBAQRpMGcwPgYI

KwYBBQUHMAKGMmh0dHA6Ly9jcnQudXNlcnRydXN0LmNvbS9JbkNvbW1vblJTQVNl

cnZlckNBXzIuY3J0MCUGCCsGAQUFBzABhhlodHRwOi8vb2NzcC51c2VydHJ1c3Qu

Y29tMD8GA1UdEQQ4MDaCEHd3dy51dGRhbGxhcy5lZHWCB3V0ZC5lZHWCDHV0ZGFs

bGFzLmVkdYILd3d3LnV0ZC5lZHUwDQYJKoZIhvcNAQELBQADggEBAGrRtMGtk0Q8

bOaKffonIZj1vOuNpWNJYDckzJL3Piz4xZgZTkGk48930nCS5u06IMdZcTIAW7hQ

07N99qZqyAfr75iUiFskGq3jARrlBWiLVg6piOKobFuTmiDdgWZRUZgkQhW1g4DE

bE4KlEN0LlPNyjajtPEVsrJCb1jgw8ssiej0X9YLdIpJhaSa5D2jCZFAKtmgpTF3

nhMB3K7VhcJRvquMI4qsahfMLrHjYuS8druYxx4QHo16tCdSY7FGXsUVfej7qJck

7yzEGiZ/6jtOetvqsuAhQ1m7z13OVBczIr85SkbYp5TpaRZllTNp42ZZkGarSTw9

oWQ5v6G1OAE=

-----END CERTIFICATE-----

1 s:/C=US/ST=MI/L=Ann Arbor/O=Internet2/OU=InCommon/CN=InCommon RSA Server CA

i:/C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust RSA Certification Authority

-----BEGIN CERTIFICATE-----

MIIF+TCCA+GgAwIBAgIQRyDQ+oVGGn4XoWQCkYRjdDANBgkqhkiG9w0BAQwFADCB

iDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCk5ldyBKZXJzZXkxFDASBgNVBAcTC0pl

cnNleSBDaXR5MR4wHAYDVQQKExVUaGUgVVNFUlRSVVNUIE5ldHdvcmsxLjAsBgNV

BAMTJVVTRVJUcnVzdCBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTQx

MDA2MDAwMDAwWhcNMjQxMDA1MjM1OTU5WjB2MQswCQYDVQQGEwJVUzELMAkGA1UE

CBMCTUkxEjAQBgNVBAcTCUFubiBBcmJvcjESMBAGA1UEChMJSW50ZXJuZXQyMREw

DwYDVQQLEwhJbkNvbW1vbjEfMB0GA1UEAxMWSW5Db21tb24gUlNBIFNlcnZlciBD

QTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJwb8bsvf2MYFVFRVA+e

xU5NEFj6MJsXKZDmMwysE1N8VJG06thum4ltuzM+j9INpun5uukNDBqeso7JcC7v

HgV9lestjaKpTbOc5/MZNrun8XzmCB5hJ0R6lvSoNNviQsil2zfVtefkQnI/tBPP

iwckRR6MkYNGuQmm/BijBgLsNI0yZpUn6uGX6Ns1oytW61fo8BBZ321wDGZq0GTl

qKOYMa0dYtX6kuOaQ80tNfvZnjNbRX3EhigsZhLI2w8ZMA0/6fDqSl5AB8f2IHpT

eIFken5FahZv9JNYyWL7KSd9oX8hzudPR9aKVuDjZvjs3YncJowZaDuNi+L7RyML

fzcCAwEAAaOCAW4wggFqMB8GA1UdIwQYMBaAFFN5v1qqK0rPVIDh2JvAnfKyA2bL

MB0GA1UdDgQWBBQeBaN3j2yW4luHS6a0hqxxAAznODAOBgNVHQ8BAf8EBAMCAYYw

EgYDVR0TAQH/BAgwBgEB/wIBADAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUH

AwIwGwYDVR0gBBQwEjAGBgRVHSAAMAgGBmeBDAECAjBQBgNVHR8ESTBHMEWgQ6BB

hj9odHRwOi8vY3JsLnVzZXJ0cnVzdC5jb20vVVNFUlRydXN0UlNBQ2VydGlmaWNh
dGlvbkF1dGhvcml0eS5jcmwwdgYIKwYBBQUHAQEEajBoMD8GCCsGAQUFBzAChjNo
dHRwOi8vY3J0LnVzZXJ0cnVzdC5jb20vVVNFUlRydXN0UlNBQWRkVHJ1c3RDQS5j
cnQwJQYIKwYBBQUHMAGGGWh0dHA6Ly9vY3NwLnVzZXJ0cnVzdC5jb20wDQYJKoZI
hvcNAQEMBQADggIBAC0RBjjW29dYaK+qOGcXjeIT16MUJNkGE+vrkS/fT2ctyNMU
11ZlUp5uH5gIjppIG8GLWZqjV5vbhvhZQPwZsHURKsISNrqOcooGTie3jVgU0W+0
+Wj8mN2knCVANt69F2YrA394gbGAdJ5fOrQmL2pIhDY0jqco74fzYefbZ/VS29fR
5jBxu4uj1P+5ZImem4Gbj1e4ZEzVBhmO55GFfBjRidj26h1oFBHZ7heDH1Bjzw72
hipu47Gkyfr2NEx3KoCGMLCj3Btx7ASn5Ji8FoU+hCazwOU1VX55mKPU1I2250Lo
RCASN18JyfsD5PVldJbtyrmz9gn/TKbRXTr80U2q5JhyvjhLf4lOJo/UzL5WCXED
Smyj4jWG3R7Z8TED9xNNCxGBMXnMete+3PvzdhssvbORDwBZByogQ9xL2LUZFI/i
eoQp0UM/L8zfP527vWjEzuDN5xwxMnhi+vCToh7J159o5ah29mP+aJnvujbXEnGa
nrNxHzu+AGOePV8hwrGGG7hOIcPDQwkuYwzN/xT29iLp/cqf9ZhEtkGcQcIImH3b
oJ8ifsCnSbu0GB9L06Yqh7lcyvKDTEADslIaeSEINxhO2Y1fmcYFX/Fqrrp1WnhH
OjplXuXE0OPa0utaKC25Aplgom88L2Z8mEWcyfoB7zKOfD759AN7JKZWCYwk

-----END CERTIFICATE-----

2 s:/C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust RSA Certification Authority

i:/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root

-----BEGIN CERTIFICATE-----

MIIFdzCCBF+gAwIBAgIQE+oocFv07O0MNmMJgGFDNjANBgkqhkiG9w0BAQwFADBv
MQswCQYDVQQGEwJTRTEUMBIGA1UEChMLQWRkVHJ1c3QgQUIxJjAkBgNVBAsTH UFk
ZFRydXN0IEV4dGVybmFsIFRUUCBOZXR3b3JrMSIwIAYDVQQDExlBZGRUcnVzdCBF
eHRlcm5hbCBDQSBSb290MB4XDTAwMDUzMDEwNDgzOFoXDTIwMDUzMDEwNDgzO Fow
gYgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpOZXcgSmVyc2V5MRQwEgYDVQQH EwtK
ZXJzZXkgQ2l0eTEeMBwGA1UEChMVVGhlIFVTRVJUUlVTVCBOZXR3b3JrMS4wLAYD

