

# Lab 08 Template

Some questions require multiple parts to be answered, be sure to discuss them in full.

Part 01:

1.

Screenshot of the output from

```
openssl rsa -text -in <netid>_private_key.pem
```

(10 points)

Private-Key: (2048 bit, 2 primes)

modulus:

00:a5:89:b8:dc:cd:e0:2b:eb:17:0f:0a:a5:aa:ce:  
bf:43:26:52:fc:90:c9:12:87:94:b4:93:94:4e:78:  
91:fb:a4:08:c4:10:b4:a0:46:cb:79:2b:79:19:4f:  
2b:51:13:4e:00:d4:8a:12:e8:d0:7c:bc:7d:b5:25:  
7a:87:cd:1f:cd:b5:98:7f:8b:98:87:b6:b7:df:f5:  
fa:a8:4b:07:f5:c1:02:1c:aa:6c:c4:ac:7f:0a:ab:  
12:84:54:4b:a7:61:87:20:f4:60:84:bf:30:9c:b9:  
83:a6:2a:35:be:35:75:a0:11:d5:10:51:6c:fd:03:  
e7:c0:4d:3c:71:1d:a7:7a:43:68:83:ea:10:17:77:  
3d:2f:e7:72:6f:ec:30:0b:e6:f4:35:36:c7:38:b9:  
aa:3a:8e:d8:71:15:79:81:4b:b7:e8:d7:fa:d1:bc:  
52:f0:9d:e3:2d:ca:4d:11:80:70:b7:04:5e:56:a7:  
ea:3a:43:81:aa:f9:68:28:0e:6f:45:44:6a:9a:f3:  
40:5d:b6:96:e4:a1:86:4a:c4:52:3e:80:93:42:a1:  
61:bd:ac:ef:a6:16:92:52:85:8a:e0:b9:8e:2f:6c:  
d1:b4:33:17:26:8e:ae:c9:42:be:48:ec:e2:a0:c8:  
17:4f:94:9f:d3:2a:fb:00:d3:e7:6a:17:df:1d:71:  
96:b7

publicExponent: 65537 (0x10001)

privateExponent:

3d:29:f8:f3:24:e2:9a:77:9f:aa:80:1d:9c:52:0d:  
db:6a:d2:a8:dd:7a:5d:ed:58:a5:ac:0d:d5:3c:b9:  
7b:c8:2d:30:fc:97:30:cd:57:ab:2a:c3:f0:f5:0e:  
a5:43:43:c4:0c:c4:03:9e:a0:42:26:87:30:22:6b:

:

privateExponent:

3d:29:f8:f3:24:e2:9a:77:9f:aa:80:1d:9c:52:0d:  
db:6a:d2:a8:dd:7a:5d:ed:58:a5:ac:0d:d5:3c:b9:  
7b:c8:2d:30:fc:97:30:cd:57:ab:2a:c3:f0:f5:0e:  
a5:43:43:c4:0c:c4:03:9e:a0:42:26:87:30:22:6b:  
f6:b7:74:f3:d6:10:45:b8:37:a0:95:83:b5:2d:b6:  
f2:ed:de:40:10:93:8e:31:ee:44:71:13:f3:c6:27:  
ee:5b:13:25:02:65:22:69:09:2c:a3:53:fb:e4:93:  
df:16:a3:8a:e7:47:d1:e0:24:e0:85:a5:86:8b:25:  
db:28:ee:97:41:04:bb:a8:89:9b:41:07:0c:15:58:  
fc:9d:3b:5c:de:52:c2:f5:08:88:ba:ed:d3:cb:92:  
6b:cf:7b:79:38:92:ef:5d:ca:eb:8c:f1:1d:b6:33:  
ed:21:9b:9e:64:03:3d:f6:7b:cd:a2:90:45:f4:1f:  
69:6e:60:77:8c:fa:32:89:05:eb:56:79:eb:b4:07:  
40:16:a9:40:67:fa:19:9f:d4:49:72:6d:9c:54:bb:  
42:15:8a:e5:57:b8:87:80:52:ee:6e:24:58:0b:3c:  
1a:6b:eb:d9:b6:ce:31:7e:25:52:46:66:c6:86:f8:  
33:19:62:f2:63:c1:cc:e6:57:68:95:74:0d:4f:fe:  
99

prime1:

