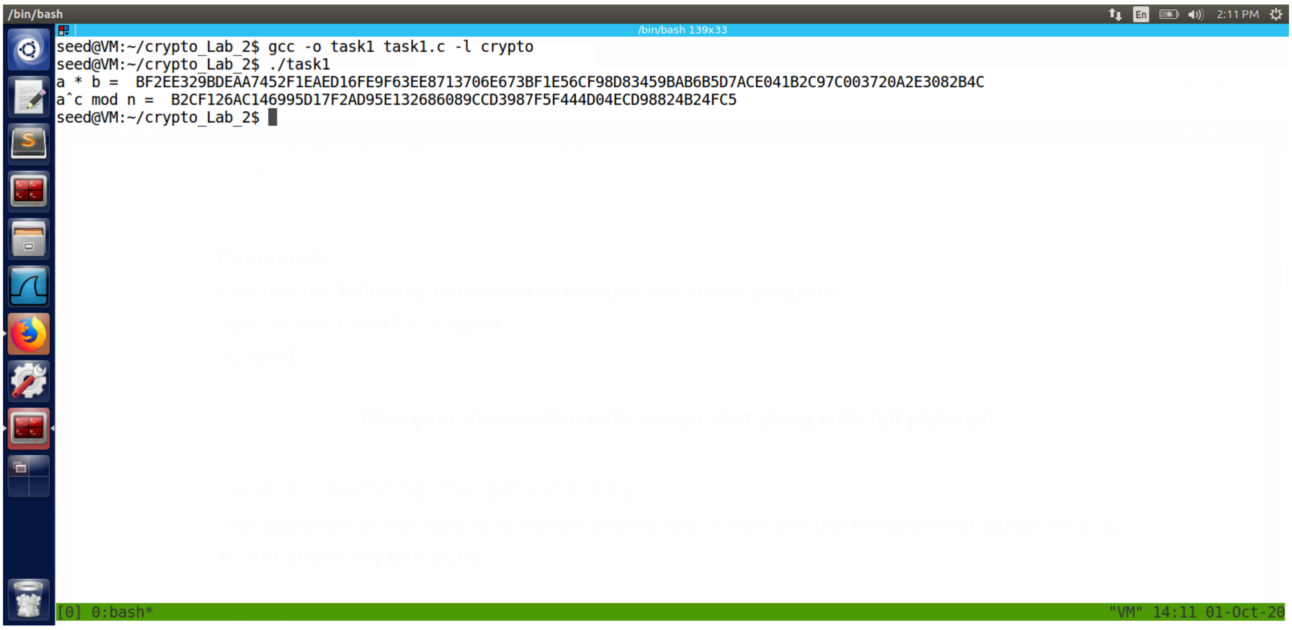
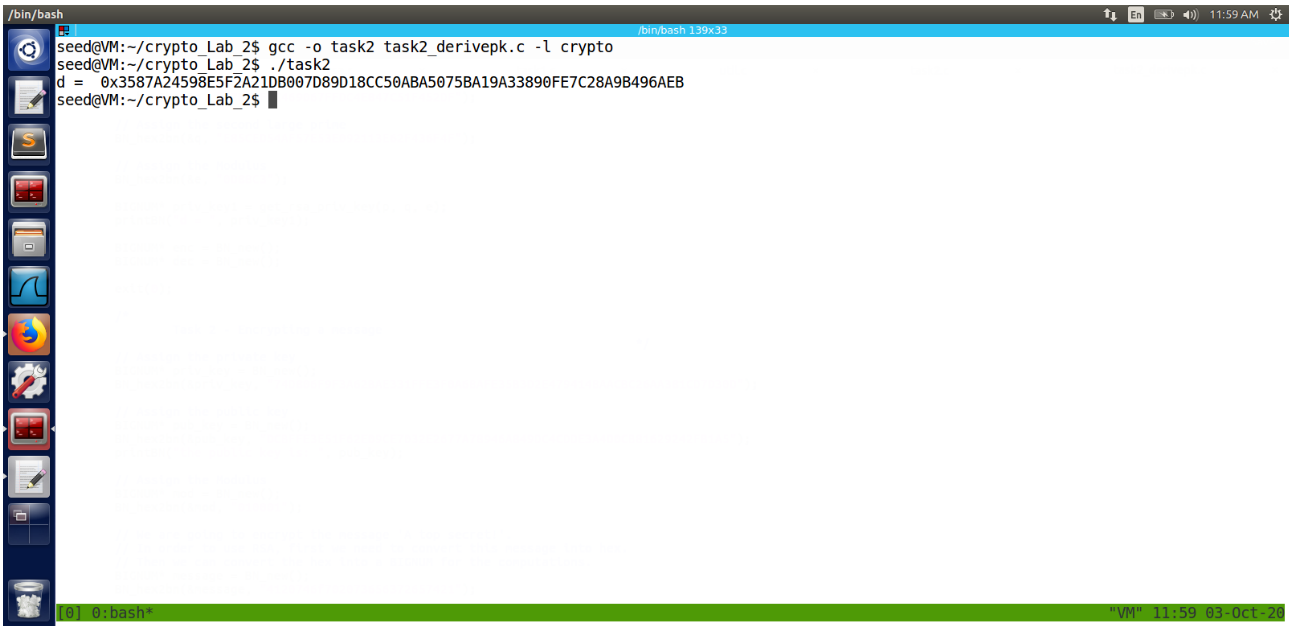
Task 1: A Complete Example of BIGNUM



```
seed@VM:~/crypto_Lab_2$ gcc -o task1 task1.c -l crypto
seed@VM:~/crypto_Lab_2$ ./task1
a * b =  BF2EE329BDEAA7452F1EAED16FE9F63EE8713706E673BF1E56CF98D83459BAB6B5D7ACE041B2C97C003720A2E3082B4C
a^c mod n =  B2CF126AC146995D17F2AD95E132686089CCD3987F5F444D04ECD98824B24FC5
seed@VM:~/crypto_Lab_2$ 
[0] 0:bash*                                                                                                   "VM" 14:11 01-Oct-20
```

Observation:
Its a long hexdecimal number NOT decimal number
finding mod_exp using openssl/bn.h libraray

