1) Part 1:
   a. **Screenshot of key (step 4c).** (10 points)

```
RSA Private-Key: (2048 bit, 2 primes)
modulus:
    00:b3:d1:d0:d3:3a:5f:d6:e7:93:49:22:43:40:dc:
    d2:84:9e:12:34:b3:31:a4:8e:eb:89:05:51:42:ce:
    50:3d:76:68:87:35:af:16:81:70:42:44:b0:71:66:
    ab:20:98:b0:71:ed:ed:4f:47:81:02:66:53:05:7f:
    48:09:1d:ab:df:a9:91:9e:37:dc:4a:0e:70:0d:fd:
    50:b5:37:f4:c8:33:ee:e3:7a:d6:45:90:68:51:30:
    8a:e0:75:1d:3f:c3:df:db:c4:9d:5c:d1:87:e3:a4:
    62:72:67:75:10:77:dd:16:c1:5c:e2:e5:77:f9:f3:
    f1:32:0a:ea:53:86:9a:79:9e:cd:8a:79:17:9d:73:
    8c:99:0a:96:01:d9:a5:88:d0:98:61:df:a8:fa:c6:
    fb:77:ba:1f:28:cd:04:59:b2:f4:16:56:e7:0a:ae:
    10:80:23:f3:bc:fe:86:7a:99:3a:3b:20:fa:0f:ec:
    1a:f1:9f:7c:2c:1a:ed:3b:45:a3:e4:9e:de:af:aa:
    be:22:7a:0b:1c:7d:38:9b:12:dc:96:26:c3:9a:79:
    b4:52:4e:4f:2d:fc:90:33:ed:62:d8:b5:fe:2e:ac:
    50:24:68:7f:6c:7c:94:98:0e:9e:0b:b3:d2:c0:ad:
    7d:27:e7:bd:4b:e1:ed:02:7c:72:85:8f:cd:71:2c:
    83:b9
publicExponent: 65537 (0x10001)
privateExponent:
    41:91:7b:3c:da:67:41:fc:95:07:30:d8:27:19:9e:
    25:bf:61:d2:17:99:3d:70:e3:cf:c5:c1:98:c3:94:
    1c:a5:45:7e:30:04:15:07:c3:c0:56:3d:a4:4c:14:
    90:41:3c:ed:7e:1d:6f:30:1a:89:9e:78:1d:64:09:
    07:51:eb:6f:15:ec:c4:2d:88:44:f4:b8:c5:51:1e:
    11:c6:42:9a:91:dd:44:d3:70:b8:52:ec:c6:d6:15:
    7d:bd:16:9a:3e:b9:2c:f0:a7:94:c5:ce:70:22:6b:
    c7:5d:94:21:1a:23:e2:fd:44:fa:73:43:e9:3f:9b:
    2e:6d:2e:7e:a0:71:49:71:12:12:b4:88:8d:7c:87:
    89:e3:8f:78:0b:af:df:45:86:8c:c2:66:bb:5a:e6:
    72:10:bb:7f:b6:e3:64:1c:ee:0a:f7:b1:f0:4c:5e:
    06:b7:5f:b3:e3:f9:b7:5f:0a:ba:6e:f4:c0:62:f0:
    b2:2d:f1:3e:23:f3:ec:cd:5b:21:53:b6:f3:2f:08:
    17:fc:31:90:2e:58:f4:70:65:92:88:77:79:e6:6d:
    9b:70:80:2e:a1:29:1a:e7:ad:fa:28:82:0d:51:f3:
    f9:21:31:54:2f:de:88:5e:ae:cf:91:ce:86:64:47:
    02:d5:3d:d8:97:91:78:38:62:89:65:4a:91:de:75:
    01
prime1:
    00:ee:bb:c9:5a:a1:94:61:ba:3a:03:87:05:f1:74:
    b0:eb:12:8d:6e:ba:60:a1:82:d9:84:8c:41:74:7b:
    8b:1c:fc:91:4b:ed:c9:e2:4e:6c:2f:a8:94:a3:68:
    1e:55:a6:7c:ea:ea:6d:e9:df:c5:7f:cf:86:b0:53:
    f9:86:22:e3:b3:85:52:15:a0:1a:17:6b:80:f5:50:
    93:0d:af:4b:62:3e:9d:58:65:ba:07:bf:cb:e7:c8:
    7a:e9:0d:6c:07:51:ce:01:53:aa:eb:49:08:79:3e:
    09:69:90:b1:e8:1a:49:d3:d7:52:40:78:53:3a:49:
    d5:e8:45:0d:e1:ec:76:51:d9
prime2:
    00:c0:d3:38:de:34:1c:bb:95:3d:3f:83:bc:fb:98:
    bd:f2:8d:a5:db:1a:bf:b2:6c:02:bf:f3:73:e2:cb:
    59:fc:04:7d:1a:8f:ac:8b:d5:1f:ca:ba:bd:d5:e1:
    97:13:a8:58:43:e7:0d:60:3f:36:73:e9:f0:e4:0e:
    33:df:cf:17:69:86:58:c0:6e:30:69:ff:6c:a0:55:
    24:d3:5b:e7:21:c9:3c:e5:5e:66:5e:62:df:b4:8e:
    72:9b:06:c5:61:e5:05:49:bc:99:57:f6:25:cc:e9:
    3e:fc:af:b5:02:70:cb:cb:6e:f0:db:f2:1a:fd:7f:
    6f:96:38:69:1c:21:72:b4:e1
exponent1:
    00:b3:12:ab:13:cf:95:e4:c4:72:d5:c8:87:5d:b9:
    c1:27:63:30:31:b9:9d:d8:28:b5:8e:a6:42:46:e4:
    90:d1:fa:65:e6:85:84:64:bb:9c:8d:17:2f:ff:6e:
    8f:2a:82:0a:bb:8f:83:48:e5:f0:58:51:cb:5f:22:
    6e:4d:fe:87:bc:56:29:df:4c:cb:a5:7b:9f:2c:e3:
    f6:9a:52:3e:02:80:a3:37:f6:7e:57:67:b7:c4:b1:
    ed:f8:38:78:2a:f9:62:c4:3e:05:3c:1d:f9:3c:30:
    9b:90:d2:d7:90:19:7f:fd:66:4b:2d:4e:d4:67:29:
    91:49:7b:da:d0:f7:b5:3c:e9
exponent2:
    00:ad:dc:c6:25:f4:af:03:a4:68:f9:5f:fb:82:90:
    12:95:25:8b:2a:a8:4f:b8:bd:13:2d:a8:82:11:38:
    72:06:7e:b5:9e:c1:75:3f:10:07:fe:6f:aa:c3:b3:
    08:d9:bc:ac:f9:6c:d7:ee:b4:90:90:ab:9b:7c:c6:
    21:97:e7:ce:a0:63:76:9a:eb:bf:d3:93:6f:8a:91:
    bb:06:a8:93:1b:2f:ac:2c:d4:95:50:fd:ad:df:cb:
    a1:22:8f:54:62:14:72:54:2e:2d:c5:d6:37:f7:2f:
    48:8f:e6:8e:3b:89:20:f8:69:2b:db:e5:cc:d8:4d:
    93:7b:cb:99:5a:b7:fe:09:81
coefficient:
    00:ea:03:0a:d2:73:25:c9:dc:56:aa:7b:3c:8f:58:
    08:56:ba:70:e2:54:5a:98:9d:fd:42:f1:7a:09:06:
    f0:18:c2:1e:5d:e6:3d:fa:33:b5:d9:12:17:7d:b7:
    07:78:9f:10:da:e4:d7:d1:89:75:be:b4:64:b9:5d:
    8c:24:c6:20:3b:f3:cc:9f:ce:dc:af:df:1f:33:16:
    0e:c7:2d:43:f4:87:ef:e5:1f:a7:06:70:a8:c3:5d:
    56:5a:4c:92:ef:6f:ce:e1:54:be:14:a4:33:09:82:
    0b:10:0c:a9:1d:77:01:8d:8d:52:3c:5a:95:2e:8f:
    9f:90:ed:a3:2a:77:b1:88:6f
writing RSA key
```