VQQDEyVVU0VSVHJ1c3QgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MIICIjAN
BgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAgBJlFzYOw9sIs9CsVw127c0n00yt
UINh4qogTQktZAnczomfzD2p7PbPwdzx07HWezcoEStH2jnGvDoZtF+mvX2do2NC
tnbyqTsrkfjib9DsFiCQCT7i6HTJGLSR1GJk23+jBvGIGGqQIjy8/hPwhxR79uQf
jtTkUcYRZ0YIUcuGFFQ/vDP+fmyc/xadGL1RjjWmp2bIcmfbIWax1Jt4A8BQOujM
8Ny8nkz+rwWWNR9XWrf/zvk9tyy29lTdyOcSOk2uTIq3XJq0tyA9yn8iNK5+O2hm
AUTnAU5GU5szYPeUvlM3kHND8zLDU+/bqv50TmnHa4xgk97Exwzf4TKuzJM7UXiV
Z4vuPVb+DNBpDxsP8yUmazNt925H+nND5X4OpWaxKXwyhGNVicQNwZNUMBkTrNN9
N6frXTpsNVzbQdcS2qlJC9/YgIoJk2KOtWbPJYjNhLixP6Q5D9kCnusSTJV882sF
qV4Wg8y4Z+LoE53MW4LTTLPtW//e5XOsIzstAL81VXQJSdhJWBp/kjbmUZIO8yZ9
HE0XvMnsQybQv0FfQKlERPSZ51eHnlAfV1SoPv10Yy+xUGUJ5lhCLkMaTLTwJUdZ
+gQek9QmRkpQgbLevni3/GcV4clXhB4PY9bpYrrWX1Uu6lzGKAgEJTm4Diup8kyX
HAc/DVL17e8vgg8CAwEAAaOB9DCB8TAfBgNVHSMEGDAWgBStvZh6NLQm9/rEJlTv
A73gJMtUGjAdBgNVHQ4EFgQUU3m/WqorSs9UgOHYm8Cd8rIDZsswDgYDVR0PAQH/
BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wEQYDVR0gBAowCDAGBgRVHSAAME
QGA1Ud
HwQ9MDswOaA3oDWGM2h0dHA6Ly9jcmwudXNlcnRydXN0LmNvbS9BZGRUcnVzdEV4
dGVybmFsQ0FSb290LmNybDA1BggrBgEFBQcBAQQpMCcwJQYIKwYBBQUHMAGGGW
h0
dHA6Ly9vY3NwLnVzZXJ0cnVzdC5jb20wDQYJKoZIhvcNAQEMBQADggEBAJNl9jeD
lQ9ew4IcH9Z35zyKwKoJ8OkLJvHgwmp1ocd5yblSYMgpEg7wrQPWCcR23+WmgZWn
RtqCV6mVksW2jwMibDN3wXsyF24HzloUQToFJBv2FAY7qCUkDrvMKnXduXBBP3zQ
YzYhBx9G/2CkkeFnvN4ffhkUyWNnkepnB2u0j4vAbkN9w6GAbLIevFOFfdyQoaS8
Le9Gclc1Bb+7RrtubTeZtv8jkpHGbkD4jylW6l/VXxRTrPBPYer3IsynVgviuDQf
Jtl7GQVoP7o81DgGotPmjw7jtHFtQELFhLRAlSv0ZaBIefYdgWOWnU914Ph85I6p
0fKtirOMxyHNwu8=

-----END CERTIFICATE-----

3 s:/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root

i:/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root

-----BEGIN CERTIFICATE-----

MIIENjCCAx6gAwIBAgIBATANBgkqhkiG9w0BAQUFADBvMQswCQYDVQQGEwJTRTEU

MBIGA1UEChMLQWRkVHJ1c3QgQUIxJjAkBgNVBAsTHUFkZFRydXN0IEV4dGVybmFs

IFRUUCBOZXR3b3JrMSIwIAYDVQQDExlBZGRUcnVzdCBFeHRlcm5hbCBDQSBSb290

MB4XDTAwMDUzMDEwNDgzOFoXDTIwMDUzMDEwNDgzOFowbzELMAkGA1UEBhMCU0Ux

FDASBgNVBAoTC0FkZFRydXN0IEFCMSYwJAYDVQQLEx1BZGRUcnVzdCBFeHRlcm5h

bCBUVFAgTmV0d29yazEiMCAGA1UEAxMZQWRkVHJ1c3QgRXh0ZXJuYWwgQ0EgUm9v

dDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALf3GjPm8gAELTngTlvt

H7xsD821+iO2zt6bETOXpClMfZOfvUq8k+0DGuOPz+VtUFrWlymUWoCwSXrbLpX9

uMq/NzgtHj6RQa1wVsfwTz/oMp50ysiQVOnGXw94nZpAPA6sYapeFI+eh6FqUNzX

mk6vBbOmcZSccbNQYArHE504B4YCqOmoaSYYkKtMsE8jqzpPhNjfzp/haW+710LX

a0Tkx63ubUFfclpxCDezeWWkWaCUN/cALw3CknLa0Dhy2xSoRcRdKn23tNbE7qzN

E0S3ySvdQwAl+mG5aWpYIxG3pzOPVnVZ9c0p10a3CitlttNCbxWyuHv77+ldU9U0

WicCAwEAAaOB3DCB2TAdBgNVHQ4EFgQUrb2YejS0Jvf6xCZU7wO94CTLVBowCwYD

VR0PBAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wgZkGA1UdIwSBkTCBjoAUrb2YejS0

Jvf6xCZU7wO94CTLVBqhc6RxMG8xCzAJBgNVBAYTAlNFMRQwEgYDVQQKEwtBZGRU

cnVzdCBBQjEmMCQGA1UECxMdQWRkVHJ1c3QgRXh0ZXJuYWwgVFRQIE5ldHdvcmsx

IjAgBgNVBAMTGUFkZFRydXN0IEV4dGVybmFsIENBIFJvb3SCAQEwDQYJKoZIhvcN

AQEFBQADggEBALCb4IUlwtYj4g+WBpKdQZic2YR5gdkeWxQHIzZlj7DYd7usQWxH

YINRsPkyPef89iYTx4AWpb9a/IfPeHmJIZriTAcKhjW88t5RxNKWt9x+Tu5w/Rw5

6wwCURQtjr0W4MHfRnXnJK3s9EK0hZNwEGe6nQY1ShjTK3rMUUKhemPR5ruhxSvC

Nr4TDea9Y355e6cJDUCrat2PisP29owaQgVR1EX1n6diIWgVIEM8med8vSTYqZEX

c4g/VhsxOBi0cQ+azcgOno4uG+GMmIPLHzHxREzGBHNJdmAPx/i9F4BrLunMTA5a

mnkPIAou1Z5jJh5VkpTYghdae9C8x49OhgQ=

-----END CERTIFICATE-----

Server certificate

subject=/C=US/postalCode=75080/ST=TX/L=Richardson/street=800 West Campbell Road/O=The University of Texas at Dallas/OU=General/CN=www.utdallas.edu

issuer=/C=US/ST=MI/L=Ann Arbor/O=Internet2/OU=InCommon/CN=InCommon RSA Server CA

No client certificate CA names sent

Peer signing digest: SHA256

Server Temp Key: ECDH, P-256, 256 bits

SSL handshake has read 5980 bytes and written 431 bytes

New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256

Server public key is 2048 bit

Secure Renegotiation IS supported

Compression: NONE

Expansion: NONE

No ALPN negotiated

SSL-Session:

Protocol : TLSv1.2

Cipher : ECDHE-RSA-AES128-GCM-SHA256

Session-ID: C23844D2177CB8B6AA017C7E7CC5603F036838B6AA4A478AB90493B64E55B04F

Session-ID-ctx:

Master-Key: 236AAC66D0D2B9ADD8CDD4AD5EC20260DA5FBBB28E7DF306E908815C4CC86B5C36E5389D4C0765DC4CBE5E0B525E1544

Key-Arg   : None

PSK identity: None

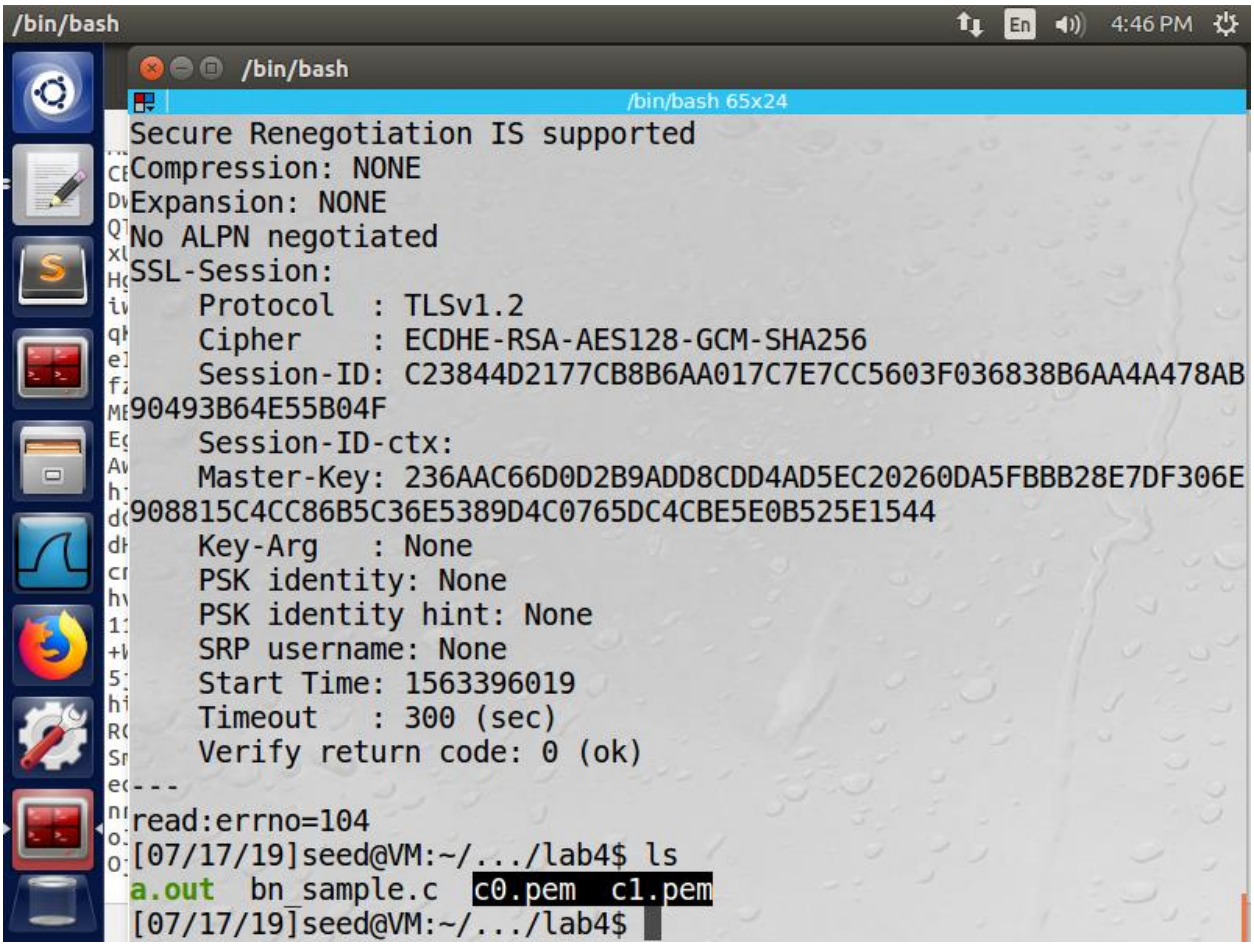
PSK identity hint: None

SRP username: None

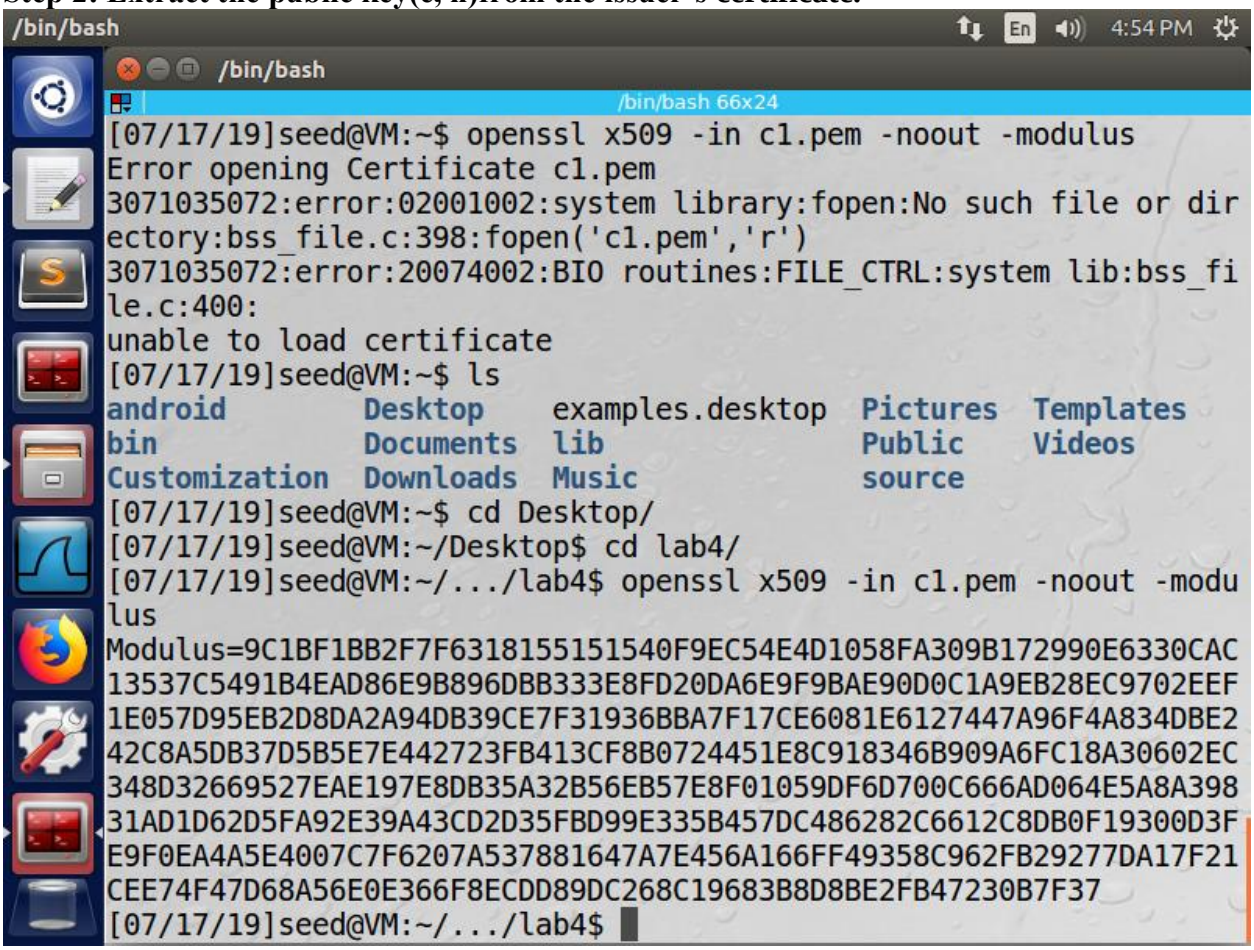
Start Time: 1563396019

Timeout   : 300 (sec)