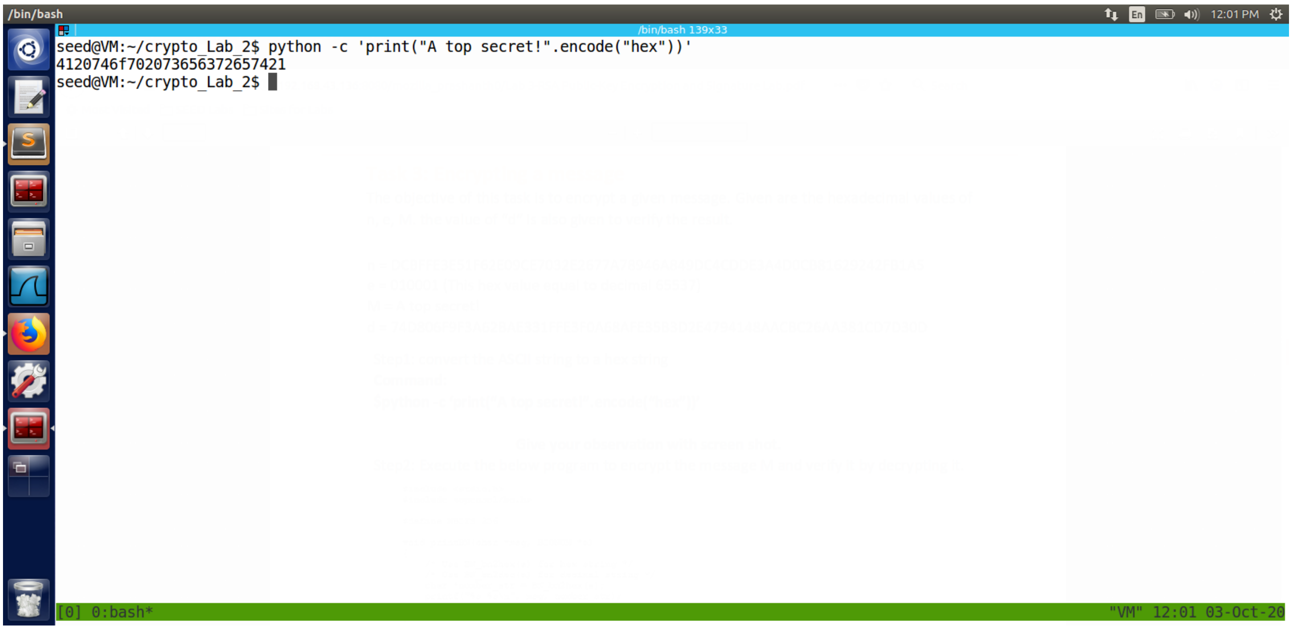
Task 2: Deriving the private key



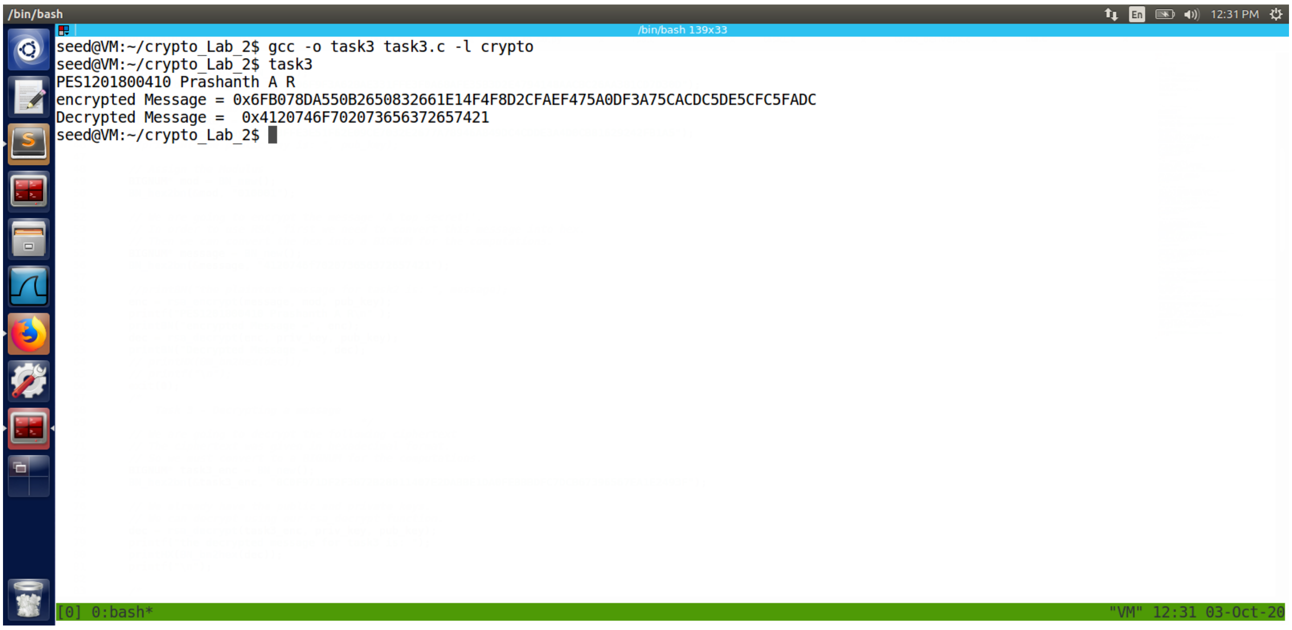
```
seed@VM:~/crypto_Lab_2$ gcc -o task2 task2_derivepk.c -l crypto
seed@VM:~/crypto_Lab_2$ ./task2
d =  0x3587A24598E5F2A21DB007D89D18CC50ABA5075BA19A33890FE7C28A9B496AEB
seed@VM:~/crypto_Lab_2$ 
[0] 0:bash*                                                                                                   "VM" 11:59 03-Oct-20
```

Observation:
finding modular inverse usig BN_mod_inverse function
d is private key

Task 3: Encrypting a message

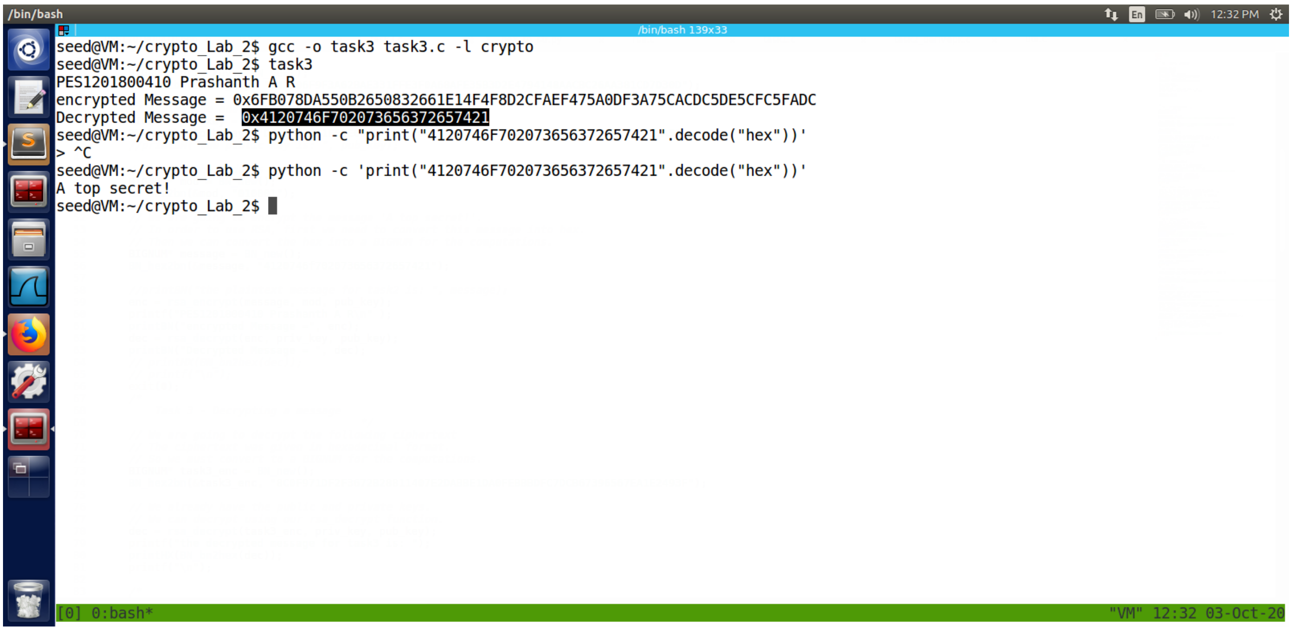


```
seed@VM:~/crypto_Lab_2$ python -c 'print("A top secret!".encode("hex"))'
4120746f702073656372657421
seed@VM:~/crypto_Lab_2$ 
```



```
seed@VM:~/crypto_Lab_2$ gcc -o task3 task3.c -l crypto
seed@VM:~/crypto_Lab_2$ task3
PES1201800410 Prashanth A R
encrypted Message = 0x6FB078DA550B2650832661E14F4F8D2CFAEF475A0DF3A75CACDC5DE5CFC5FADC
Decrypted Message =  0x4120746F702073656372657421
seed@VM:~/crypto_Lab_2$ 
```

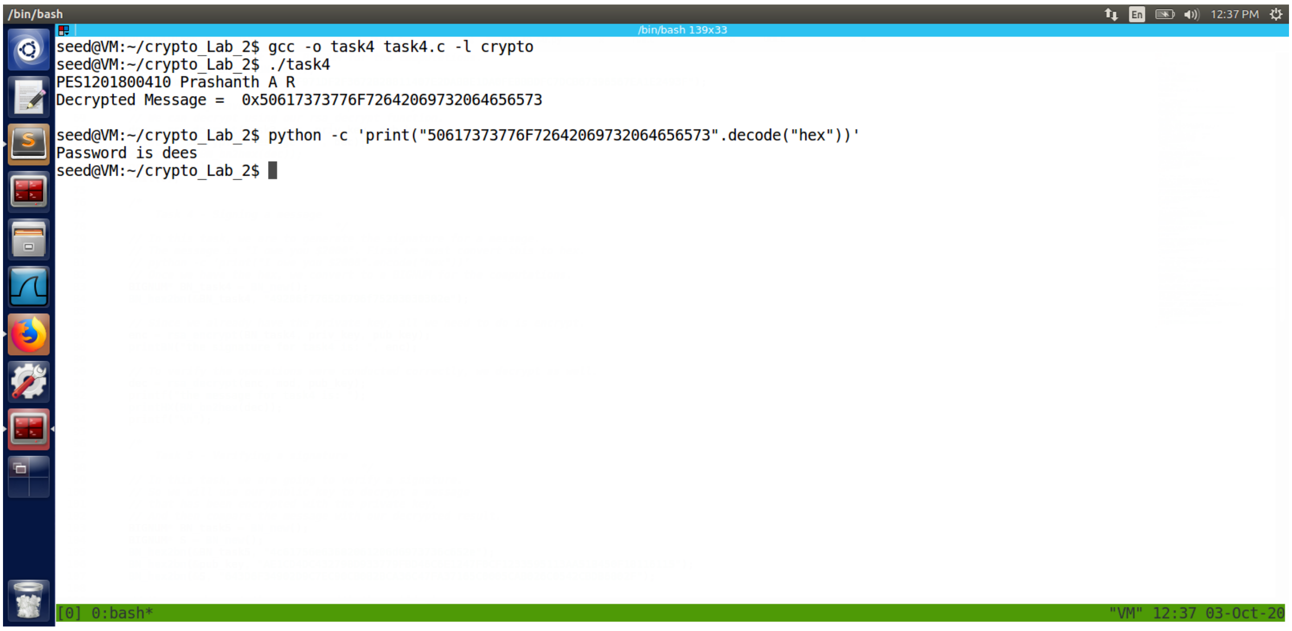
using python to convert hex to string and vice versa



```
seed@VM:~/crypto_Lab_2$ gcc -o task3 task3.c -l crypto
seed@VM:~/crypto_Lab_2$ task3
PES1201800410 Prashanth A R
encrypted Message = 0x6FB078DA550B2650832661E14F4F8D2CFAEF475A0DF3A75CACDC5DE5CFC5FADC
Decrypted Message =  0x4120746F702073656372657421
seed@VM:~/crypto_Lab_2$ python -c "print("4120746F702073656372657421".decode("hex"))'
> ^C
seed@VM:~/crypto_Lab_2$ python -c 'print("4120746F702073656372657421".decode("hex"))'
A top secret!
seed@VM:~/crypto_Lab_2$ 
[0] 0:bash*                                                                          "VM" 12:32 03-Oct-20
```

```
Observation:
we are using python to convert from hex to string and vice versa
decrypting the message using n , e , d , m = meassage.
enc = m^e mod n ;//to encrypt
dec = enc^d mod n ; // to decrypt
```