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAs9HQ0zpf1ueTSSJDQNzShJ4SNLMxpI7riQVRQs5QPXZohzWv
FoFwQkSwcWarIJiwce3tT0eBAmZTBX9ICR2r36mRnjfcSg5wDf1QtTf0yDPu43rW
RZBoUTCK4HUdP8Pf28SdXNGH46Ricmd1EHfdFsFc4uV3+fPxMgrqU4aaeZ7NinkX
nXOMmQqWAdmliNCYYd+o+sb7d7ofKM0EWbL0FlbnCq4QgCPzvP6Gepk6OyD6D+wa
8Z98LBrtO0Wj5J7er6q+InoLHH04mxLclibDmnm0Uk5PLfyQM+1i2LX+LqxQJGh/
bHyUmA6eC7PSwK19J+e9S+HtAnxyhY/NcSyDuQIDAQABAoIBAEGRezzaZ0H8lQcw
2CcZniW/YdIXmT1w48/FwZjDlBylRX4wBBUHw8BWPaRMFJBBPO1+HW8wGomeeB1k
CQdR628V7MQtiET0uMVRHhHGQpqR3UTTcLhS7MbWFX29Fpo+uSzwp5TFznAia8dd
lCEaI+L9RPpzQ+k/my5tLn6gcUlxEhK0iI18h4njj3gLr99FhozCZrta5nIQu3+2
42Qc7gr3sfBMXga3X7Pj+bdfCrpu9MBi8LIt8T4j8+zNWyFTtvMvCBf8MZAuWPRw
ZZKId3nmbZtwgC6hKRrnrfoogg1R8/khMVQv3ohers+RzoZkRwLVPdiXkXg4Yoll
SpHedQECgYEA7rvJWqGUYbo6A4cF8XSw6xKNbrpgoYLZhIxBdHuLHPyRS+3J4k5s
L6iUo2geVaZ86upt6d/Ff8+GsFP5hiLjs4VSFaAaF2uA9VCTDa9LYj6dWGW6B7/L
58h66Q1sB1HOAVOq60kIeT4JaZCx6BpJ09dSQHhTOknV6EUN4ex2UdkCgYEAwNM4
3jQcu5U9P4O8+5i98o2l2xq/smwCv/Nz4stZ/AR9Go+si9Ufyrq91eGXE6hYQ+cN
YD82c+nw5A4z388XaYZYwG4waf9soFUk01vnIck85V5mXmLftI5ymwbFYeUFSbyZ
V/YlzOk+/K+1AnDLy27w2/Ia/X9vljhpHCFytOECgYEAsxKrE8+V5MRy1ciHXbnB
J2MwMbmd2Ci1jqZCRuSQ0fpl5oWEZLucjRcv/26PKoIKu4+DSOXwWFHLXyJuTf6H
vFYp30zLpXufLOP2mlI+AoCjN/Z+V2e3xLHt+Dh4KvlixD4FPB35PDCbkNLXkBl/
/WZLLU7UZymRSXva0Pe1POkCgYEArdzGJfSvA6Ro+V/7gpASlSWLKqhPuL0TLaiC
EThyBn61nsF1PxAH/m+qw7MI2bys+WzX7rSQkKubfMYhl+fOoGN2muu/05NvipG7
BqiTGy+sLNSVUP2t38uhIo9UYhRyVC4txdY39y9Ij+aOO4kg+Gkr2+XM2E2Te8uZ
Wrf+CYECgYEA6gMK0nMlydxWqns8j1gIVrpw4lRamJ39QvF6CQbwGMIeXeY9+jO1
2RIXfbcHeJ8Q2uTX0Yl1vrRkuV2MJMYgO/PMn87cr98fMxYOxy1D9Ifv5R+nBnCo
w11WWkyS72/O4VS+FKQzCYILEAypHXcBjY1SPFqVLo+fkO2jKnexiG8=
-----END RSA PRIVATE KEY-----
```

b. Brief comparison of the same/different values observed across the extra generated keys (3 questions in step 4d)

i. Which ones are constant throughout?

1. **Only the public exponent.**
2. **Little bit of the start of Private Keys are the same**

ii. Which ones vary?

1. **Everything else modulus, private expo, primes, exponents, coefficient and key.**

iii. What do these values represent?

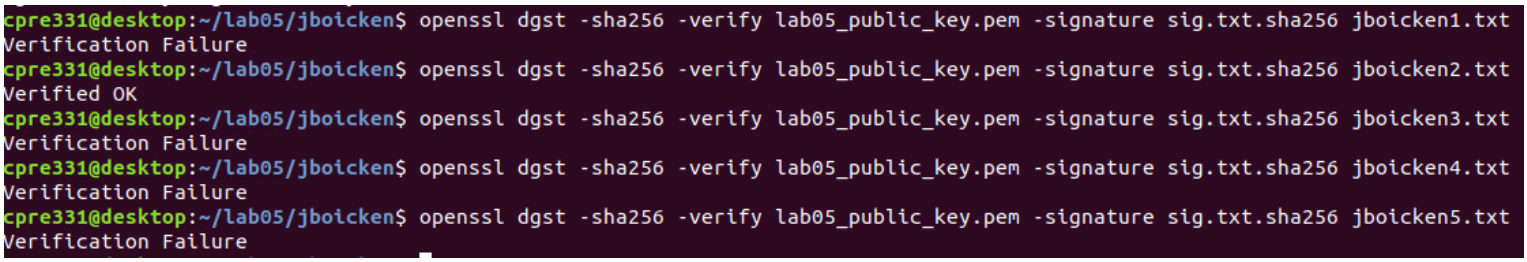
1. **Modulus (N) and public expo (e) are the public key**
2. **Prime1 (p) and prime2 (q) multiplied is modulus**
3. **Public expo (e) is a coprime number to p and q usually 65537**