Verify return code: 0 (ok)



Step 2: Extract the public key(e, n)from the issuer's certificate.



openssl x509 -in c1.pem -noout –modulus

Modulus=9C1BF1BB2F7F6318155151540F9EC54E4D1058FA309B172990E6330CAC13537C5491B4EAD86E9B896DBB333E8FD20DA6E9F9BAE90D0C1A9EB28EC9702EEF1E057D95EB2D8DA2A94DB39CE7F31936BBA7F17CE6081E6127447A96F4A834DBE242C8A5DB37D5B5E7E442723FB413CF8B0724451E8C918346B909A6FC18A30602EC348D32669527EAE197E8DB35A32B56EB57E8F01059DF6D700C666AD064E5A8A39831AD1D62D5FA92E39A43CD2D35FBD99E335B457DC486282C6612C8DB0F19300D3FE9F0EA4A5E4007C7F6207A537881647A7E456A166FF49358C962FB29277DA17F21CEE74F47D68A56E0E366F8ECDD89DC268C19683B8D8BE2FB47230B7F37

[07/17/19]seed@VM:~/.../lab4$ openssl x509 -in c1.pem -text -noout

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

47:20:d0:fa:85:46:1a:7e:17:a1:64:02:91:84:63:74

Signature Algorithm: sha384WithRSAEncryption

Issuer: C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust RSA Certification Authority

Validity

Not Before: Oct 6 00:00:00 2014 GMT

Not After : Oct 5 23:59:59 2024 GMT

Subject: C=US, ST=MI, L=Ann Arbor, O=Internet2, OU=InCommon, CN=InCommon RSA Server CA

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:9c:1b:f1:bb:2f:7f:63:18:15:51:51:54:0f:9e:

c5:4e:4d:10:58:fa:30:9b:17:29:90:e6:33:0c:ac:

13:53:7c:54:91:b4:ea:d8:6e:9b:89:6d:bb:33:3e:

8f:d2:0d:a6:e9:f9:ba:e9:0d:0c:1a:9e:b2:8e:c9:

70:2e:ef:1e:05:7d:95:eb:2d:8d:a2:a9:4d:b3:9c:

e7:f3:19:36:bb:a7:f1:7c:e6:08:1e:61:27:44:7a:

96:f4:a8:34:db:e2:42:c8:a5:db:37:d5:b5:e7:e4:

42:72:3f:b4:13:cf:8b:07:24:45:1e:8c:91:83:46:

b9:09:a6:fc:18:a3:06:02:ec:34:8d:32:66:95:27:

ea:e1:97:e8:db:35:a3:2b:56:eb:57:e8:f0:10:59:

df:6d:70:0c:66:6a:d0:64:e5:a8:a3:98:31:ad:1d:

62:d5:fa:92:e3:9a:43:cd:2d:35:fb:d9:9e:33:5b:

45:7d:c4:86:28:2c:66:12:c8:db:0f:19:30:0d:3f:

e9:f0:ea:4a:5e:40:07:c7:f6:20:7a:53:78:81:64:

7a:7e:45:6a:16:6f:f4:93:58:c9:62:fb:29:27:7d:

a1:7f:21:ce:e7:4f:47:d6:8a:56:e0:e3:66:f8:ec:

```
            dd:89:dc:26:8c:19:68:3b:8d:8b:e2:fb:47:23:0b:
            7f:37
        Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Authority Key Identifier:
        keyid:53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB

    X509v3 Subject Key Identifier:
        1E:05:A3:77:8F:6C:96:E2:5B:87:4B:A6:B4:86:AC:71:00:0C:E7:38
    X509v3 Key Usage: critical
        Digital Signature, Certificate Sign, CRL Sign
    X509v3 Basic Constraints: critical
        CA:TRUE, pathlen:0
    X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication
    X509v3 Certificate Policies:
        Policy: X509v3 Any Policy
        Policy: 2.23.140.1.2.2

    X509v3 CRL Distribution Points:

        Full Name:
          URI:http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl

    Authority Information Access:
        CA Issuers - URI:http://crt.usertrust.com/USERTrustRSAAddTrustCA.crt
        OCSP - URI:http://ocsp.usertrust.com
```

Signature Algorithm: sha384WithRSAEncryption

2d:11:06:38:d6:db:d7:58:68:af:aa:38:67:17:8d:e2:13:d7:
a3:14:24:d9:06:13:eb:eb:91:2f:df:4f:67:2d:c8:d3:14:d7:
56:65:52:9e:6e:1f:98:08:8e:9a:48:1b:c1:8b:59:9a:a3:57:
9b:db:86:f8:59:40:fc:19:b0:75:11:2a:c2:12:36:ba:8e:72:
8a:06:4e:27:b7:8d:58:14:d1:6f:b4:f9:68:fc:98:dd:a4:9c:
25:40:36:de:bd:17:66:2b:03:7f:78:81:b1:80:74:9e:5f:3a:
b4:26:2f:6a:48:84:36:34:8e:a7:28:ef:87:f3:61:e7:db:67:
f5:52:db:d7:d1:e6:30:71:bb:8b:a3:d4:ff:b9:64:89:9e:9b:
81:9b:8f:57:b8:64:4c:d5:06:19:8e:e7:91:85:7c:18:d1:89:
d8:f6:ea:1d:68:14:11:d9:ee:17:83:1f:50:63:cf:0e:f6:86:
2a:6e:e3:b1:a4:c9:fa:f6:34:4c:77:2a:80:86:30:b0:a3:dc:
1b:71:ec:04:a7:e4:98:bc:16:85:3e:84:26:b3:c0:e5:35:55:
7e:79:98:a3:d4:d4:8d:b6:e7:42:e8:44:20:12:37:5f:09:c9:
fb:03:e4:f5:65:74:96:ed:ca:b9:b3:f6:09:ff:4c:a6:d1:5d:
3a:fc:d1:4d:aa:e4:98:72:be:38:4b:7f:89:4e:26:8f:d4:cc:
be:56:09:71:03:4a:6c:a3:e2:35:86:dd:1e:d9:f1:31:03:f7:
13:4d:0b:11:81:31:79:cc:7a:d7:be:dc:fb:f3:76:1b:2c:bd:
b3:91:0f:00:59:07:2a:20:43:dc:4b:d8:b5:19:14:8f:e2:7a:
84:29:d1:43:3f:2f:cc:df:3f:9d:bb:bd:68:c4:ce:e0:cd:e7:
1c:31:32:78:62:fa:f0:93:a2:1e:c9:d7:9f:68:e5:a8:76:f6:
63:fe:68:99:ef:ba:36:d7:12:71:9a:9e:b3:71:1f:3b:be:00:
63:9e:3d:5f:21:c2:b1:86:1b:b8:4e:21:c3:c3:43:09:2e:63:
0c:cd:ff:14:f6:f6:22:e9:fd:ca:9f:f5:98:44:b6:41:9c:41:
c2:08:98:7d:db:a0:9f:22:7e:c0:a7:49:bb:b4:18:1f:4b:d3:
a6:2a:87:b9:5c:ca:f2:83:4c:40:03:b2:52:1a:79:21:08:37:
18:4e:d9:8d:5f:99:c6:05:5f:f1:6a:ae:ba:75:5a:78:47:3a:
3a:65:5e:e5:c4:d0:e3:da:d2:eb:5a:28:2d:b9:02:99:60:a2:

6f:3c:2f:66:7c:98:45:9c:c9:fa:01:ef:32:8e:7c:3e:f9:f4:

03:7b:24:a6:56:09:8c:24

Exponent: 65537 (0x10001)

Step 3: Extract the signature from the server's certificate

[07/17/19]seed@VM:~/.../lab4$ openssl x509 -in c0.pem -text -noout

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

66:a6:92:38:aa:2a:bd:62:7f:ec:e0:ff:0c:38:4a:77

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=US, ST=MI, L=Ann Arbor, O=Internet2, OU=InCommon, CN=InCommon RSA Server CA

Validity

Not Before: Mar 5 00:00:00 2018 GMT

Not After : Mar 4 23:59:59 2020 GMT

Subject: C=US/postalCode=75080, ST=TX, L=Richardson/street=800 West Campbell Road, O=The University of Texas at Dallas, OU=General, CN=www.utdallas.edu

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:a2:c9:b0:d1:f6:8c:f4:94:83:1b:67:ce:f5:b9:

a2:8f:c3:bc:ba:bb:1e:33:25:5c:84:5c:d2:b5:95:

2e:86:27:59:5e:04:9d:73:79:7f:61:2f:bc:fd:38:

96:c5:43:7b:f4:90:51:df:76:56:ee:f1:d4:5b:d9:

6e:ef:38:33:a5:3b:8a:a2:00:12:a9:58:46:d8:20:

d4:4d:8c:ee:4a:09:2d:20:20:6b:35:61:58:bd:4d:
79:7c:63:4b:08:f3:d6:da:22:42:11:a8:9b:a8:7f:
17:6e:57:48:74:d5:ac:b6:c6:cf:a1:40:26:f8:33:
b5:70:1c:34:0f:51:56:4d:52:c0:8f:73:9d:09:ff:
5e:8f:3f:0b:73:ce:46:47:bd:e9:7e:38:3e:c6:88:
27:1e:8e:20:1e:89:39:6e:1e:03:fc:72:2b:de:20:
d3:6b:b4:02:26:a0:c8:60:d4:7e:1b:0d:21:c2:31:
f2:1a:3d:17:fa:ca:d6:43:7f:3b:d2:9c:1d:4f:86:
f8:f9:bd:f0:11:04:74:ad:26:4f:fb:3b:f8:63:90:
a9:75:65:cb:fc:5f:68:91:da:21:ec:07:7e:92:ab:
00:bd:0f:5b:4f:a2:72:dd:aa:cb:ef:b6:d9:4c:51:
ed:17:a0:55:49:50:0a:7b:fe:5e:f0:cf:84:ca:82:
a6:09
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Authority Key Identifier:
keyid:1E:05:A3:77:8F:6C:96:E2:5B:87:4B:A6:B4:86:AC:71:00:0C:E7:38

X509v3 Subject Key Identifier:
6B:2C:2A:28:E7:52:4C:3D:A4:9E:B7:1C:AB:97:0A:96:D8:24:D1:D4
X509v3 Key Usage: critical
Digital Signature, Key Encipherment
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.5923.1.4.3.1.1

CPS: https://www.incommon.org/cert/repository/cps_ssl.pdf

Policy: 2.23.140.1.2.2

X509v3 CRL Distribution Points:

Full Name:

URI:http://crl.incommon-rsa.org/InCommonRSAServerCA.crl

Authority Information Access:

CA Issuers - URI:http://crt.usertrust.com/InCommonRSAServerCA_2.crt

OCSP - URI:http://ocsp.usertrust.com

X509v3 Subject Alternative Name:

DNS:www.utdallas.edu, DNS:utd.edu, DNS:utdallas.edu, DNS:www.utd.edu

Signature Algorithm: sha256WithRSAEncryption

6a:d1:b4:c1:ad:93:44:3c:6c:e6:8a:7d:fa:27:21:98:f5:bc:
eb:8d:a5:63:49:60:37:24:cc:92:f7:3e:2c:f8:c5:98:19:4e:
41:a4:e3:cf:77:d2:70:92:e6:ed:3a:20:c7:59:71:32:00:5b:
b8:50:d3:b3:7d:f6:a6:6a:c8:07:eb:ef:98:94:88:5b:24:1a:
ad:e3:01:1a:e5:05:68:8b:56:0e:a9:88:e2:a8:6c:5b:93:9a:
20:dd:81:66:51:51:98:24:42:15:b5:83:80:c4:6c:4e:0a:94:
43:74:2e:53:cd:ca:36:a3:b4:f1:15:b2:b2:42:6f:58:e0:c3:
cb:2c:89:e8:f4:5f:d6:0b:74:8a:49:85:a4:9a:e4:3d:a3:09:
91:40:2a:d9:a0:a5:31:77:9e:13:01:dc:ae:d5:85:c2:51:be:
ab:8c:23:8a:ac:6a:17:cc:2e:b1:e3:62:e4:bc:76:bb:98:c7:
1e:10:1e:8d:7a:b4:27:52:63:b1:46:5e:c5:15:7d:e8:fb:a8:
97:24:ef:2c:c4:1a:26:7f:ea:3b:4e:7a:db:ea:b2:e0:21:43:
59:bb:cf:5d:ce:54:17:33:22:bf:39:4a:46:d8:a7:94:e9:69:

16:65:95:33:69:e3:66:59:90:66:ab:49:3c:3d:a1:64:39:bf:

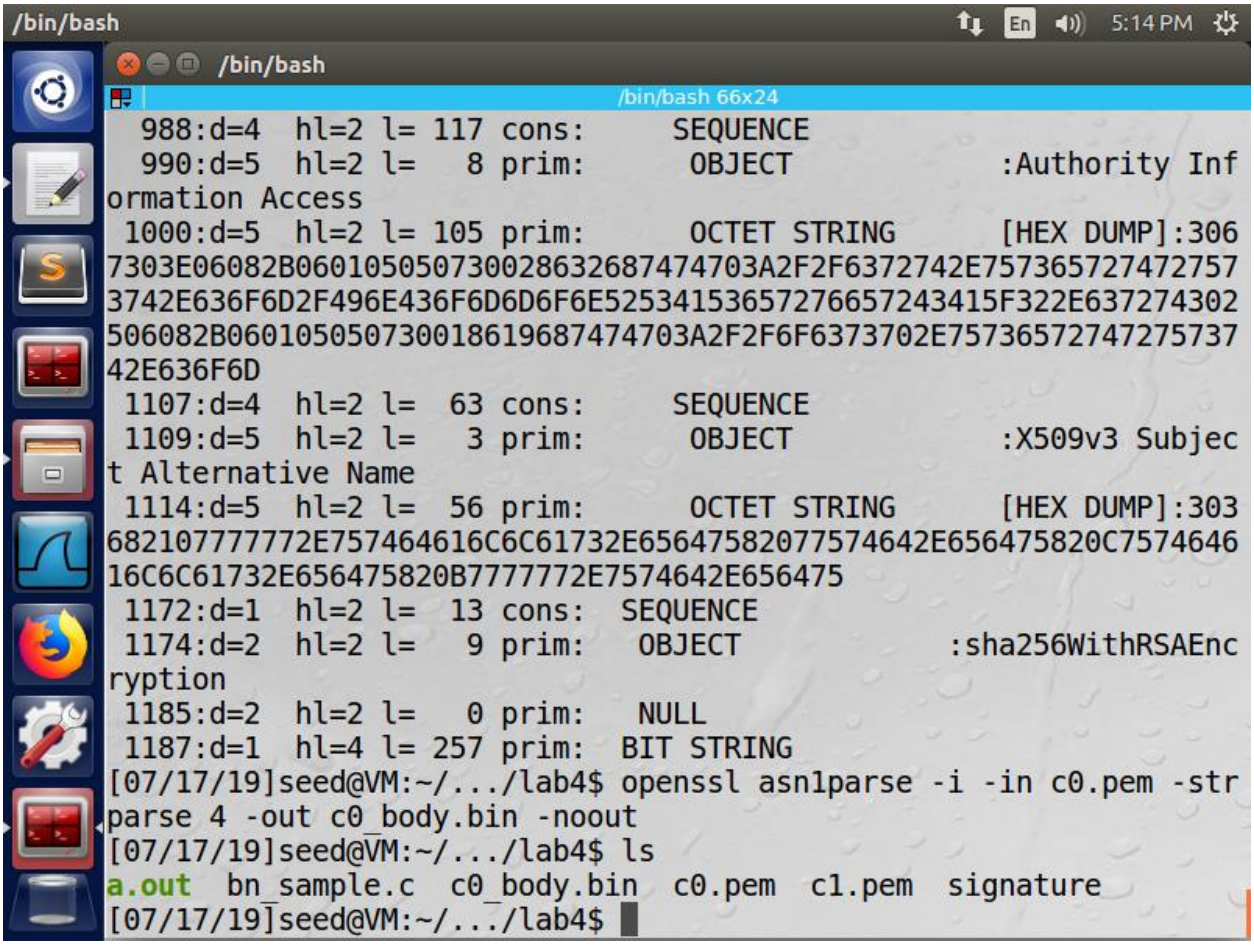
a1:b5:38:01

Signature

[07/17/19]seed@VM:~/.../lab4$ cat signature | tr -d ’[:space:]:’

6ad1b4c1ad93443c6ce68a7dfa272198f5bceb8da56349603724cc92f73e2cf8c598194e41a4e3cf77d27092e6ed3a20c7597132005bb850d3b37df6a66ac807ebef9894885b241aade3011ae505688b560ea988e2a86c5b939a20dd8166515198244215b58380c46c4e0a9443742e53cdca36a3b4f115b2b2426f58e0c3cb2c89e8f45fd60b748a4985a49ae43da30991402ad9a0a531779e1301dcaed585c251beab8c238aac6a17cc2eb1e362e4bc76bb98c71e101e8d7ab4275263b1465ec5157de8fba89724ef2cc41a267fea3b4e7adbeab2e0214359bbcf5dce54173322bf394a46d8a794e9691665953369e366599066ab493c3da16439bfa1b53801

Step 4: Extract the body of the server’s certificate.



[07/17/19]seed@VM:~/.../lab4$ openssl asn1parse -i -in c0.pem

0:d=0 hl=4 l=1444 cons: SEQUENCE

4:d=1 hl=4 l=1164 cons: SEQUENCE

```
  8:d=2  hl=2 l=   3 cons:   cont [ 0 ]
 10:d=3  hl=2 l=   1 prim:    INTEGER           :02
 13:d=2  hl=2 l=  16 prim:   INTEGER           :66A69238AA2ABD627FECE0FF0C384A77
 31:d=2  hl=2 l=  13 cons:   SEQUENCE
 33:d=3  hl=2 l=   9 prim:    OBJECT            :sha256WithRSAEncryption
 44:d=3  hl=2 l=   0 prim:    NULL
 46:d=2  hl=2 l= 118 cons:   SEQUENCE
 48:d=3  hl=2 l=  11 cons:    SET
 50:d=4  hl=2 l=   9 cons:     SEQUENCE
 52:d=5  hl=2 l=   3 prim:      OBJECT            :countryName
 57:d=5  hl=2 l=   2 prim:      PRINTABLESTRING   :US
 61:d=3  hl=2 l=  11 cons:    SET
 63:d=4  hl=2 l=   9 cons:     SEQUENCE
 65:d=5  hl=2 l=   3 prim:      OBJECT            :stateOrProvinceName
 70:d=5  hl=2 l=   2 prim:      PRINTABLESTRING   :MI
 74:d=3  hl=2 l=  18 cons:    SET
 76:d=4  hl=2 l=  16 cons:     SEQUENCE
 78:d=5  hl=2 l=   3 prim:      OBJECT            :localityName
 83:d=5  hl=2 l=   9 prim:      PRINTABLESTRING   :Ann Arbor
 94:d=3  hl=2 l=  18 cons:    SET
 96:d=4  hl=2 l=  16 cons:     SEQUENCE
 98:d=5  hl=2 l=   3 prim:      OBJECT            :organizationName
103:d=5  hl=2 l=   9 prim:      PRINTABLESTRING   :Internet2
114:d=3  hl=2 l=  17 cons:    SET
116:d=4  hl=2 l=  15 cons:     SEQUENCE
118:d=5  hl=2 l=   3 prim:      OBJECT            :organizationalUnitName
123:d=5  hl=2 l=   8 prim:      PRINTABLESTRING   :InCommon
133:d=3  hl=2 l=  31 cons:    SET
```

```
135:d=4  hl=2 l=  29 cons:     SEQUENCE
137:d=5  hl=2 l=   3 prim:      OBJECT            :commonName
142:d=5  hl=2 l=  22 prim:      PRINTABLESTRING   :InCommon RSA Server CA
166:d=2  hl=2 l=  30 cons:   SEQUENCE
168:d=3  hl=2 l=  13 prim:    UTCTIME           :180305000000Z
183:d=3  hl=2 l=  13 prim:    UTCTIME           :200304235959Z
198:d=2  hl=3 l= 185 cons:   SEQUENCE
201:d=3  hl=2 l=  11 cons:    SET
203:d=4  hl=2 l=   9 cons:     SEQUENCE
205:d=5  hl=2 l=   3 prim:      OBJECT            :countryName
210:d=5  hl=2 l=   2 prim:      PRINTABLESTRING   :US
214:d=3  hl=2 l=  14 cons:    SET
216:d=4  hl=2 l=  12 cons:     SEQUENCE
218:d=5  hl=2 l=   3 prim:      OBJECT            :postalCode
223:d=5  hl=2 l=   5 prim:      PRINTABLESTRING   :75080
230:d=3  hl=2 l=  11 cons:    SET
232:d=4  hl=2 l=   9 cons:     SEQUENCE
234:d=5  hl=2 l=   3 prim:      OBJECT            :stateOrProvinceName
239:d=5  hl=2 l=   2 prim:      PRINTABLESTRING   :TX
243:d=3  hl=2 l=  19 cons:    SET
245:d=4  hl=2 l=  17 cons:     SEQUENCE
247:d=5  hl=2 l=   3 prim:      OBJECT            :localityName
252:d=5  hl=2 l=  10 prim:      PRINTABLESTRING   :Richardson
264:d=3  hl=2 l=  31 cons:    SET
266:d=4  hl=2 l=  29 cons:     SEQUENCE
268:d=5  hl=2 l=   3 prim:      OBJECT            :streetAddress
273:d=5  hl=2 l=  22 prim:      PRINTABLESTRING   :800 West Campbell Road
297:d=3  hl=2 l=  42 cons:    SET
```