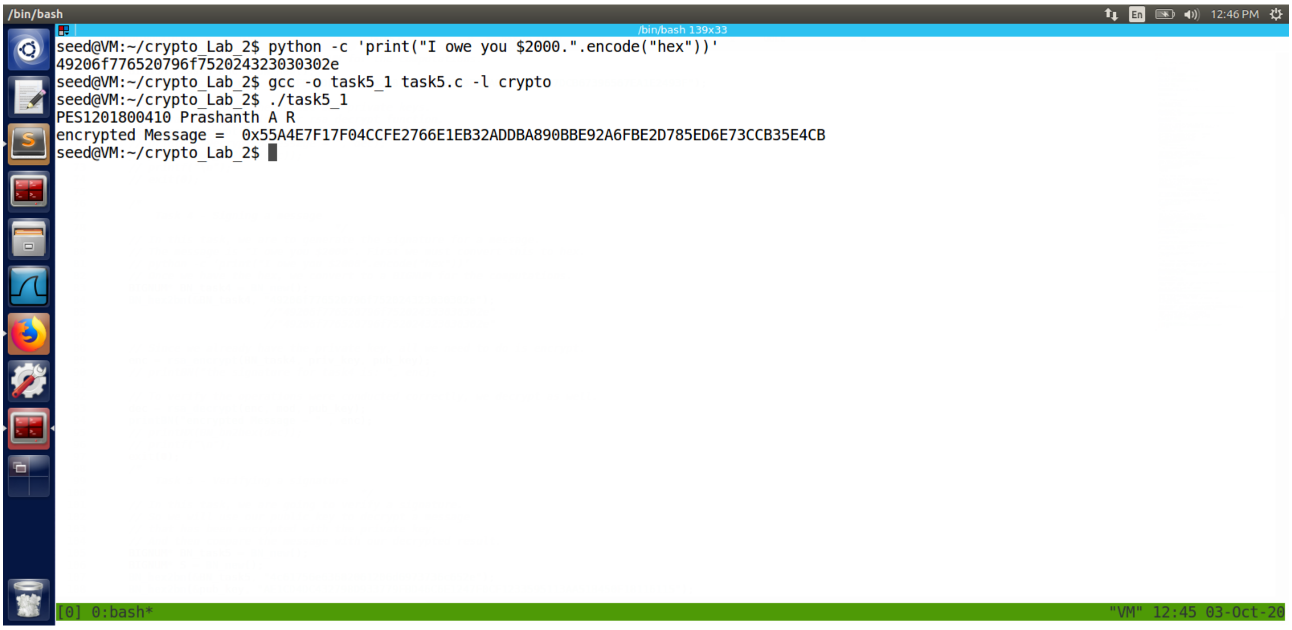
Task 4: Decrypting a message



```
seed@VM:~/crypto_Lab_2$ gcc -o task4 task4.c -l crypto
seed@VM:~/crypto_Lab_2$ ./task4
PES1201800410 Prashanth A R
Decrypted Message =  0x50617373776F72642069732064656573

seed@VM:~/crypto_Lab_2$ python -c 'print("50617373776F72642069732064656573".decode("hex"))'
Password is dees
seed@VM:~/crypto_Lab_2$ 
[0] 0:bash*                                                                          "VM" 12:37 03-Oct-20
```

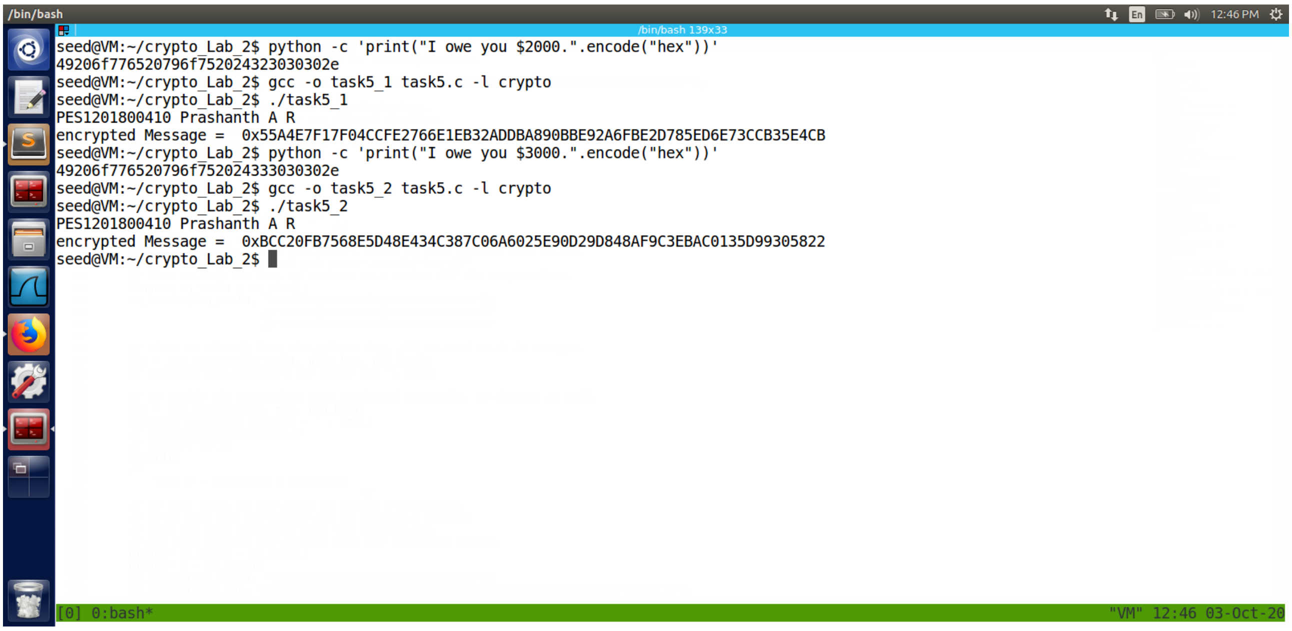
```
Observation:
decrypting a give message , n , e, d
same as last task
decrypted message is “Password is dees”
which apperently is seed lab root password xD.
```

Task 5: Signing a Message



```
seed@VM:~/crypto_Lab_2$ python -c 'print("I owe you $2000.".encode("hex"))'
49206f776520796f752024323030302e
seed@VM:~/crypto_Lab_2$ gcc -o task5_1 task5.c -l crypto
seed@VM:~/crypto_Lab_2$ ./task5_1
PES1201800410 Prashanth A R
encrypted Message =  0x55A4E7F17F04CCFE2766E1EB32ADDBA890BBE92A6FBE2D785ED6E73CCB35E4CB
seed@VM:~/crypto_Lab_2$ 
```

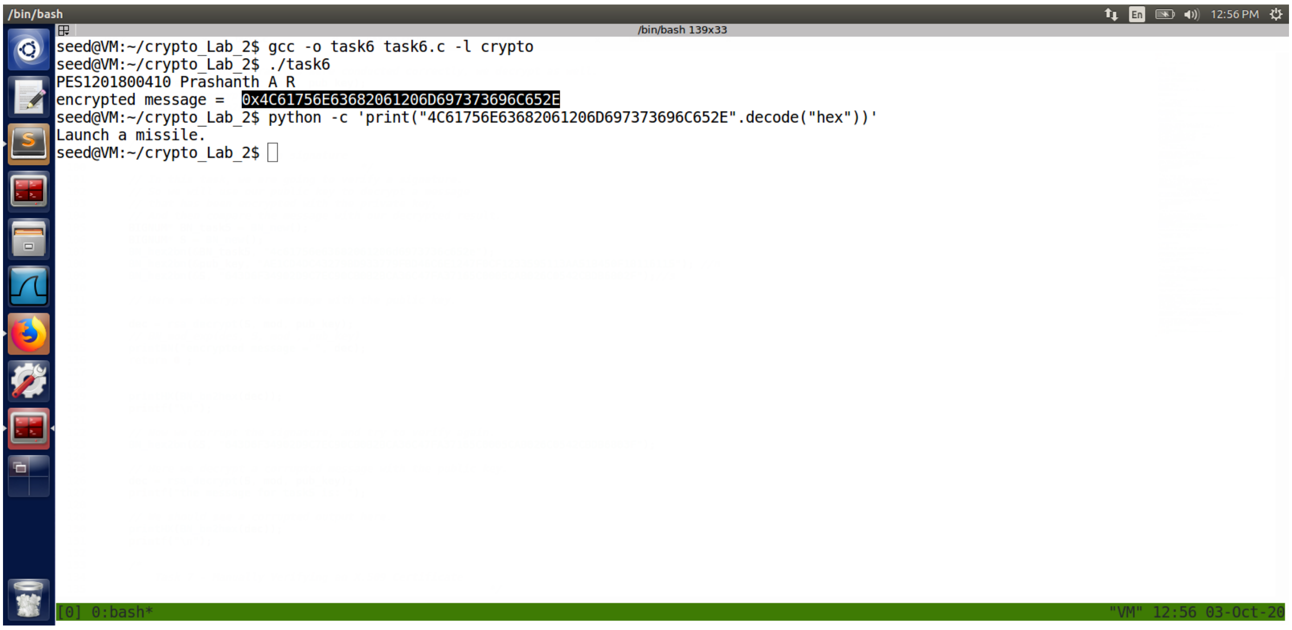
After changing $2000 to $3000



```
seed@VM:~/crypto_Lab_2$ python -c 'print("I owe you $2000.".encode("hex"))'
49206f776520796f752024323030302e
seed@VM:~/crypto_Lab_2$ gcc -o task5_1 task5.c -l crypto
seed@VM:~/crypto_Lab_2$ ./task5_1
PES1201800410 Prashanth A R
encrypted Message =  0x55A4E7F17F04CCFE2766E1EB32ADDBA890BBE92A6FBE2D785ED6E73CCB35E4CB
seed@VM:~/crypto_Lab_2$ python -c 'print("I owe you $3000.".encode("hex"))'
49206f776520796f752024333030302e
seed@VM:~/crypto_Lab_2$ gcc -o task5_2 task5.c -l crypto
seed@VM:~/crypto_Lab_2$ ./task5_2
PES1201800410 Prashanth A R
encrypted Message =  0xBCC20FB7568E5D48E434C387C06A6025E90D29D848AF9C3EBAC0135D99305822
seed@VM:~/crypto_Lab_2$ 
```

Observation:
we can see a great change in cipher text just by chaning one letter for plaintext
We can observer avalanche effect in RSA .