4. **Private exponent is d value in e*d mod (p-1)(q-1) = 1**
5. **Expo1 is d mod (p-1)**
6. **Expo2 is d mod (q-1)**
7. **Coefficient is q^-1 mod p**

(10 points)

c. **Discussion of the differences between FTP and SFTP. (Three question in step 6h)**
   i. **Why would you want one over the other?**
      1. **SFTP is encrypted using openssh**
   ii. **Why did we need to specify our private key?**
      1. **This is what we decrypt the data received from the SFTP server with**
   iii. **What protection does this offer?**
      1. **Provides confidentiality to data sent to server**
      2. **Can provide integrity with signing as well**

   (10 points)

d. **Screenshot of the verified message (Step 7b)**
   (10 points)



e. **Discussion on hash verification (Two questions in step 7c)**
   i. **What is known about the message?**
      1. **It has not been modified**
      2. **It actually came from the owner of the lab05 private key**
   ii. **What is the message protected against and what is it vulnerable to?**
      1. **This only provides integrity regarding the message**
      2. **The message is still plain text and can be read by anyone**

   (10 points)

f. **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).**
   (10 points)

   This message is only encrypted. This means it provides confidentiality but lacks integrity. Essentially, anyone could encrypt a message with my public key and send it to me. Then, I have no way of checking who sent it or that it wasn't modified in transmission.

2) Part 2:
   a. **<u>Screenshot of the</u> signed certificate when looked at through openssl. (Step 12c)**
   (10 points)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 17 (0x11)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = Iowa, L = Ames, O = 331.com, OU = homework, CN = certs.homework.331.com, emailAddress = certs@homework.331.com
        Validity
            Not Before: Sep 28 10:13:04 2021 GMT
            Not After : Sep 28 10:13:04 2022 GMT
        Subject: C = US, ST = Iowa, O = 331.com, OU = homework, CN = jboicken.homework.331.com, emailAddress = jboicken@homework.331.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:b3:d1:d0:d3:3a:5f:d6:e7:93:49:22:43:40:dc:
                    d2:84:9e:12:34:b3:31:a4:8e:eb:89:05:51:42:ce:
                    50:3d:76:68:87:35:af:16:81:70:42:44:b0:71:66:
                    ab:20:98:b0:71:ed:ed:4f:47:81:02:66:53:05:7f:
                    48:09:1d:ab:df:a9:91:9e:37:dc:4a:0e:70:0d:fd:
                    50:b5:37:f4:c8:33:ee:e3:7a:d6:45:90:68:51:30:
                    8a:e0:75:1d:3f:c3:df:db:c4:9d:5c:d1:87:e3:a4:
                    62:72:67:75:10:77:dd:16:c1:5c:e2:e5:77:f9:f3:
                    f1:32:0a:ea:53:86:9a:79:9e:cd:8a:79:17:9d:73:
                    8c:99:0a:96:01:d9:a5:88:d0:98:61:df:a8:fa:c6:
                    fb:77:ba:1f:28:cd:04:59:b2:f4:16:56:e7:0a:ae:
                    10:80:23:f3:bc:fe:86:7a:99:3a:3b:20:fa:0f:ec:
                    1a:f1:9f:7c:2c:1a:ed:3b:45:a3:e4:9e:de:af:aa:
                    be:22:7a:0b:1c:7d:38:9b:12:dc:96:26:c3:9a:79:
                    b4:52:4e:4f:2d:fc:90:33:ed:62:d8:b5:fe:2e:ac:
                    50:24:68:7f:6c:7c:94:98:0e:9e:0b:b3:d2:c0:ad:
                    7d:27:e7:bd:4b:e1:ed:02:7c:72:85:8f:cd:71:2c:
                    83:b9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                F9:17:12:78:DC:4A:C5:E5:95:03:24:30:E9:FC:75:B8:64:E9:26:B3
            X509v3 Authority Key Identifier:
                keyid:C8:B4:E7:29:2F:01:DF:2D:6F:8A:EC:B7:5C:7D:8C:42:21:90:CC:42

    Signature Algorithm: sha256WithRSAEncryption
         50:36:8c:b9:4f:12:d2:99:b2:e1:b3:98:e4:2a:b1:fe:ff:f9:
         2b:a8:31:a8:87:ed:47:c9:82:41:3e:04:40:d6:e3:79:f2:cb:
         32:18:7a:d7:ab:b1:27:1e:0e:18:ae:77:2e:b3:8c:5a:3f:59:
         bd:63:f1:48:ce:87:a5:85:1e:a2:9a:01:c3:47:7e:50:58:21:
         d2:2b:58:cd:f4:18:fd:e7:fd:15:4b:18:46:6b:45:ac:7c:60:
         5a:64:83:86:63:46:b5:b2:92:00:73:91:5e:e8:d1:9e:09:ed:
         ad:9c:5e:04:6b:b6:b2:9d:66:c5:e1:82:55:25:4d:5f:94:7d:
         87:38:9b:c1:cf:14:50:57:46:55:86:e2:38:26:27:57:b4:15:
         03:07:8a:b0:fc:44:41:62:d9:7b:a1:9d:71:97:e0:81:33:28:
         1b:fc:f0:ef:4d:58:83:fc:ce:a7:89:d6:aa:31:e1:9c:3a:48:
         2c:6d:18:19:1c:12:bd:f9:74:1e:0e:a6:fd:52:ad:53:58:4d:
         7b:7a:ed:9c:5e:b7:cd:72:7a:a2:3d:40:66:90:bc:70:a3:ea:
         8a:ce:0c:79:7f:55:35:9e:24:d5:08:61:34:3d:34:53:0e:9e:
         67:56:bf:29:c1:5b:8e:d2:7a:50:6d:e1:3b:02:1f:c9:62:4c:
         19:ae:af:37
```