00:ba:73:e3:56:f9:b9:7e:d1:c7:ab:d2:37:37:ac:  
a1:f2:16:23:f0:4c:cd:02:1a:87:83:82:3a:82:57:  
77:43:7a:5d:21:e9:4d:e3:81:f1:26:80:1d:6a:01:  
a3:3a:dd:92:e7:aa:a5:70:65:6b:ec:50:62:ff:8e:  
24:c0:94:cc:8d:84:3c:a7:94:e4:a7:ab:7b:b1:8d:  
99:14:50:db:52:31:05:24:35:fc:1d:c2:da:3b:88:

:

prime1:

00:ba:73:e3:56:f9:b9:7e:d1:c7:ab:d2:37:37:ac:  
a1:f2:16:23:f0:4c:cd:02:1a:87:83:82:3a:82:57:  
77:43:7a:5d:21:e9:4d:e3:81:f1:26:80:1d:6a:01:  
a3:3a:dd:92:e7:aa:a5:70:65:6b:ec:50:62:ff:8e:  
24:c0:94:cc:8d:84:3c:a7:94:e4:a7:ab:7b:b1:8d:  
99:14:50:db:52:31:05:24:35:fc:1d:c2:da:3b:88:  
7a:d7:90:b4:05:10:74:d3:1b:e1:a3:51:8b:5a:e2:  
e4:08:ec:18:30:2e:43:92:a0:a4:1c:11:b5:30:f6:  
5c:64:32:63:32:b8:48:ac:85

prime2:

00:e3:48:b7:8b:e8:c8:35:89:03:22:fb:70:f4:41:  
b6:68:93:a5:4c:2d:97:de:09:be:74:cc:d0:28:c7:  
3a:65:ae:17:c2:85:2a:fa:bc:49:d6:c7:d5:92:5d:  
d0:66:4c:a7:0d:c5:7e:96:3b:7f:82:6e:49:f9:da:  
c2:46:a0:2e:e7:5f:93:64:86:a9:63:2c:ff:88:b5:  
a9:df:af:da:fd:a7:69:4f:1a:43:30:59:6c:76:c4:  
5d:bf:ca:43:b0:c8:f5:b0:32:6c:e4:f7:6a:f4:7e:  
d0:64:04:7b:e1:a9:96:f5:6c:08:b1:37:ad:cc:25:  
f9:3c:e2:15:bd:09:b3:89:0b

exponent1:

00:90:6a:3c:76:dc:7b:d1:7f:98:c1:3b:d4:6a:f9:  
fa:81:70:a6:ab:74:41:01:d5:1c:8b:3e:ae:24:d0:  
ac:5e:86:83:66:45:b7:7f:74:e1:1c:a9:f4:9e:6b:  
e0:4b:32:dd:9b:34:70:69:ab:14:b9:77:d6:06:0c:

:  
:

exponent1:

00:90:6a:3c:76:dc:7b:d1:7f:98:c1:3b:d4:6a:f9:  
fa:81:70:a6:ab:74:41:01:d5:1c:8b:3e:ae:24:d0:  
ac:5e:86:83:66:45:b7:7f:74:e1:1c:a9:f4:9e:6b:  
e0:4b:32:dd:9b:34:70:69:ab:14:b9:77:d6:06:0c:  
c9:e8:a4:17:ff:b0:a1:ee:47:04:07:de:69:b3:2f:  
72:96:ea:bd:c5:5e:94:95:e4:7e:7f:6a:b1:ef:94:  
99:59:28:0a:57:35:d4:d6:c2:ec:b4:bb:ef:4d:19:  
19:f8:d3:2d:34:fc:50:78:5c:96:5f:eb:53:45:36:  
3c:7f:9b:0b:7c:78:82:49:a5

exponent2:

00:9b:af:c7:ea:d2:7d:b2:0e:34:53:d6:20:bd:6f:  
f5:df:14:a3:f9:d6:91:5c:cb:17:e7:32:14:b4:9a:  
23:ea:5a:a2:73:e0:7c:5c:5c:75:c7:e6:02:e9:cb:  
d1:61:01:c8:bc:aa:37:d7:f8:d1:93:2a:b1:09:b1:  
4b:ba:cd:26:d3:de:a8:3c:07:f2:27:b9:3f:21:0a:  
2f:5e:c6:3b:1f:dd:79:49:72:17:ec:1a:95:2d:95:  
bd:12:0f:1e:e7:0e:01:1d:bc:ac:d2:fa:98:0c:fa:  
81:0c:c1:f5:89:d2:7d:51:87:bb:3c:89:83:47:80:  
0b:86:24:e7:f7:21:9a:15:99

coefficient:

4c:95:87:44:cb:92:cc:b7:d6:05:89:a5:5f:c5:09:  
cc:88:6b:35:33:35:48:a6:83:a3:53:55:c3:43:15:  
40:26:4b:c9:33:c1:de:48:82:c5:e2:9d:e5:06:94:  
25:e3:3e:59:e8:ba:02:37:99:32:32:18:88:23:70:  
65:7a:1c:23:7f:37:15:f0:86:6e:f7:34:37:37:91:

:



coefficient:

4c:95:87:44:cb:92:cc:b7:d6:05:89:a5:5f:c5:09:  
cc:88:6b:35:33:35:48:a6:83:a3:53:55:c3:43:15:  
40:26:4b:c9:33:c1:de:48:82:c5:e2:9d:e5:06:94:  
25:e3:3e:59:e8:ba:02:37:99:32:32:18:88:23:70:  
65:7a:1c:23:7f:37:15:f0:86:6e:f7:34:37:37:91:  
c2:16:70:bc:cc:5b:4f:5b:87:5e:63:83:84:18:1b:  
01:db:ac:c7:3b:0c:a1:70:78:e4:aa:af:8d:e9:94:  
13:98:8c:77:3d:1a:ba:a7:53:9d:13:40:05:5f:c5:  
49:b2:5c:15:c5:cb:5b:9d