Task 6: Verifying a Signature

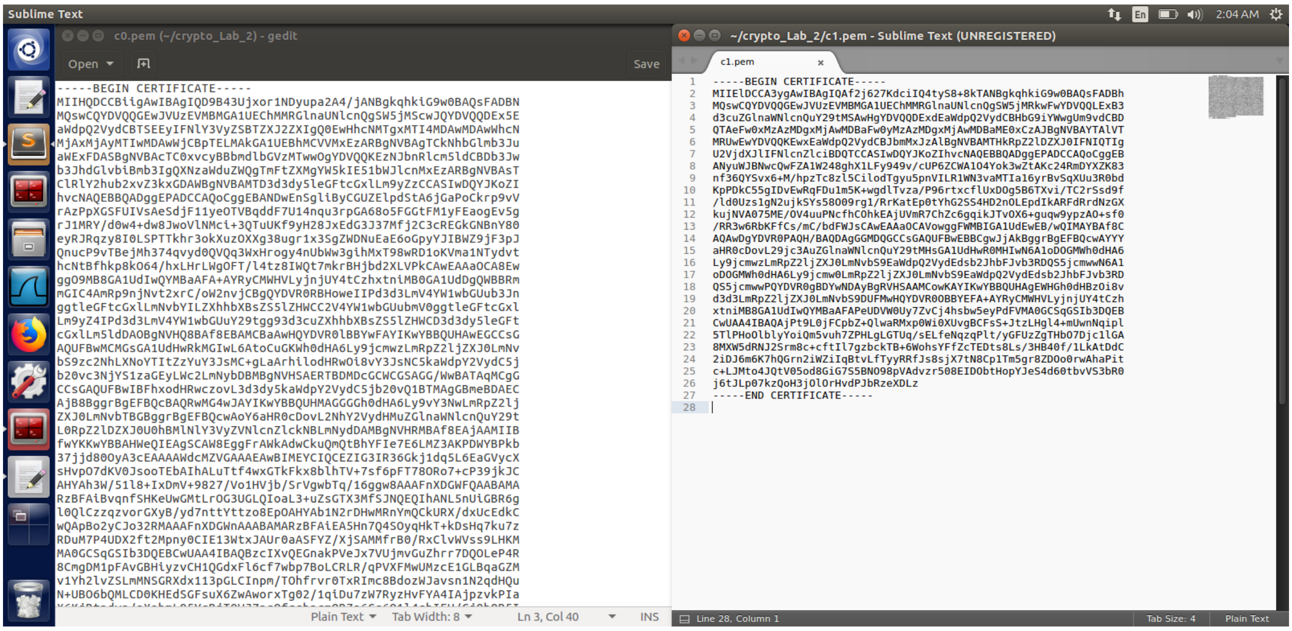


```
seed@VM:~/crypto_Lab_2$ gcc -o task6 task6.c -l crypto
seed@VM:~/crypto_Lab_2$ ./task6
PES1201800410 Prashanth A R
encrypted message =  0x4C61756E63682061206D697373696C652E
seed@VM:~/crypto_Lab_2$ python -c 'print("4C61756E63682061206D697373696C652E".decode("hex"))'
Launch a missile.
seed@VM:~/crypto_Lab_2$ 
[0] 0:bash*                                                                        "VM" 12:56 03-Oct-20
```

Observation:
Same as Task5 or Task4 given message , S(signature) which is d, e , n decrypt the message
decrypted message is Launch a missile.

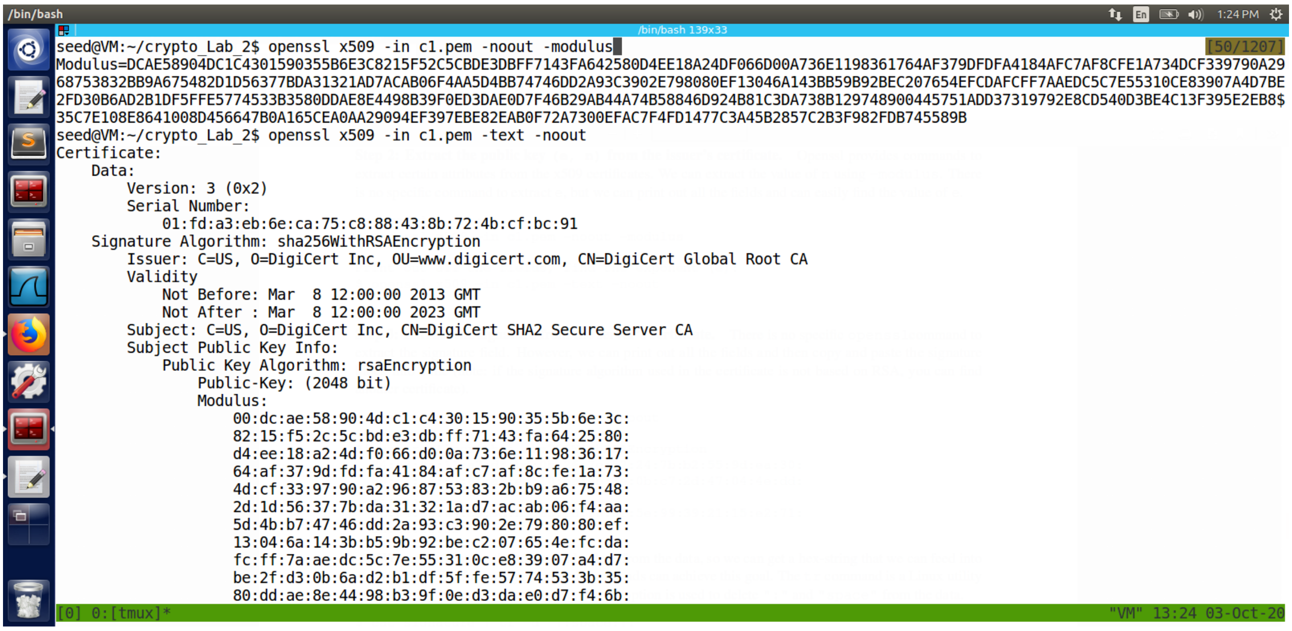
Task 7: Manually verifying an X.509 Certificate

