

Crypto Lab – 4

Name: H M Mythreya

SRN: PES2UG20CS130

Task 1: A Complete Example of BIGNUM

```
[10/25/22]seed@VM:~/.../crypto$ gcc task1.c -o task1 -lcrypto
[10/25/22]seed@VM:~/.../crypto$ ./task1
a*b= 9B6946097E7EBE7F3E84D6F8E573D61A449CD7278647FF3B89A5DE0782499562FD621C5331E
D2ADE20190F587B34E93C
a^b mod n= 28E66847C606C2CF3B832EBC225043528AD640C17341BBEFF614AC74C338879F
[10/25/22]seed@VM:~/.../crypto$
```

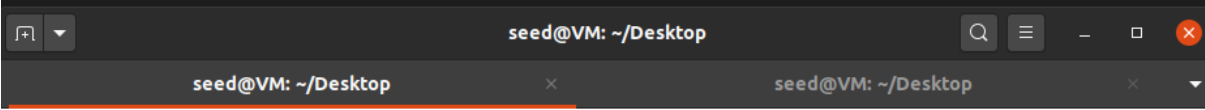
Task 2: Deriving the Private Key

```
[10/25/22]seed@VM:~/.../crypto$ gcc -o task2 task2.c -lcrypto
[10/25/22]seed@VM:~/.../crypto$ ./task2
d= 3587A24598E5F2A21DB007D89D18CC50ABA5075BA19A33890FE7C28A9B496AEB
[10/25/22]seed@VM:~/.../crypto$ █
```

Task 3: Encrypting a message

```
[10/25/22]seed@VM:~/.../crypto$ python3
Python 3.8.5 (default, Jul 28 2020, 12:59:40)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> bytes.hex(bytes("A top secret!","utf-8"))
'4120746f702073656372657421'
>>> exit()
[10/25/22]seed@VM:~/.../crypto$ gcc -o task3 task3.c -lcrypto
[10/25/22]seed@VM:~/.../crypto$ ./task3
Encrypted Message = 6FB078DA550B2650832661E14F4F8D2CFAEF475A0DF3A75CACDC5DE5CFC5FADC
Decrypted Message= 4120746F702073656372657421
[10/25/22]seed@VM:~/.../crypto$ python3
Python 3.8.5 (default, Jul 28 2020, 12:59:40)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> bytes.fromhex("4120746f702073656372657421")
b'A top secret!'
>>> exit()
[10/25/22]seed@VM:~/.../crypto$
```

Task 4: Decrypting a Message



Every 0.1s: cat /proc/sys/kernel/rando... VM: Tue Sep 27 00:32:10 2022

19

```
[10/25/22]seed@VM:~/.../crypto$ gcc -o task4 task4.c -lcrypto
[10/25/22]seed@VM:~/.../crypto$ ./task4
Decrypted Message = 50617373776F72642069732064656573
[10/25/22]seed@VM:~/.../crypto$ python3
Python 3.8.5 (default, Jul 28 2020, 12:59:40)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> bytes.fromhex("50617373776F72642069732064656573")
b'Password is dees'
>>> exit()
[10/25/22]seed@VM:~/.../crypto$ █
```

Task 5: Signing a Message

Message 1: "I owe you \$2000."

```
[10/25/22]seed@VM:~/.../crypto$ python3
Python 3.8.5 (default, Jul 28 2020, 12:59:40)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> bytes.hex(bytes("I owe you $2000.", "utf-8"))
'49206f776520796f752024323030302e'
>>> exit()
[10/25/22]seed@VM:~/.../crypto$ gcc -o task5 task5.c -lcrypto
[10/25/22]seed@VM:~/.../crypto$ ./task5
encrypted Message = 55A4E7F17F04CCFE2766E1EB32ADDBA890BBE92A6FBE2D785ED6E73CCB35E4CB
[10/25/22]seed@VM:~/.../crypto$ █
```