-----BEGIN PRIVATE KEY-----

MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAKgwggSkAgEAAoIBAQClibjczeAr6xcP  
CqWqzr9DJLL8kMkSh5S0k5R0eJH7pAJEELSgRst5K3kZTytRE04A1IoS6NB8vH21  
JXqHzR/NtZh/i5iHtrff9fqoS wf1wQIcq mZE rH8KqxKEVEunYYcg9GCEvzCcuY0m  
KjW+NXWgEdUQUWz9A+fATTxxHad6Q2iD6hAXdz0v53Jv7DAL5vQ1Nsc4uao6jthx  
FXmBS7fo1/rRvFLwneMtyk0RgHC3BF5Wp+o6Q4Gq+WgoDm9FRGqa80BdtpbkoYZK  
xFI+gJNCoWG9r0+mFpJShYrguY4vbNG0Mxcmjq7JQr5I70KgyBdPLJ/TKvsA0+dq  
F98dcZa3AgMBAAECggEAPSn48yTimnefqoAdnFIN22rSqN16Xe1YpawN1Ty5e8gt  
MPyXMM1XqyrD8PUOpUNDxAzEA56gQiaHMCJr9rd089YQRbg3oJWDtS228u3eQBCT  
jjHuRHET88Yn7lsTJQJlImkJLKNT++ST3xajiudH0eAk4Iwlhosl2yju10EEu6iJ  
m0EHDBVY/J07XN5SwvUIiLrt08uSa897eTiS713K64zxHbYz7SGbnmQDPfZ7zaKQ  
RfQfaW5gd4z6MokF61Z567QHQBapQGf6GZ/USXJtnFS7QhWK5Ve4h4BS7m4kWA s8  
Gmvr2bb0MX4lUkZmxob4Mxli8mPBzOZXaJV0DU/+mQKBgQC6c+NW+bl+0cer0jc3  
rKHyFiPwTM0CGoeDgj qCV3dDel0h6U3jgfEmgB1qAaM63ZLnqqVwZWvsUGL/jiT  
A lMyNhDynlOSnq3uxjZkUUNTSMQUknfwdwto7iHrXkLQFEHTTG+GjUYta4uQI7Bgw  
LkOSoKQcEbUw9lxkMmMyuEishQKBgQDjSLeL6Mg1iQMl+3D0QbZok6VMLZfeCb50  
:

```
CqWqzr9DJLL8kMkSh5S0k5R0eJH7pAjEELSgRst5K3kZTytrE04A1IoS6NB8vH21
JXqHzR/NtZh/i5iHtrff9fgoSwf1wQIcqmzErH8KqxKEVEunYYcg9GCEvzCcuY0m
KjW+NXWgEdUQUWz9A+fATTxxHad6Q2iD6hAXdz0v53Jv7DAL5vQ1Nsc4uao6jthx
FXmBS7fo1/rRvFLWneMtyk0RgHC3BF5Wp+o6Q4Gq+WgoDm9FRGqa80BdtpbkoYZK
xFI+gJNCowG9rO+mFpJShYrguY4vbNG0MxcmjQ7JQr5I7OKgyBdPlJ/TKvsA0+dq
F98dcZa3AgMBAAECggEAPSn48yTimnefgoAdnFIN22rSqN16Xe1YpawN1Ty5e8gt
MPyXMM1XqyrD8PUOpUNDxAzEA56gQiaHMCJr9rd089YQRbg3oJWDtS228u3eQBCT
jjHuRHET88Yn7lsTJQJLImkJLKNT++ST3xajiudH0eAk4IwLhosl2yjuL0EEu6iJ
m0EHDBVY/J07XN5SwvUIiLrt08uSa897eTiS713K64zxHbYz7SGbnmQDPfZ7zaKQ
RfQfaW5gd4z6MokF61Z567QHQBapQGf6GZ/USXJtnFS7QhWK5Ve4h4BS7m4kWas8
Gmvr2bb0MX4lUkZmxob4Mxli8mPBzOZXaJV0DU/+mQKBgQC6c+NW+bl+0cer0jc3
rKHfFiPwTM0CGoeDgjQCV3dDel0h6U3jgfEmgB1qAaM63ZLnqqVwZWvsUGL/jiTA
lMyNhDynl0Ssq3uxjZkUUNTSMQUkNfwdwto7iHrXkLQFEHTTG+GjUYta4uQI7Bgw
Lk0SoKQcEbUw9lxkMmMyuEishQKBgQDjSLeL6Mg1iQMi+3D0QbZok6VMLZfeCb50
zNAoxzplrhfChSr6vEnWx9WSXdBmTKcNxx6W03+Cbkn52sJGoC7nX5NkhqljLP+I
tanfr9r9p2lPGkMwWwX2xF2/yk0WypWwMmzk92r0ftBkBVhVhQZb1bAixN63MJfk8
4hW9Cb0JCwKBgQCQajx23HvRf5jB09Rq+fQbCKardEEB1RyLPq4k0KxehoNmRbd/
d0EcqfSea+BLMt2bNHBpqxS5d9YGDmnopBF/sKHuRwQH3mmzL3KW6r3FXpSV5H5/
arHvLJLZKApXNdTWwuy0u+9NGRn40y00/FB4XJZf61NFnjx/mwt8eIJJpQKBgQCb
r8fq0n2yDjRT1iC9b/XfFKP51pFcyxfnMhS0miPqWqJz4HxcXHXH5gLPy9FhAc18
qjfX+NGTKrEJsUu6zSbT3qg8B/InuT8hCi9exjsf3XlJchfsGpUtlb0SDx7nDgEd
vKzS+pgM+oEMwfWJ0n1Rh7s8iYNHgAuGJO3IZoVmQKBgEyVh0TLksy31gWJpV/F
CcyIazUzNUimg6NTVcNDFUAmS8kzwd5IgsXineUGLCXjPlnougI3mTIyGIgjcGV6
HCN/NxxWhm73NDc3kcIWcLzMW09bh15jg4QYGwHbrMc7DKFwe0Sqr43plBOYjHc9
GrqnU50TQAVfxUmyXBxFy1ud
-----END PRIVATE KEY-----
(END)
```

2. Comparison of the same/different values observed across the extra generated keys

i. Which values are constant?

The key size and public exponent are constant.

ii. Which ones vary?

The modulus, private exponent, prime factors, and exponents change.

iii. What do these values represent?

Modulus: Product of two large primes.

Private exponent: A value found using  $e$  and  $(p-1)(q-1)$  used for decryption.

Prime numbers: Two large numbers randomly chosen.

Public exponent: A fixed value for encryption.

(15 points, 5 points each question)

3.

Discussion of the differences between FTP and SFTP.

i. Why would you want one over the other?



SFTP encrypts data while FTP does not. This is helpful to avoid data theft. SFTP also supports public key authentication therefore it is more secure than FTP's username/password. FTP is more vulnerable to attacks over SFTP.

ii. Why did we need to specify our private key?

SFTP needs private key authentication for logging in. Private key proves we are the owner of the public key stored on the server.

iii. What protection does this offer?

Since we do not use passwords attackers cannot steal credentials via brute force and this prevents password attacks. It ensures identity verification as only users with the correct private key can access the system.

(15 points, 5 points each question)

4.