c0.pem has server certificate , c1.pem has root certificate



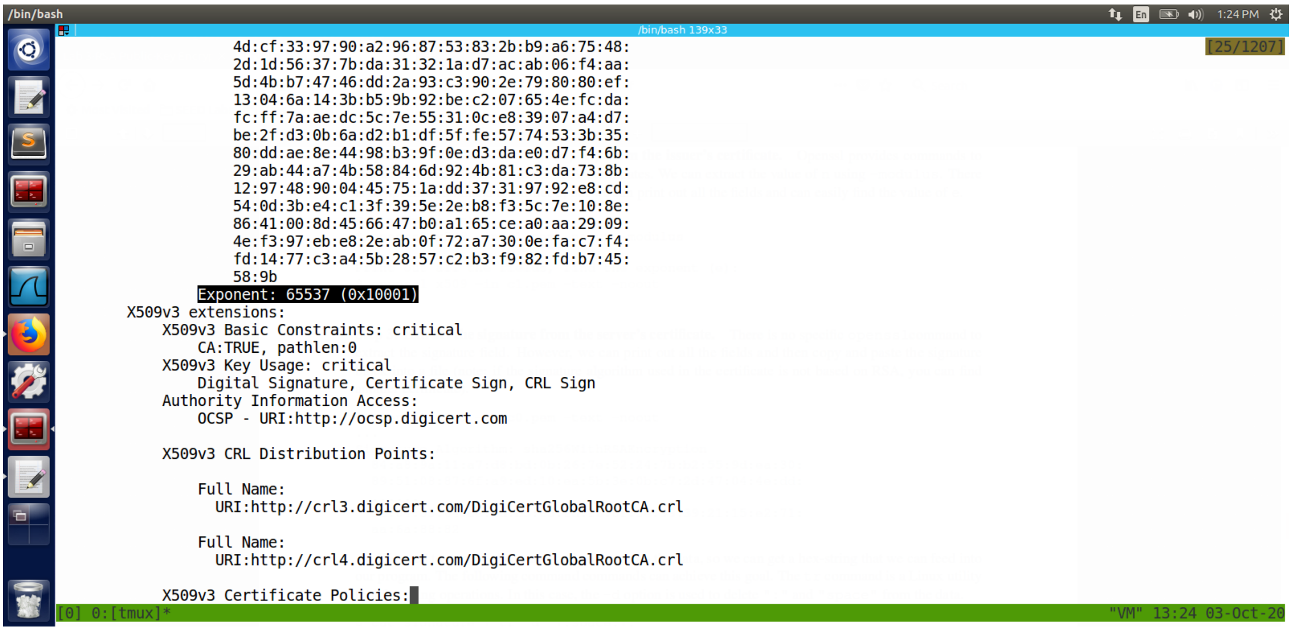
```
-----BEGIN CERTIFICATE-----
MIIHQDCCBiigAwIBAgIQD9B43Ujxor1NDyupa2A4/jANBgkqhkiG9w0BAQsFADBN
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMScwJQYDVQQDEx5E
aWdpQ2VydCBTSEEyIFNlY3VyZSBTZXJ2ZXIgQ0EwHhcNMTgxMTI4MDAwMDAwWhcN
MjAxMjAyMTIwMDAwWjCBpTELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3Ju
aWExFDASBgNVBAcTC0xvcyBBbmdlbGVzMTwwOgYDVQQKEzNJbnRlcm5ldCBDb3Jw
b3JhdGlvbiBmb3IgQXNzaWduZWQgTmFtZXMgYW5kIE51bWJlcnMxEzARBgNVBAsT
ClRlY2hub2xvZ3kxGDAWBgNVBAMTD3d3dy5leGFtcGxlLm9yZzCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBANDwEnSgliByCGUZElpdStA6jGaPoCkrp9vV
rAzPpXGSFUIVsAeSdjF11yeOTVBqddF7U14nqu3rpGA68o5FGGtFM1yFEaogEv5g
rJ1MRY/d0w4+dw8JwoVlNMci+3QTuUKf9yH28JxEdG3J37Mfj2C3cREGkGNBnY80
eyRJRqzy8I0LSPTTkhr3okXuzOXXg38ugr1x3SgZWDNuEaE6oGpyYJIBWZ9jF3pJ
QnucP9vTBejMh374qvyd0QVQq3WxHrogy4nUbWw3gihMxT98wRD1oKVma1NTydvt
hcNtBfhkp8kO64/hxLHrLWgOFT/l4tz8IWQt7mkrBHjbd2XLVPkCAwEAAaOCA8Ew
ggO9MB8GA1UdIwQYMBaAFA+AYRyCMWHVLyjnjUY4tCzhxtniMB0GA1UdDgQWBBRm
mGIC4AmRp9njNvt2xrC/oW2nvjCBgQYDVR0RBHoweIIPd3d3LmV4YW1wbGUub3Jn
ggtleGFtcGxlLmNvbYILZXhhbXBsZS5lZHWCC2V4YW1wbGUubmV0ggtleGFtcGxl
Lm9yZ4IPd3d3LmV4YW1wbGUuY29tgg93d3cuZXhhbXBsZS5lZHWCD3d3dy5leGFt
cGxlLm5ldDAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsG
AQUFBwMCMGsGA1UdHwRkMGIwL6AtoCuGKWh0dHA6Ly9jcmwzLmRpZ2ljZXJ0LmNv
bS9zc2NhLXNoYTItZzYuY3JsMC+gLaArhilodHRwOi8vY3JsNC5kaWdpY2VydC5j
b20vc3NjYS1zaGEyLWc2LmNybDBMBgNVHSAERTBDMDcGCWCGSAGG/WwBATAqMCgG
CCsGAQUFBwIBFhxodHRwczovL3d3dy5kaWdpY2VydC5jb20vQ1BTMAgGBmeBDAEC
AjB8BggrBgEFBQcBAQRwMG4wJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRpZ2lj
ZXJ0LmNvbTBGBggrBgEFBQcwAoY6aHR0cDovL2NhY2VydHMuZGlnaWNlcnQuY29t
L0RpZ2lDZXJ0U0hBMlNlY3VyZVNlcnZlckNBLmNydDAMBgNVHRMBAf8EAjAAMIIB
fwYKKwYBBAHWeQIEAgSCAW8EggFrAWkAdwCkuQmQtBhYFIe7E6LMZ3AKPDWYBPkb
37jjd80OyA3cEAAAAWdcMZVGAAAEAwBIMEYCIQCEZIG3IR36Gkj1dq5L6EaGVycX
sHvpO7dKV0JsooTEbAIhALuTtf4wxGTkFkx8blhTV+7sf6pFT78ORo7+cP39jkJC
AHYAh3W/51l8+IxDmV+9827/Vo1HVjb/SrVgwbTq/16ggw8AAAFnXDGWFQAABAMA
RzBFAiBvqnfSHKeUwGMtLrOG3UGLQIoaL3+uZsGTX3MfSJNQEQIhANL5nUiGBR6g
l0QlCzzqzvorGXyB/yd7nttYttzo8EpOAHYAb1N2rDHwMRnYmQCkURX/dxUcEdkC
wQApBo2yCJo32RMAAAFnXDGWnAAABAMARzBFAiEA5Hn7Q4SOyqHkT+kDsHq7ku7z
RDuM7P4UDX2ft2Mpny0CIE13WtxJAUr0aASFYZ/XjSAMMfrB0/RxClvWVss9LHKM
MA0GCSqGSIb3DQEBCwUAA4IBAQBzcIXvQEGnakPVeJx7VUjmvGuZhrr7DQOLeP4R
8CmgDM1pFAvGBHiyzvCH1QGdxFl6cf7wbp7BoLCRLR/qPVXFMwUMzcE1GLBqaGZM
v1Yh2lvZSLmMNSGRXdx113pGLCInpm/TOhfrvr0TxRImc8BdozWJavsn1N2qdHQu
N+UBO6bQMLCD0KHEdSGFsuX6ZwAworxTg02/1qiDu7zW7RyzHvFYA4IAjpzvkPIa
```

```
-----BEGIN CERTIFICATE-----
MIIElDCCA3ygAwIBAgIQAf2j627KdciIQ4tyS8+8kTANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0xMzAzMDgxMjAwMDBaFw0yMzAzMDgxMjAwMDBaME0xCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxJzAlBgNVBAMTHkRpZ2lDZXJ0IFNIQTIg
U2VjdXJlIFNlcnZlciBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ANyuWJBNwcQwFZA1W248ghX1LFy949v/cUP6ZCWA1O4Yok3wZtAKc24RmDYXZK83
nf36QYSvx6+M/hpzTc8zl5CilodTgyu5pnVILR1WN3vaMTIa16yrBvSqXUu3R0bd
KpPDkC55gIDvEwRqFDu1m5K+wgdlTvza/P96rtxcflUxDOg5B6TXvi/TC2rSsd9f
/ld0Uzs1gN2ujkSYs58O09rg1/RrKatEp0tYhG2SS4HD2nOLEpdIkARFdRrdNzGX
kujNVA075ME/OV4uuPNcfhCOhkEAjUVmR7ChZc6gqikJTvOX6+guqw9ypzAO+sf0
/RR3w6RbKFfCs/mC/bdFWJsCAwEAAaOCAVowggFWMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDgYDVR0PAQH/BAQDAgGGMDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYY
aHR0cDovL29jc3AuZGlnaWNlcnQuY29tMHsGA1UdHwR0MHIwN6A1oDOGMWh0dHA6
Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwwN6A1
oDOGMWh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RD
QS5jcmwwPQYDVR0gBDYwNDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8v
d3d3LmRpZ2ljZXJ0LmNvbS9DUFMwHQYDVR0OBBYEFA+AYRyCMWHVLyjnjUY4tCzh
xtniMB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA0GCSqGSIb3DQEB
CwUAA4IBAQAjPt9L0jFCpbZ+QlwaRMxp0Wi0XUvgBCFsS+JtzLHgl4+mUwnNqipl
5TlPHoOlblyYoiQm5vuh7ZPHLgLGTUq/sELfeNqzqPlt/yGFUzZgTHbO7Djc1lGA
8MXW5dRNJ2Srm8c+cftIl7gzbckTB+6WohsYFfZcTEDts8Ls/3HB40f/1LkAtDdC
2iDJ6m6K7hQGrn2iWZiIqBtvLfTyyRRfJs8sjX7tN8Cp1Tm5gr8ZDOo0rwAhaPit
c+LJMto4JQtV05od8GiG7S5BNO98pVAdvzr508EIDObtHopYJeS4d60tbvVS3bR0
j6tJLp07kzQoH3jOlOrHvdPJbRzeXDLz
-----END CERTIFICATE-----
```