Message 2: "I owe \$3000"

```
[10/25/22]seed@VM:~/.../crypto$ python3
Python 3.8.5 (default, Jul 28 2020, 12:59:40)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> bytes.hex(bytes("I owe $3000", "utf-8"))
'49206f7765202433303030'
>>> exit()
[10/25/22]seed@VM:~/.../crypto$ gcc -o task5 task5.c -lcrypto
[10/25/22]seed@VM:~/.../crypto$ ./task5
encrypted Message = A57E9876B3499A03958825B1FA3A8713A7B2214E34A396755B720B2AEA8B6BB2
[10/25/22]seed@VM:~/.../crypto$
```

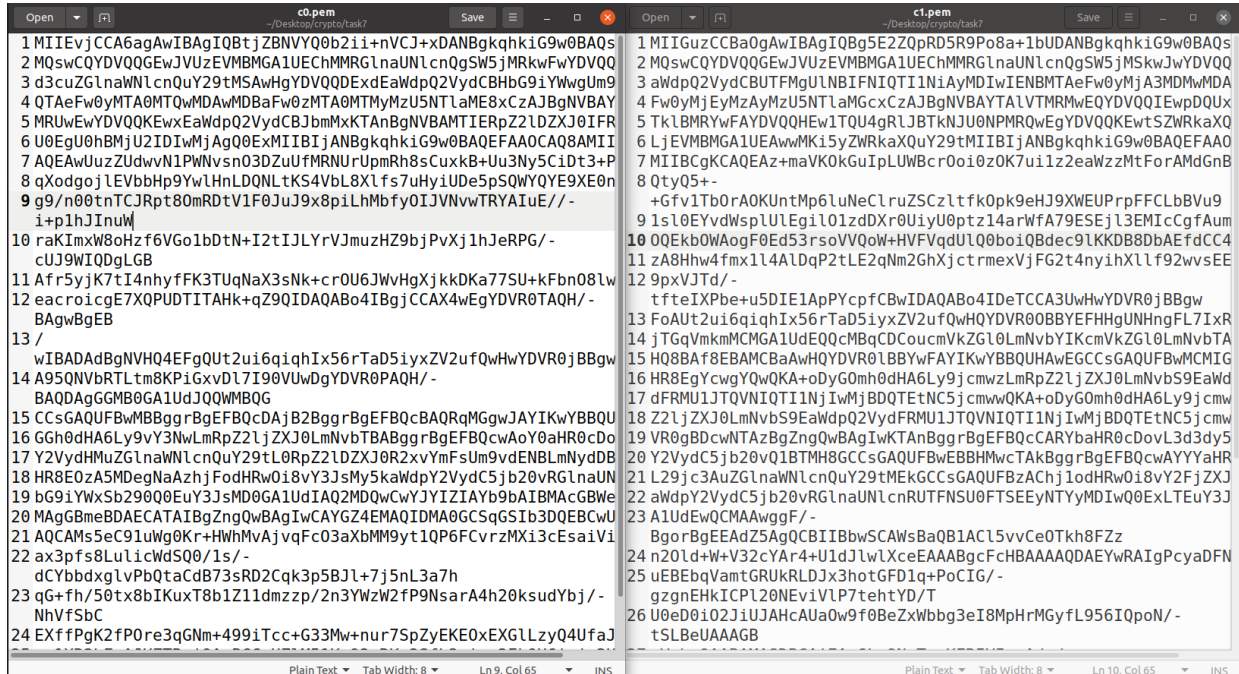
Task 6: Verifying a Signature

```
[10/25/22]seed@VM:~/.../crypto$ gcc -o task6 task6.c -lcrypto
[10/25/22]seed@VM:~/.../crypto$ ./task6
encrypted Message = 4C61756E63682061206D697373696C652E
[10/25/22]seed@VM:~/.../crypto$ python3
Python 3.8.5 (default, Jul 28 2020, 12:59:40)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> bytes.fromhex("4C61756E63682061206D697373696C652E")
b'Launch a missile.'
>>> exit()
[10/25/22]seed@VM:~/.../crypto$ █
```