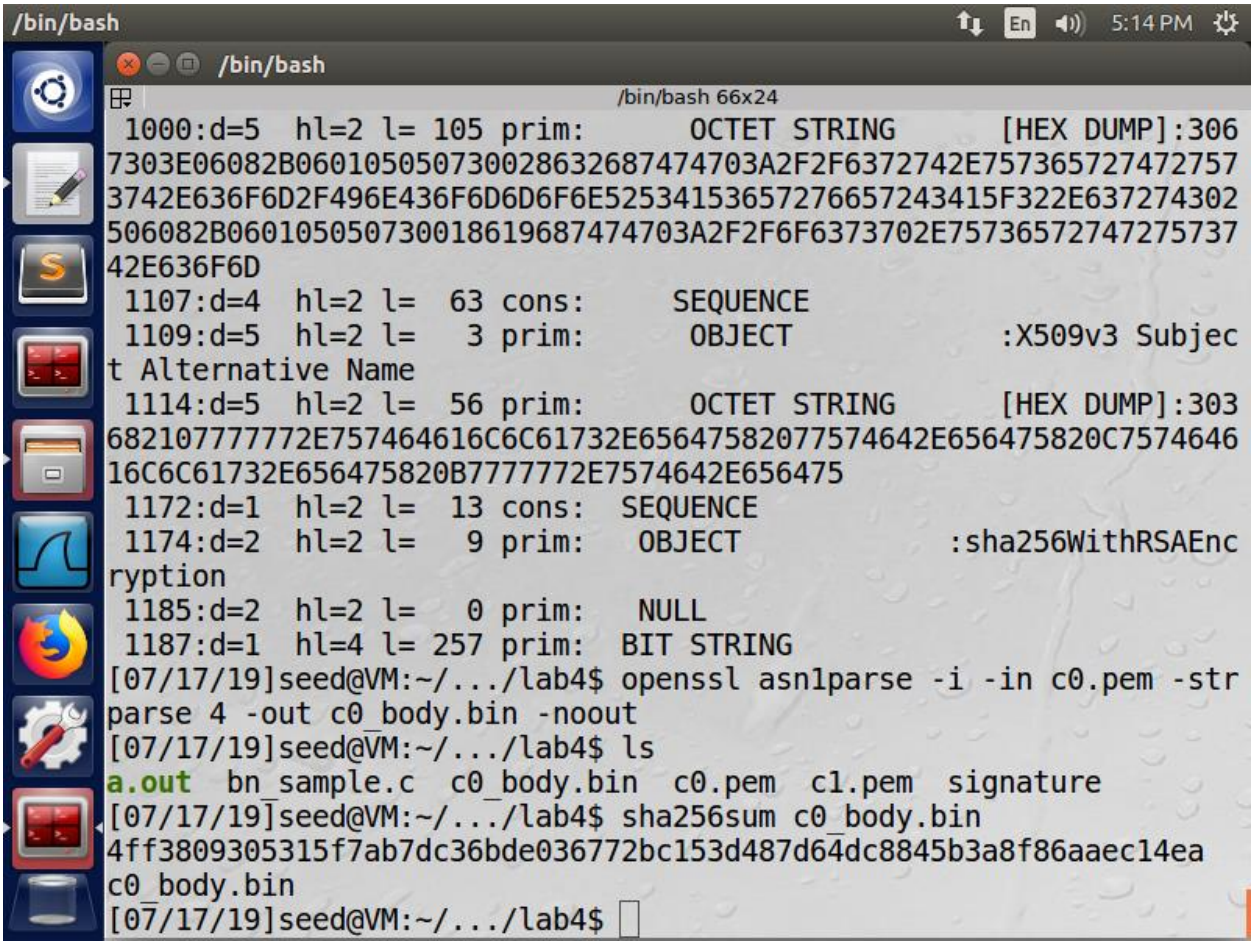
```
  299:d=4  hl=2 l=  40 cons:     SEQUENCE
  301:d=5  hl=2 l=   3 prim:      OBJECT            :organizationName
  306:d=5  hl=2 l=  33 prim:      PRINTABLESTRING   :The University of Texas at Dallas
  341:d=3  hl=2 l=  16 cons:    SET
  343:d=4  hl=2 l=  14 cons:     SEQUENCE
  345:d=5  hl=2 l=   3 prim:      OBJECT            :organizationalUnitName
  350:d=5  hl=2 l=   7 prim:      PRINTABLESTRING   :General
  359:d=3  hl=2 l=  25 cons:    SET
  361:d=4  hl=2 l=  23 cons:     SEQUENCE
  363:d=5  hl=2 l=   3 prim:      OBJECT            :commonName
  368:d=5  hl=2 l=  16 prim:      PRINTABLESTRING   :www.utdallas.edu
  386:d=2  hl=4 l= 290 cons:   SEQUENCE
  390:d=3  hl=2 l=  13 cons:    SEQUENCE
  392:d=4  hl=2 l=   9 prim:     OBJECT            :rsaEncryption
  403:d=4  hl=2 l=   0 prim:     NULL
  405:d=3  hl=4 l= 271 prim:    BIT STRING
  680:d=2  hl=4 l= 488 cons:   cont [ 3 ]
  684:d=3  hl=4 l= 484 cons:    SEQUENCE
  688:d=4  hl=2 l=  31 cons:     SEQUENCE
  690:d=5  hl=2 l=   3 prim:      OBJECT            :X509v3 Authority Key Identifier
  695:d=5  hl=2 l=  24 prim:      OCTET STRING      [HEX
DUMP]:301680141E05A3778F6C96E25B874BA6B486AC71000CE738
  721:d=4  hl=2 l=  29 cons:     SEQUENCE
  723:d=5  hl=2 l=   3 prim:      OBJECT            :X509v3 Subject Key Identifier
  728:d=5  hl=2 l=  22 prim:      OCTET STRING      [HEX
DUMP]:04146B2C2A28E7524C3DA49EB71CAB970A96D824D1D4
  752:d=4  hl=2 l=  14 cons:     SEQUENCE
  754:d=5  hl=2 l=   3 prim:      OBJECT            :X509v3 Key Usage
  759:d=5  hl=2 l=   1 prim:      BOOLEAN           :255
```

```
  762:d=5  hl=2 l=   4 prim:      OCTET STRING      [HEX DUMP]:030205A0

  768:d=4  hl=2 l=  12 cons:     SEQUENCE

  770:d=5  hl=2 l=   3 prim:      OBJECT            :X509v3 Basic Constraints

  775:d=5  hl=2 l=   1 prim:      BOOLEAN           :255

  778:d=5  hl=2 l=   2 prim:      OCTET STRING      [HEX DUMP]:3000

  782:d=4  hl=2 l=  29 cons:     SEQUENCE

  784:d=5  hl=2 l=   3 prim:      OBJECT            :X509v3 Extended Key Usage

  789:d=5  hl=2 l=  22 prim:      OCTET STRING      [HEX
DUMP]:301406082B06010505070301060 82B06010505070302

  813:d=4  hl=2 l= 103 cons:     SEQUENCE

  815:d=5  hl=2 l=   3 prim:      OBJECT            :X509v3 Certificate Policies

  820:d=5  hl=2 l=  96 prim:      OCTET STRING      [HEX
DUMP]:305E3052060C2B06010401AE230104030101304230400608 2B0601050507020116346
8747470733A2F2F7777772E696E636F6D6D6F6E2E6F72672F636572742F7265706F7369746
F72792F6370735F73736C2E706466300806066781 0C010202

  918:d=4  hl=2 l=  68 cons:     SEQUENCE

  920:d=5  hl=2 l=   3 prim:      OBJECT            :X509v3 CRL Distribution Points

  925:d=5  hl=2 l=  61 prim:      OCTET STRING      [HEX
DUMP]:303B3039A037A0358633687474703A2F2F63726C2E696E636F6D6D6F6E2D727361 2
2E6F72672F496E436F6D6D6F6E525341536572766572434 12E63726C

  988:d=4  hl=2 l= 117 cons:     SEQUENCE

  990:d=5  hl=2 l=   8 prim:      OBJECT            :Authority Information Access

 1000:d=5  hl=2 l= 105 prim:      OCTET STRING      [HEX
DUMP]:3067303E06082B06010505073002863268747470 3A2F2F6372742E757365727472757
3742E636F6D2F496E436F6D6D6F6E525341536572766572434 15F322E637274302506082B0
6010505073001861968747470 3A2F2F6F6373702E757365727472757374 2E636F6D

 1107:d=4  hl=2 l=  63 cons:     SEQUENCE

 1109:d=5  hl=2 l=   3 prim:      OBJECT            :X509v3 Subject Alternative Name

 1114:d=5  hl=2 l=  56 prim:      OCTET STRING      [HEX
DUMP]:303682107777772E757464616C6C61732E65647582077574642E656475820C7574646
16C6C61732E656475820B7777772E7574642E656475

 1172:d=1  hl=2 l=  13 cons:  SEQUENCE
```