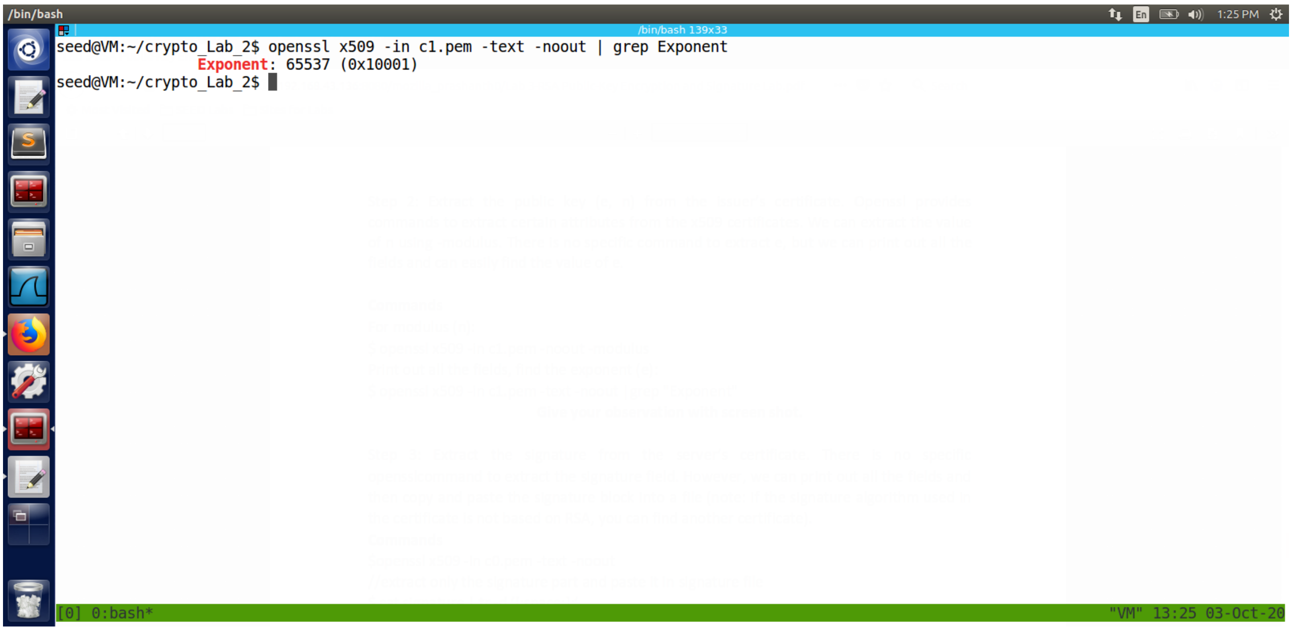
```
seed@VM:~/crypto_Lab_2$ openssl x509 -in c1.pem -noout -modulus                                                                  [50/1207]
Modulus=DCAE58904DC1C4301590355B6E3C8215F52C5CBDE3DBFF7143FA642580D4EE18A24DF066D00A736E1198361764AF379DFDFA4184AFC7AF8CFE1A734DCF339790A29
68753832BB9A675482D1D56377BDA31321AD7ACAB06F4AA5D4BB74746DD2A93C3902E798080EF13046A143BB59B92BEC207654EFCDAFCFF7AAEDC5C7E55310CE83907A4D7BE
2FD30B6AD2B1DF5FFE5774533B3580DDAE8E4498B39F0ED3DAE0D7F46B29AB44A74B58846D924B81C3DA738B129748900445751ADD37319792E8CD540D3BE4C13F395E2EB8$
35C7E108E8641008D456647B0A165CEA0AA29094EF397EBE82EAB0F72A7300EFAC7F4FD1477C3A45B2857C2B3F982FDB745589B
seed@VM:~/crypto_Lab_2$ openssl x509 -in c1.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            01:fd:a3:eb:6e:ca:75:c8:88:43:8b:72:4b:cf:bc:91
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA
        Validity
            Not Before: Mar  8 12:00:00 2013 GMT
            Not After : Mar  8 12:00:00 2023 GMT
        Subject: C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:dc:ae:58:90:4d:c1:c4:30:15:90:35:5b:6e:3c:
                    82:15:f5:2c:5c:bd:e3:db:ff:71:43:fa:64:25:80:
                    d4:ee:18:a2:4d:f0:66:d0:0a:73:6e:11:98:36:17:
                    64:af:37:9d:fd:fa:41:84:af:c7:af:8c:fe:1a:73:
                    4d:cf:33:97:90:a2:96:87:53:83:2b:b9:a6:75:48:
                    2d:1d:56:37:7b:da:31:32:1a:d7:ac:ab:06:f4:aa:
                    5d:4b:b7:47:46:dd:2a:93:c3:90:2e:79:80:80:ef:
                    13:04:6a:14:3b:b5:9b:92:be:c2:07:65:4e:fc:da:
                    fc:ff:7a:ae:dc:5c:7e:55:31:0c:e8:39:07:a4:d7:
                    be:2f:d3:0b:6a:d2:b1:df:5f:fe:57:74:53:3b:35:
                    80:dd:ae:8e:44:98:b3:9f:0e:d3:da:e0:d7:f4:6b:
[0] 0:[tmux]*                                                                                                        "VM" 13:24 03-Oct-20
```

Find Modulus ie n



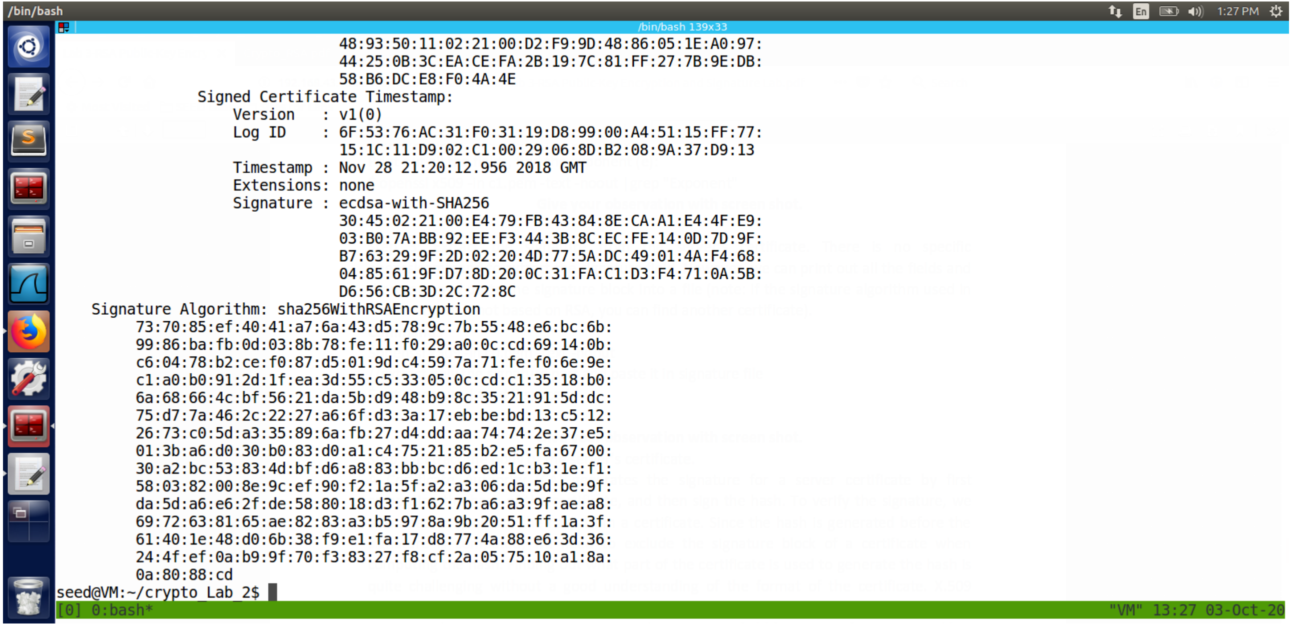
```
                    4d:cf:33:97:90:a2:96:87:53:83:2b:b9:a6:75:48:                                                      [25/1207]
                    2d:1d:56:37:7b:da:31:32:1a:d7:ac:ab:06:f4:aa:
                    5d:4b:b7:47:46:dd:2a:93:c3:90:2e:79:80:80:ef:
                    13:04:6a:14:3b:b5:9b:92:be:c2:07:65:4e:fc:da:
                    fc:ff:7a:ae:dc:5c:7e:55:31:0c:e8:39:07:a4:d7:
                    be:2f:d3:0b:6a:d2:b1:df:5f:fe:57:74:53:3b:35:
                    80:dd:ae:8e:44:98:b3:9f:0e:d3:da:e0:d7:f4:6b:
                    29:ab:44:a7:4b:58:84:6d:92:4b:81:c3:da:73:8b:
                    12:97:48:90:04:45:75:1a:dd:37:31:97:92:e8:cd:
                    54:0d:3b:e4:c1:3f:39:5e:2e:b8:f3:5c:7e:10:8e:
                    86:41:00:8d:45:66:47:b0:a1:65:ce:a0:aa:29:09:
                    4e:f3:97:eb:e8:2e:ab:0f:72:a7:30:0e:fa:c7:f4:
                    fd:14:77:c3:a4:5b:28:57:c2:b3:f9:82:fd:b7:45:
                    58:9b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            Authority Information Access:
                OCSP - URI:http://ocsp.digicert.com

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crl3.digicert.com/DigiCertGlobalRootCA.crl

                Full Name:
                  URI:http://crl4.digicert.com/DigiCertGlobalRootCA.crl

            X509v3 Certificate Policies:
[0] 0:[tmux]*                                                                                                        "VM" 13:24 03-Oct-20
```