b. Discussion from step 12

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

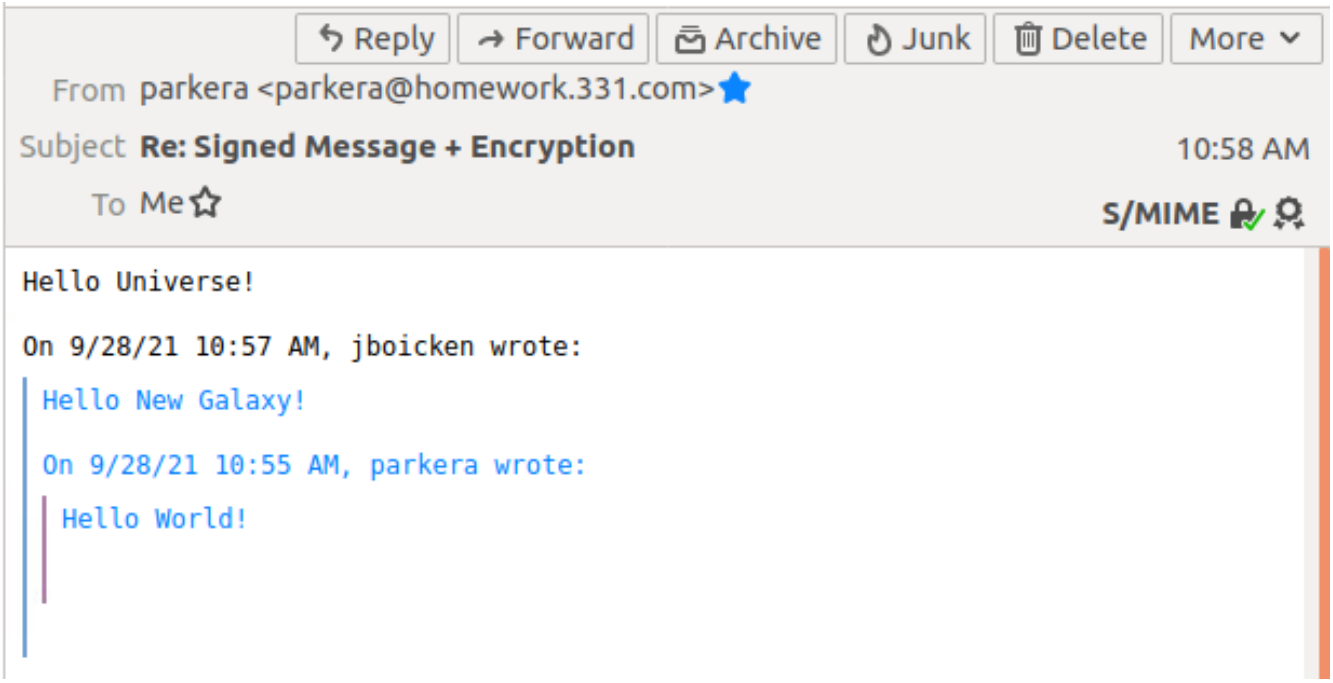
1. **The modulus and exponent are the same from the private key.**
2. **The certificate only needs my public key, which is the mod and expo. That way information can be encrypted with the public key or verify a signed message in the private key.**

ii. What was happening during the Certificate Signing process? Why did you need to submit it for signing?

1. **We needed a CA, certificate authority, to verify who we are/ the certificate. The CA gets our public key and signed information, and returns a verified certificate if the signing was valid. (In this case)**
2. **With it being verified, we can use the certificate in TLS communications without warnings. Essentially having a third party confirm who we are for us to contact others and vise versa.**

(10 points)

c. **Screenshot of signed and encrypted message received from a classmate** (10 points)



d. **Discussion of what properties the email (Step 4)**
   i. **The messages signed by my private key (Part 1 step 6)**
      1. **This email is signed like in 1s6 so we have integrity within the communications**
      2. **However, it is encrypted as well providing confidentiality.**

   ii. **The message encrypted with my public key (Part 1 step 7)**
      1. **This email is encrypted like in 1s7 but it also signed by the private key to confirm it was sent by the me and only me**

   iii. **Explain why you couldn't send an encrypted message straight away - why did you need to send a signed-only message first?**
      1. **We don't have the other user's public key so we send them a signed message which gives them our public key. (They can ensure it was sent by the owner of the private key.)**
      2. **Then, they can encrypt the message to us using our public key and sign it using their private key, which gives us their public key. (We can then confirm its from them)**
      3. **Then, signed and encrypted communications can go both ways.**
      4. **(I do see a weakness to MITM at initializing comms, though)**

(10 points)