1174:d=2 hl=2 l= 9 prim: OBJECT :sha256WithRSAEncryption

1185:d=2 hl=2 l= 0 prim: NULL

1187:d=1 hl=4 l= 257 prim: BIT STRING



Body starts at line 4 and ends at line 1171

[07/17/19]seed@VM:~/.../lab4$ sha256sum c0_body.bin

4ff3809305315f7ab7dc36bde036772bc153d487d64dc8845b3a8f86aaec14ea c0_body.bin

Step 5:

Public key (n) - Modulus

9C1BF1BB2F7F6318155151540F9EC54E4D1058FA309B172990E6330CAC13537C5491B4E
AD86E9B896DBB333E8FD20DA6E9F9BAE90D0C1A9EB28EC9702EEF1E057D95EB2D8D
A2A94DB39CE7F31936BBA7F17CE6081E6127447A96F4A834DBE242C8A5DB37D5B5E7
E442723FB413CF8B0724451E8C918346B909A6FC18A30602EC348D32669527EAE197E8D
B35A32B56EB57E8F01059DF6D700C666AD064E5A8A39831AD1D62D5FA92E39A43CD2

D35FBD99E335B457DC486282C6612C8DB0F19300D3FE9F0EA4A5E4007C7F6207A53788
1647A7E456A166FF49358C962FB29277DA17F21CEE74F47D68A56E0E366F8ECDD89DC2
68C19683B8D8BE2FB47230B7F37

Public key (e) - Exponent: 65537 (0x10001)

Signature:
6ad1b4c1ad93443c6ce68a7dfa272198f5bceb8da56349603724cc92f73e2cf8c598194e41a4e3cf7
7d27092e6ed3a20c7597132005bb850d3b37df6a66ac807ebef9894885b241aade3011ae505688b5
60ea988e2a86c5b939a20dd8166515198244215b58380c46c4e0a9443742e53cdca36a3b4f115b2b
2426f58e0c3cb2c89e8f45fd60b748a4985a49ae43da30991402ad9a0a531779e1301dcaed585c251
beab8c238aac6a17cc2eb1e362e4bc76bb98c71e101e8d7ab4275263b1465ec5157de8fba89724ef2
cc41a267fea3b4e7adbeab2e0214359bbcf5dce54173322bf394a46d8a794e9691665953369e3665
99066ab493c3da16439bfa1b53801

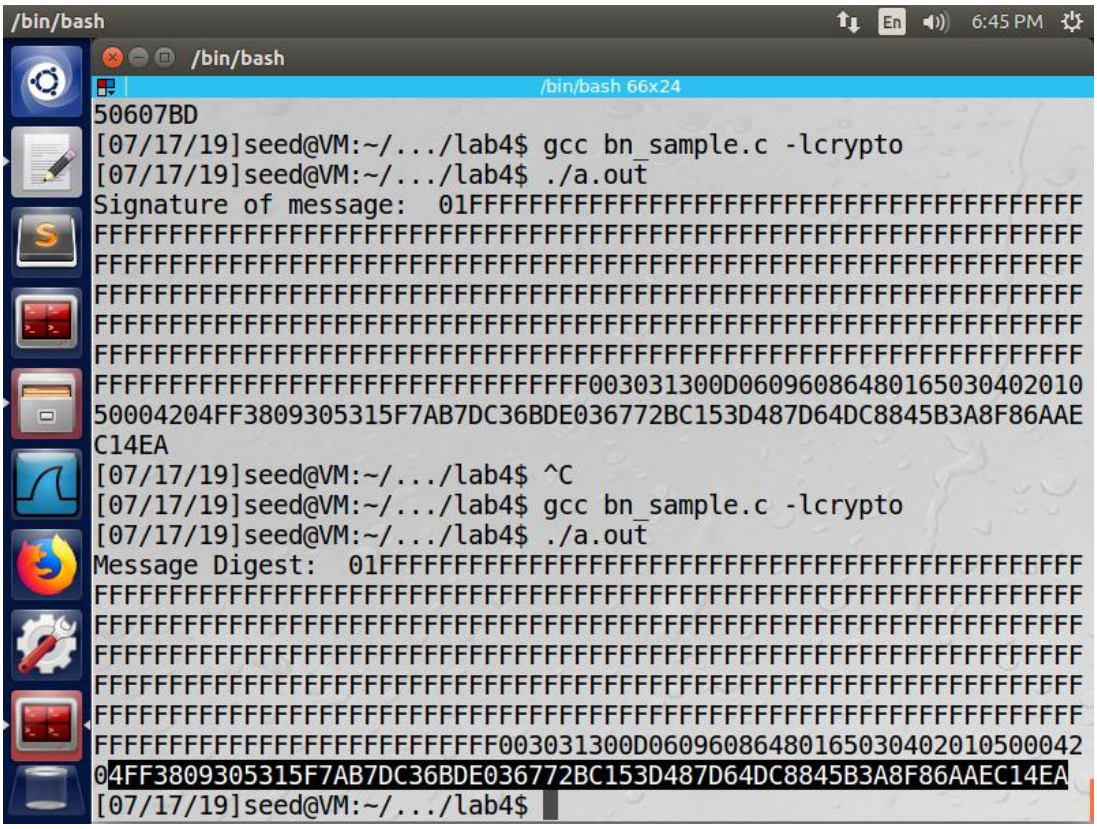
BN_mod_exp(res, s, e, n, ctx)

Where s is the signature, and (e, n) are their public key values.

Using the values after running the program the result of BN_mod_exp(res,s,e,n,ctx) was

4FF3809305315F7AB7DC36BDE036772BC153D487D64DC8845B3A8F86AAEC14EA

The values matched.



```
50607BD
[07/17/19]seed@VM:~/.../lab4$ gcc bn_sample.c -lcrypto
[07/17/19]seed@VM:~/.../lab4$ ./a.out
Signature of message:  01FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF003031300D0609608648016503040201 0
50004204FF3809305315F7AB7DC36BDE036772BC153D487D64DC8845B3A8F86AAE
C14EA
[07/17/19]seed@VM:~/.../lab4$ ^C
[07/17/19]seed@VM:~/.../lab4$ gcc bn_sample.c -lcrypto
[07/17/19]seed@VM:~/.../lab4$ ./a.out
Message Digest:  01FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFF003031300D060960864801650304020105000042
04FF3809305315F7AB7DC36BDE036772BC153D487D64DC8845B3A8F86AAEC14EA
[07/17/19]seed@VM:~/.../lab4$ 
```