Finding Exponent e

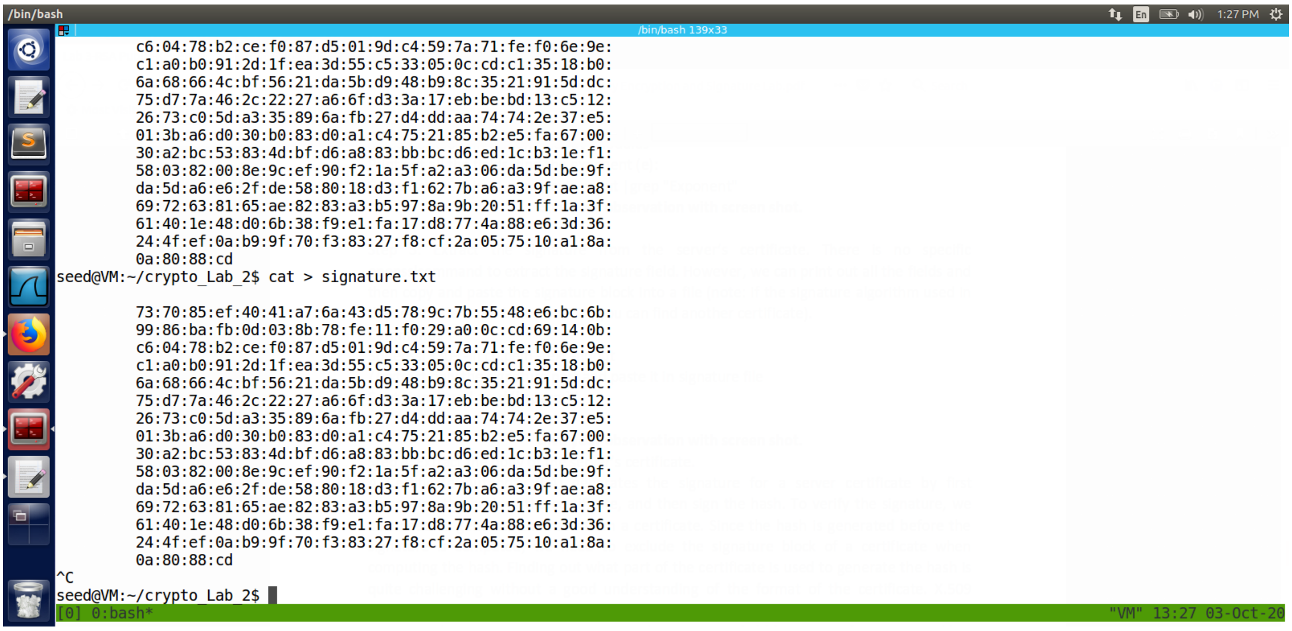


```
seed@VM:~/crypto_Lab_2$ openssl x509 -in c1.pem -text -noout | grep Exponent
                Exponent: 65537 (0x10001)
seed@VM:~/crypto_Lab_2$ 
[0] 0:bash*                                                                                                          "VM" 13:25 03-Oct-20
```

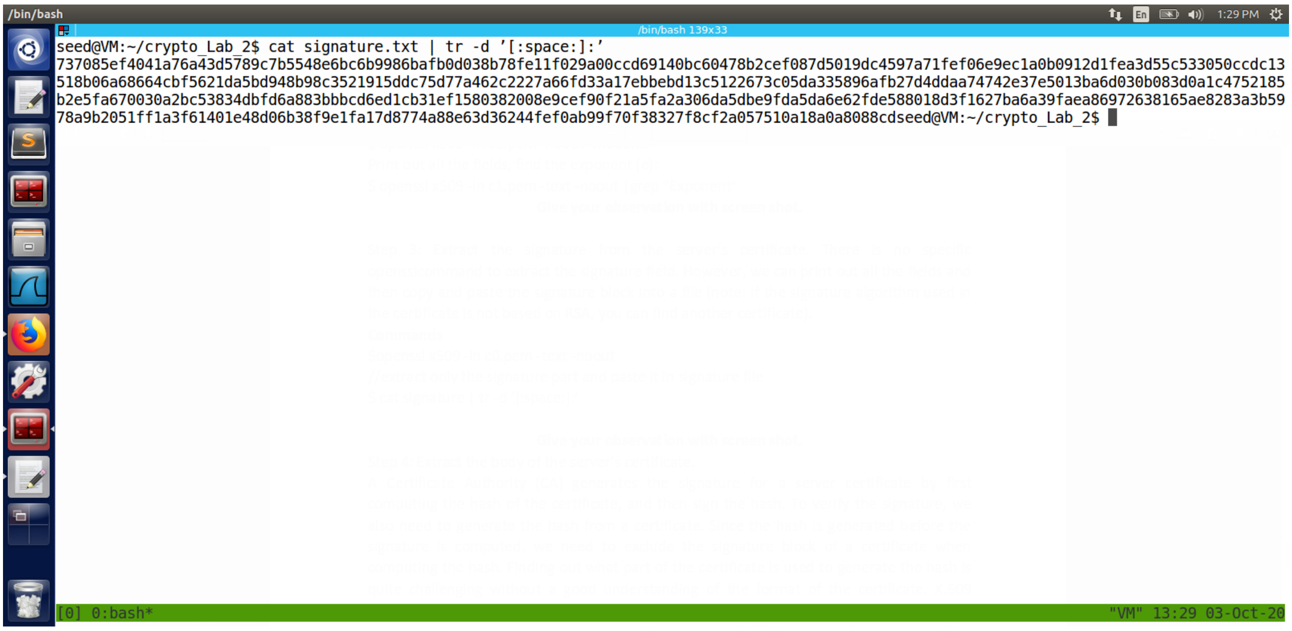
extract signature from server certificate



```
                                48:93:50:11:02:21:00:D2:F9:9D:48:86:05:1E:A0:97:
                                44:25:0B:3C:EA:CE:FA:2B:19:7C:81:FF:27:7B:9E:DB:
                                58:B6:DC:E8:F0:4A:4E
                Signed Certificate Timestamp:
                    Version   : v1(0)
                    Log ID    : 6F:53:76:AC:31:F0:31:19:D8:99:00:A4:51:15:FF:77:
                                15:1C:11:D9:02:C1:00:29:06:8D:B2:08:9A:37:D9:13
                    Timestamp : Nov 28 21:20:12.956 2018 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:45:02:21:00:E4:79:FB:43:84:8E:CA:A1:E4:4F:E9:
                                03:B0:7A:BB:92:EE:F3:44:3B:8C:EC:FE:14:0D:7D:9F:
                                B7:63:29:9F:2D:02:20:4D:77:5A:DC:49:01:4A:F4:68:
                                04:85:61:9F:D7:8D:20:0C:31:FA:C1:D3:F4:71:0A:5B:
                                D6:56:CB:3D:2C:72:8C
    Signature Algorithm: sha256WithRSAEncryption
         73:70:85:ef:40:41:a7:6a:43:d5:78:9c:7b:55:48:e6:bc:6b:
         99:86:ba:fb:0d:03:8b:78:fe:11:f0:29:a0:0c:cd:69:14:0b:
         c6:04:78:b2:ce:f0:87:d5:01:9d:c4:59:7a:71:fe:f0:6e:9e:
         c1:a0:b0:91:2d:1f:ea:3d:55:c5:33:05:0c:cd:c1:35:18:b0:
         6a:68:66:4c:bf:56:21:da:5b:d9:48:b9:8c:35:21:91:5d:dc:
         75:d7:7a:46:2c:22:27:a6:6f:d3:3a:17:eb:be:bd:13:c5:12:
         26:73:c0:5d:a3:35:89:6a:fb:27:d4:dd:aa:74:74:2e:37:e5:
         01:3b:a6:d0:30:b0:83:d0:a1:c4:75:21:85:b2:e5:fa:67:00:
         30:a2:bc:53:83:4d:bf:d6:a8:83:bb:bc:d6:ed:1c:b3:1e:f1:
         58:03:82:00:8e:9c:ef:90:f2:1a:5f:a2:a3:06:da:5d:be:9f:
         da:5d:a6:e6:2f:de:58:80:18:d3:f1:62:7b:a6:a3:9f:ae:a8:
         69:72:63:81:65:ae:82:83:a3:b5:97:8a:9b:20:51:ff:1a:3f:
         61:40:1e:48:d0:6b:38:f9:e1:fa:17:d8:77:4a:88:e6:3d:36:
         24:4f:ef:0a:b9:9f:70:f3:83:27:f8:cf:2a:05:75:10:a1:8a:
         0a:80:88:cd
seed@VM:~/crypto_Lab_2$ 
[0] 0:bash*                                                                                                          "VM" 13:27 03-Oct-20
```