Screenshot of the five messages [netid]1.txt, [netid]2.txt, ... [netid]5.txt

(10 points)

```
cp3310@cp3310:~/homework/Lab08/teja$ openssl dgst -sha256 -verify lab08_public_key.pem -signature sig.txt.sha256 teja1.txt 2>/dev/null
Verification failure
cp3310@cp3310:~/homework/Lab08/teja$ openssl dgst -sha256 -verify lab08_public_key.pem -signature sig.txt.sha256 teja2.txt 2>/dev/null
Verification failure
cp3310@cp3310:~/homework/Lab08/teja$ openssl dgst -sha256 -verify lab08_public_key.pem -signature sig.txt.sha256 teja3.txt 2>/dev/null
Verified OK
cp3310@cp3310:~/homework/Lab08/teja$ openssl dgst -sha256 -verify lab08_public_key.pem -signature sig.txt.sha256 teja4.txt 2>/dev/null
Verification failure
cp3310@cp3310:~/homework/Lab08/teja$ openssl dgst -sha256 -verify lab08_public_key.pem -signature sig.txt.sha256 teja5.txt 2>/dev/null
Verification failure
cp3310@cp3310:~/homework/Lab08/teja$
```

5.

## Discussion on hash verification

i.

What is known about the message?

The authentic message was not modified since it was signed. The rest of 4 messages were tampered with breaking the verification.

ii.

What is the message protected against and what is it vulnerable to?

It is protected against tampering and impersonation. Tampering is changes to the message that will cause the hash to change which in turn will lead to verification failure. Impersonation will be that only the CA/ trusted source with the private key can generate a valid signature.

It is vulnerable to compromises in the key and man in the middle attacks. If the private key is stolen then the attacker can forge a valid signature.

(10 points, 5 points each question)

6.

Discussion on what the message generated in step 8e protected against

and what it is vulnerable to (compared to the message we downloaded in

step 6).

Step 6 protects authenticity and integrity but not confidentiality while this step protects confidentiality but not authenticity or integrity.

In step 6: Sender's identity is proved by signature, signature ensures no tampering occurred, and prevents modification.

In this step: Anyone can encrypt with a public key, the encrypted message could be altered, only the private key holder can decrypt, and man in the middle could replace the encrypted message.

(10 points, 5 points each part)

7.

Screenshot of the signed certificate ([netid]\_certificate.pem) when looked

at through openssl

(10 points)

```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 72 (0x48)
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C = US, ST = Iowa, L = Ames, O = 3310.com, OU = homework, CN = certs.homework.3310.com, emailAddress = certs@homework.3310.com
  Validity
    Not Before: Mar 30 21:34:01 2025 GMT
    Not After : Mar 30 21:34:01 2026 GMT
  Subject: C = US, ST = Iowa, O = 3310.com, OU = homework, CN = tejal.homework.3310.com, emailAddress = tejal@homework.3310.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:a5:89:b8:dc:cd:e0:2b:eb:17:0f:0a:a5:aa:ce:
      bf:43:26:52:fc:90:c9:12:87:94:b4:93:94:4e:78:
      91:fb:a4:08:c4:10:b4:a0:46:cb:79:2b:79:19:4f:
      2b:51:13:4e:00:d4:8a:12:e8:d0:7c:bc:7d:b5:25:
      7a:87:cd:1f:cd:b5:98:7f:8b:98:87:b6:b7:df:f5:
      fa:a8:4b:07:f5:c1:02:1c:aa:6c:c4:ac:7f:0a:ab:
      12:84:54:4b:a7:61:87:20:f4:60:84:bf:30:9c:b9:
      83:a6:2a:35:be:35:75:a0:11:d5:10:51:6c:fd:03:
      e7:c0:4d:3c:71:1d:a7:7a:43:68:83:ea:10:17:77:
      3d:2f:e7:72:6f:ec:30:0b:e0:f4:35:36:c7:38:b9:
      aa:3a:8e:d8:71:15:79:81:4b:b7:e8:d7:fa:d1:bc:
      52:f0:9d:e3:2d:ca:4d:11:80:70:b7:04:5e:56:a7:
```

```

bf:43:26:52:fc:90:c9:12:87:94:b4:93:94:4e:78:
91:fb:a4:08:c4:10:b4:a0:46:cb:79:2b:79:19:4f:
2b:51:13:4e:00:d4:8a:12:e8:d0:7c:bc:7d:b5:25:
7a:87:cd:1f:cd:b5:98:7f:8b:98:87:b6:b7:df:f5:
fa:a8:4b:07:f5:c1:02:1c:aa:6c:c4:ac:7f:0a:ab:
12:84:54:4b:a7:61:87:20:f4:60:84:bf:30:9c:b9:
83:a6:2a:35:be:35:75:a0:11:d5:10:51:6c:fd:03:
e7:c0:4d:3c:71:1d:a7:7a:43:68:83:ea:10:17:77:
3d:2f:e7:72:6f:ec:30:0b:e6:f4:35:36:c7:38:b9:
aa:3a:8e:d8:71:15:79:81:4b:b7:e8:d7:fa:d1:bc:
52:f0:9d:e3:2d:ca:4d:11:80:70:b7:04:5e:56:a7:
ea:3a:43:81:aa:f9:68:28:0e:6f:45:44:6a:9a:f3:
40:5d:b6:96:e4:a1:86:4a:c4:52:3e:80:93:42:a1:
61:bd:ac:ef:a6:16:92:52:85:8a:e0:b9:8e:2f:6c:
d1:b4:33:17:26:8e:ae:c9:42:be:48:ec:e2:a0:c8:
17:4f:94:9f:d3:2a:fb:00:d3:e7:6a:17:df:1d:71:
96:b7
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
78:56:CE:E4:F1:6F:FD:79:EB:96:05:D0:7A:11:43:47:EF:2A:F5:0B
X509v3 Authority Key Identifier:

```

```

X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
78:56:CE:E4:F1:6F:FD:79:EB:96:05:D0:7A:11:43:47:EF:2A:F5:0B
X509v3 Authority Key Identifier:
3F:DB:00:BB:9C:2C:CC:94:9E:44:5E:AA:90:0B:DD:41:60:44:46:80
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
78:51:28:51:e5:b9:c3:04:84:83:56:c9:3d:6b:cb:c5:50:9b:
d3:81:f7:89:d3:c1:b6:04:ef:f1:e8:fe:61:9d:ae:d0:45:5e:
b7:91:03:fc:c8:52:5f:fc:a5:a2:37:53:a6:9b:96:13:6f:b9:
53:7b:3f:91:da:9c:49:fa:dd:00:a4:5e:fc:30:8e:12:ac:bf:
1a:2f:5c:f7:c5:3f:19:a8:9d:de:42:70:ec:ca:b4:d0:e8:55:
1f:2d:4b:0a:41:82:42:a8:45:03:e9:9b:6a:5a:50:94:72:e6:
cd:7f:aa:e4:9f:ce:1d:3e:d8:bb:6d:56:04:82:7c:8d:3a:2d:
e0:05:c9:c7:d1:11:36:96:bb:75:22:4d:3d:21:9e:5d:1e:d4:
3e:b6:b7:e2:14:9c:60:97:e9:2c:1f:51:4a:7a:73:0f:ed:ff:
ee:0b:92:31:70:7b:14:82:ed:c2:95:35:f2:b1:ce:0c:51:58:
cd:0f:51:d7:61:c2:f9:a8:8c:5f:41:3c:14:28:ba:3d:08:f7:
ec:41:d2:56:7b:61:82:b3:cc:75:77:1f:ea:93:2b:8d:15:46:
81:a4:50:4d:69:8a:7f:45:45:3b:25:61:a6:e7:bb:61:d3:8a:
f0:c0:ee:a0:ed:1a:1a:be:74:6b:8e:08:75:60:ac:e1:5a:32:
9c:35:0f:0c

```

(END)

8.

Discussion from step 12



i.

Do any parts of the certificate match with your private key? If so, why?

Yes, parts of the certificate match with the private key because the certificate contains the public key that corresponds to the private key used to generate the Certificate Signing Request. The certificate is signed using the Certificate Authority private key, which ensures that it can be validated against the CA's public key. The private key is not included in the certificate itself but the key pair remains linked.

ii.

What was happening during the Certificate Signing process?

Why did you need to submit it for signing?

(20 points, 10 points each answer, 10 points each why)

First we generate the CSR that contains the public key and write in our information like organization name. We prove we have control over the key when we request this using our private key. Then we submit the CSR. The certificate is signed digitally using the private key and can be validated by anyone with CA's public key.

Self signed certificates are not trusted by default. The CA signed certificate ensures that the certificate is authentic and issued by a trusted entity. Modifications will break the signature. It also enables secure encrypted communication.