Task 7: Manually verifying an X.509 Certificate

c0.pem - Server

c1.pem - Issuer



Extracting public key from issuer certificate.

```
[10/25/22] seed@VM:~/.../task7$ openssl x509 -in c1.pem -noout -modulus
Modulus=CFE99A54A3A41AE2292D458172B3A88B4CCE2BBBA2D73D9E696CF332D168AC031D1A7055F8865A4
2DC90E7EF867EFD536CEAC038A527B4CA7A96E35E0A5AEE6520B396D7E43A993D78727D5D61143EBA451422
DB055BBDD6C974118BDD5ACA655251208A53B5CDD0D7AF4522C94D29B73D786AB59F03BF444848E5DC43087
0281F0E29A7E5DF6E3901246CE580A2017411DE77AEC15550A16F8754556A754950D1BA2240175E73D94A2
8307C0DB0047DD082E39CD58C6CC0F07870E1F9B1D65E00943A8FDAD2C4DAA366D868578DCB6B99EC558C51
B6B789F28A15E595FF76C2FB04106459F17F69C5525377FB5FB5E2173DB7BEBB90C81350293D87297C207
[10/25/22] seed@VM:~/.../task7$ openssl x509 -in c1.pem -text -noout | grep "Exponent"
    Exponent: 65537 (0x10001)
[10/25/22] seed@VM:~/.../task7$
```

Extracting signature from server certificate.

```
[10/25/22] seed@VM:~/.../task7$ cat signature.txt | tr -d '[:space:]'
8032ce5e0bdd6e5a0d0aafe1d684cbc08efa8570edda5db30cf72b7540fe850afaf33178b7704b1a
8958ba80bdf36b1de97ecf0bba589c59d490d3fd6cfdd0986db771825bcf6d0b5a09d07bdec443d8
2aa4de9e41265fbb8f99cbddae1a86f9f87fe74b71f1b20abb14fc6f5675d5d9b3ce9ff69f7616c
d6d9f3fd36c6ab038876d24b2e7586e3fcd8557d26c21177df3e02b67cf3ab7b7a86366fb8f7d893
71cf86df7330fa7babad2a59c842843b11171a52f3c90e147da25b7267ba71ed574766c5b8024a65
345e8bd02a3c209c51994ce7529ef76b112b0d927e1de88aeb36164387ea2a63bf753febdec403bb
0a3cf730efebaf4cfc8b3610733ef3a4[10/25/22] seed@VM:~/.../task7$
```

Extracting body of the server's certificate

```
[10/25/22] seed@VM:~/.../task7$ openssl asn1parse -i -in c0.pem -strparse 4 -out c0_body.bin -noout
[10/25/22] seed@VM:~/.../task7$ sha256sum c0_body.bin
3689022b62bd20e807ccc1f32720ab2a9eeb0712e84cc373464b29cc436def97  c0_body.bin
[10/25/22] seed@VM:~/.../task7$ █
```

Verifying the signature.

```
[10/25/22] seed@VM:~/.../task7$ gcc task7.c -lcrypto
[10/25/22] seed@VM:~/.../task7$ ./a.out
encrypted Message = BA86138B5EDD2E7415BE976B7E0116215B5A77F45971B213FA783EBA232
BF6520D00F0965705275EB49F6810A4FD82A25CC2CFF5AC161D51F234F3C8572DF4BB7B3CC6630A4
9095637F099154D830272EB43D971E31718FBDC8766EBB3BBED146A10A13C509D8347FBE8C3D6EEA
2DB305521C874645E4DC73468DF3ACE399260117048642821578B17DA75B6B5493EE7765FA118FF7
F3408B6508F149FBF81C32D0B947F2AE4D260360940D47FCD22F7C1D23D2E54B95F3C1FC64504794
7CADCB23D65DB78600A0D885802C8392429E76586D4E6583B9C6752A80BF076C62273AD9AA606BF9
1FF0D6FC901E38FB16F826D3A92B27F143B166643B76511DE7140
[10/25/22] seed@VM:~/.../task7$ █
```