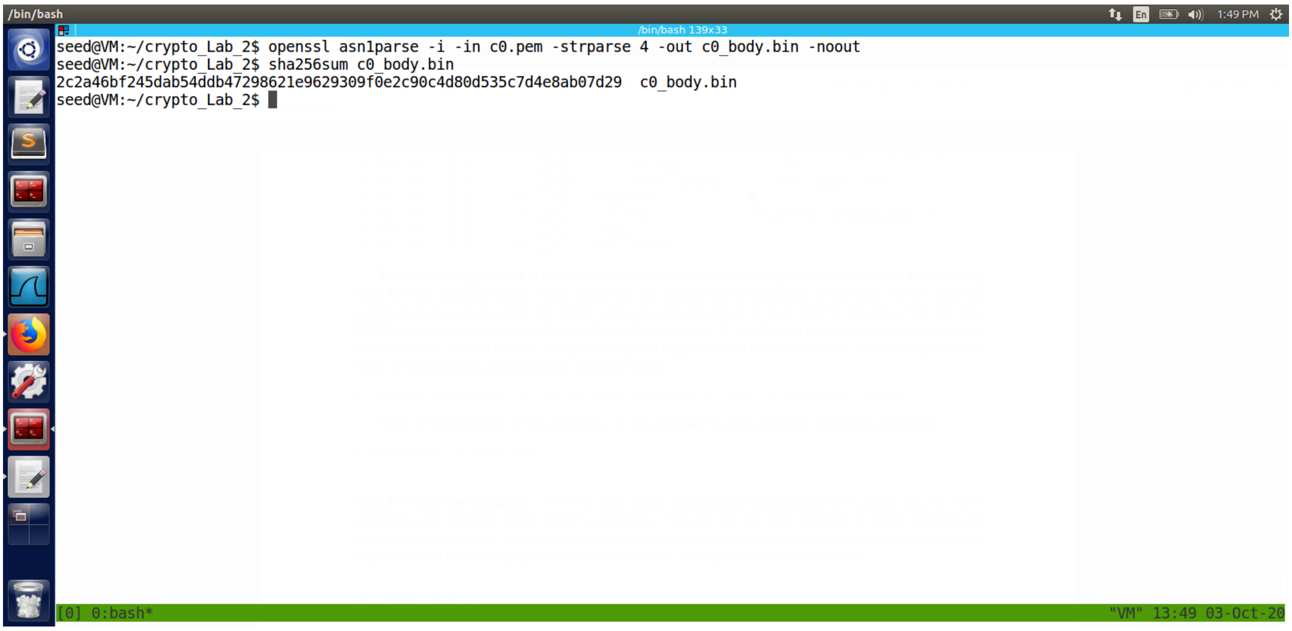


```
         c6:04:78:b2:ce:f0:87:d5:01:9d:c4:59:7a:71:fe:f0:6e:9e:
         c1:a0:b0:91:2d:1f:ea:3d:55:c5:33:05:0c:cd:c1:35:18:b0:
         6a:68:66:4c:bf:56:21:da:5b:d9:48:b9:8c:35:21:91:5d:dc:
         75:d7:7a:46:2c:22:27:a6:6f:d3:3a:17:eb:be:bd:13:c5:12:
         26:73:c0:5d:a3:35:89:6a:fb:27:d4:dd:aa:74:74:2e:37:e5:
         01:3b:a6:d0:30:b0:83:d0:a1:c4:75:21:85:b2:e5:fa:67:00:
         30:a2:bc:53:83:4d:bf:d6:a8:83:bb:bc:d6:ed:1c:b3:1e:f1:
         58:03:82:00:8e:9c:ef:90:f2:1a:5f:a2:a3:06:da:5d:be:9f:
         da:5d:a6:e6:2f:de:58:80:18:d3:f1:62:7b:a6:a3:9f:ae:a8:
         69:72:63:81:65:ae:82:83:a3:b5:97:8a:9b:20:51:ff:1a:3f:
         61:40:1e:48:d0:6b:38:f9:e1:fa:17:d8:77:4a:88:e6:3d:36:
         24:4f:ef:0a:b9:9f:70:f3:83:27:f8:cf:2a:05:75:10:a1:8a:
         0a:80:88:cd
seed@VM:~/crypto_Lab_2$ cat > signature.txt

         73:70:85:ef:40:41:a7:6a:43:d5:78:9c:7b:55:48:e6:bc:6b:
         99:86:ba:fb:0d:03:8b:78:fe:11:f0:29:a0:0c:cd:69:14:0b:
         c6:04:78:b2:ce:f0:87:d5:01:9d:c4:59:7a:71:fe:f0:6e:9e:
         c1:a0:b0:91:2d:1f:ea:3d:55:c5:33:05:0c:cd:c1:35:18:b0:
         6a:68:66:4c:bf:56:21:da:5b:d9:48:b9:8c:35:21:91:5d:dc:
         75:d7:7a:46:2c:22:27:a6:6f:d3:3a:17:eb:be:bd:13:c5:12:
         26:73:c0:5d:a3:35:89:6a:fb:27:d4:dd:aa:74:74:2e:37:e5:
         01:3b:a6:d0:30:b0:83:d0:a1:c4:75:21:85:b2:e5:fa:67:00:
         30:a2:bc:53:83:4d:bf:d6:a8:83:bb:bc:d6:ed:1c:b3:1e:f1:
         58:03:82:00:8e:9c:ef:90:f2:1a:5f:a2:a3:06:da:5d:be:9f:
         da:5d:a6:e6:2f:de:58:80:18:d3:f1:62:7b:a6:a3:9f:ae:a8:
         69:72:63:81:65:ae:82:83:a3:b5:97:8a:9b:20:51:ff:1a:3f:
         61:40:1e:48:d0:6b:38:f9:e1:fa:17:d8:77:4a:88:e6:3d:36:
         24:4f:ef:0a:b9:9f:70:f3:83:27:f8:cf:2a:05:75:10:a1:8a:
         0a:80:88:cd
^C
seed@VM:~/crypto_Lab_2$ 
[0] 0:bash*                                                                                              "VM" 13:27 03-Oct-20
```



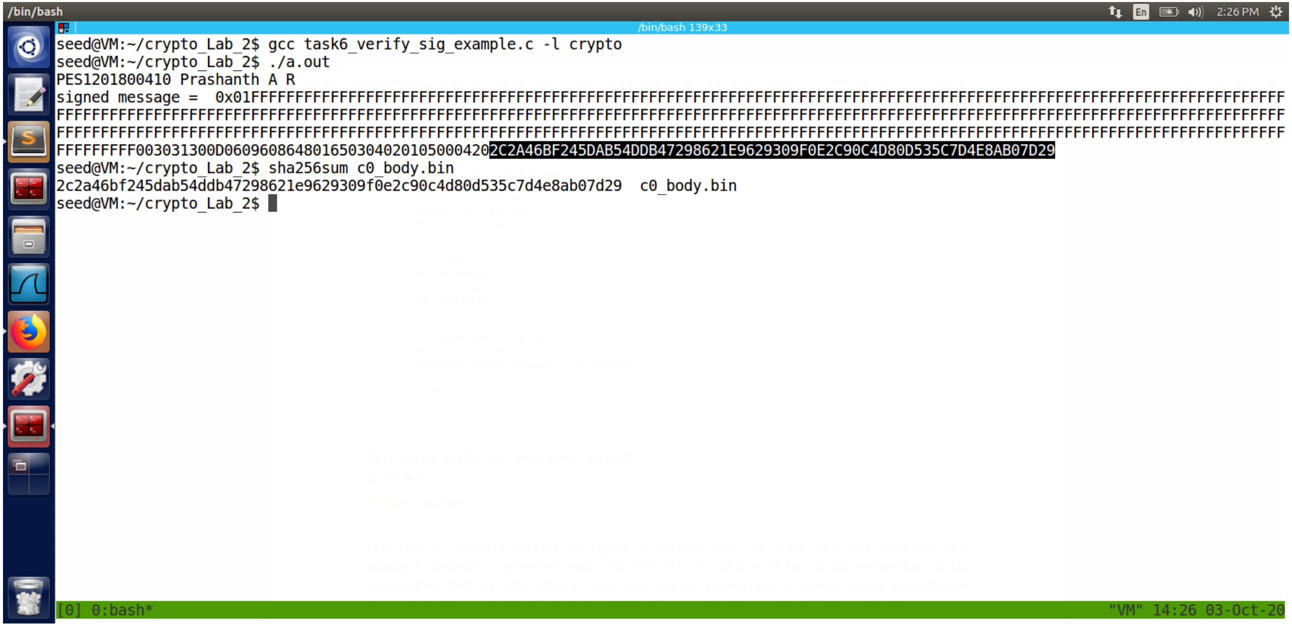
```
seed@VM:~/crypto_Lab_2$ cat signature.txt | tr -d '[:space:]:'
737085ef4041a76a43d5789c7b5548e6bc6b9986bafb0d038b78fe11f029a00ccd69140bc60478b2cef087d5019dc4597a71fef06e9ec1a0b0912d1fea3d55c533050ccdc13
518b06a68664cbf5621da5bd948b98c3521915ddc75d77a462c2227a66fd33a17ebbebd13c5122673c05da335896afb27d4ddaa74742e37e5013ba6d030b083d0a1c4752185
b2e5fa670030a2bc53834dbfd6a883bbbcd6ed1cb31ef1580382008e9cef90f21a5fa2a306da5dbe9fda5da6e62fde588018d3f1627ba6a39faea86972638165ae8283a3b59
78a9b2051ff1a3f61401e48d06b38f9e1fa17d8774a88e63d36244fef0ab99f70f38327f8cf2a057510a18a0a8088cdseed@VM:~/crypto_Lab_2$ 
[0] 0:bash*                                                                                              "VM" 13:29 03-Oct-20
```

extract signature and find sha256 checksum



```
seed@VM:~/crypto_Lab_2$ openssl asn1parse -i -in c0.pem -strparse 4 -out c0_body.bin -noout
seed@VM:~/crypto_Lab_2$ sha256sum c0_body.bin
2c2a46bf245dab54ddb47298621e9629309f0e2c90c4d80d535c7d4e8ab07d29  c0_body.bin
seed@VM:~/crypto_Lab_2$ 
[0] 0:bash*                                                                                                          "VM" 13:49 03-Oct-20
```

Verify the signature



```
seed@VM:~/crypto_Lab_2$ gcc task6_verify_sig_example.c -l crypto
seed@VM:~/crypto_Lab_2$ ./a.out
PES1201800410 Prashanth A R
signed message =  0x01FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFF003031300D0609608648016503040201050004202C2A46BF245DAB54DDB47298621E9629309F0E2C90C4D80D535C7D4E8AB07D29
seed@VM:~/crypto_Lab_2$ sha256sum c0_body.bin
2c2a46bf245dab54ddb47298621e9629309f0e2c90c4d80d535c7d4e8ab07d29  c0_body.bin
seed@VM:~/crypto_Lab_2$ 
[0] 0:bash*                                                                                                          "VM" 14:26 03-Oct-20
```

Observation:
The sha256 checksum and the calculated hash matched
hence we can say it is a valid signature .