Lab09 - Keys & Certificates

Part 01:

1. **Screenshot of the output from** `openssl rsa -text -in <netid>_private_key.pem`
   (10 points)

```
cpre331@cpre331:~/labs/lab09$ openssl rsa -text -in rjlawson_private_key.pem
Private-Key: (2048 bit, 2 primes)
modulus:
    00:84:98:70:59:33:00:7f:7a:64:d5:b7:d7:35:56:
    84:09:10:bd:81:50:53:12:42:37:ce:6d:df:78:1c:
    0e:2e:2c:9f:4a:c0:63:c3:ad:49:73:2f:67:3b:3f:
    fe:c3:5d:55:04:0e:b3:9d:62:c1:e8:93:30:8d:b8:
    d9:93:bf:0c:44:46:72:21:68:fa:bf:a8:9b:51:e0:
    bc:83:32:dd:fe:59:0c:b4:df:f4:18:f2:27:e0:15:
    f3:67:35:f5:56:99:b0:08:e0:73:ef:0f:d0:ec:b3:
    7d:93:8c:d8:ee:21:86:15:d3:0a:be:84:36:bd:f8:
    32:55:c9:7c:b7:83:c7:01:ba:bf:d3:8f:70:ff:3f:
    c7:85:64:3e:3f:53:af:39:e1:2a:d4:c0:f4:de:e5:
    7b:75:5e:10:0f:ad:d9:33:a2:2a:d1:32:02:3a:47:
    87:00:59:4f:ef:04:39:5f:e0:14:44:0b:62:4b:88:
    78:3f:4f:b9:03:b3:67:37:d2:66:88:54:dd:b3:7f:
    3d:71:fc:87:78:07:2e:42:b8:f7:3e:34:a3:1d:7f:
    0f:a2:55:86:dd:68:64:8c:f1:f4:0a:02:03:2d:39:
    6a:6e:19:40:58:96:ac:9d:2c:1e:2a:82:d0:a8:c9:
    a0:84:d5:12:06:47:73:2c:a9:b0:a3:2d:fa:9b:08:
    a2:b1
publicExponent: 65537 (0x10001)
privateExponent:
    21:a8:80:7c:64:11:f0:4a:25:66:8a:f0:3a:3d:e7:
    ee:55:2d:85:b1:da:24:7c:62:a6:28:05:dd:fb:61:
    2e:1f:6d:a0:10:0e:43:11:ad:df:6b:5d:0d:11:45:
    9e:5a:06:c6:ac:e4:b3:42:ea:6e:1b:4e:eb:ea:cc:
    70:50:c2:d0:62:01:7e:b1:a3:55:1b:7b:b1:e1:16:
    79:47:64:4a:b8:58:1d:61:ec:18:98:ff:be:46:54:
    2f:12:e7:60:40:4b:0b:35:ce:b8:14:8f:b8:46:27:
    ce:58:a6:88:6c:42:19:30:25:3e:0f:59:c6:07:46:
    df:b7:f1:cc:b3:ca:c4:89:41:b6:fe:d3:9d:2c:2c:
    26:1c:25:c8:8d:6e:5a:6c:6a:05:6c:3f:d2:dc:d3:
    e8:8b:2b:60:ab:23:c1:51:61:f1:32:df:19:d6:f5:
    f0:f5:a6:20:25:99:15:e6:98:ac:a2:ee:79:5a:37:
    ef:e8:2e:d1:a6:41:99:d5:37:ef:6c:a0:50:bb:83:
    ce:66:c6:e6:f1:4f:7d:90:5b:a9:54:d0:19:14:2b:
    ad:ed:f5:7e:86:13:49:1f:73:26:ce:23:f9:80:9c:
    f0:68:05:02:31:ae:ab:10:d0:40:a3:2b:5d:36:be:
    c1:11:d8:9b:f2:fa:95:0c:d9:24:ae:ce:dd:6b:9e:
    71
prime1:
    00:b8:25:f8:98:23:1a:2d:b9:1e:ba:db:5b:6c:d2:
    16:59:f7:2c:e5:64:b6:f9:ec:f5:ec:63:2d:b2:35:
    2b:1b:b3:52:8c:9a:92:d8:83:05:ea:04:b5:09:93:
    8f:9c:36:fd:28:13:09:ef:c2:57:7e:d2:ba:4b:ec:
    99:39:fe:28:85:ad:45:9e:5d:69:a6:e9:73:89:0d:
    96:85:86:54:3b:ca:c6:7c:27:28:a5:b2:29:24:d6:
    e7:46:62:04:f4:2c:dc:ef:b7:4d:0e:f1:4e:c4:d1:
    c6:e3:11:a5:68:d0:9f:c4:c0:28:56:e0:86:52:9d:
    a2:4b:ac:1c:91:e2:ef:a4:0f
```

```
prime2:
    00:b8:55:01:7a:8f:74:6e:1f:1e:1e:ec:c0:d1:16:
    8f:98:45:13:74:de:80:e2:16:bb:6c:10:1d:d8:62:
    29:f1:b7:50:09:27:f3:f6:33:48:94:2c:f9:cb:1a:
    cc:b4:91:d4:ff:20:0c:06:35:71:62:3b:f9:7c:ca:
    f6:ea:5c:2f:2d:e6:a6:9f:ba:5b:c4:56:ce:64:29:
    bf:e0:eb:44:28:d1:45:36:b0:25:bf:8d:ad:66:bf:
    8a:55:e8:79:f8:0c:2b:a1:4a:d1:86:be:66:1d:65:
    59:1d:87:7c:26:c6:d5:a7:73:6a:4a:0b:e8:8b:3a:
    e4:f3:ce:81:51:e1:1d:8d:3f
exponent1:
    00:a3:1a:46:b0:81:ce:cb:16:bf:28:23:e8:3b:5f:
    6d:1a:ac:3a:60:c7:ae:e5:78:c3:6d:67:7e:ee:eb:
    f6:cd:a7:2c:03:8b:59:6b:59:c9:a0:38:21:1d:65:
    4c:7a:c1:9d:c2:a3:f2:56:21:1d:1c:20:8b:8f:79:
    f5:51:8f:52:d6:eb:dc:d0:e2:ce:14:5f:8b:cc:a5:
    73:5f:ba:d5:da:cb:c4:b7:ec:7b:2d:1f:bb:1f:7d:
    15:05:9b:05:e6:3b:e2:48:94:63:35:4b:f8:47:8d:
    c2:8a:16:74:1a:7d:46:35:9f:39:5b:91:ac:87:7a:
    45:68:9e:fe:03:1d:2c:c2:73
exponent2:
    51:84:16:11:53:1b:54:0f:a2:cc:5e:3a:ae:bc:61:
    68:1f:34:09:7c:d4:56:27:63:5e:d8:89:ba:45:3e:
    f3:4b:f3:b2:f8:de:24:44:6d:96:49:85:75:d2:36:
    30:ac:45:1b:45:da:cb:6c:1a:e6:2c:4b:9a:6a:4f:
    63:38:bd:0c:79:71:ba:35:39:9b:cc:1f:9d:9f:f0:
    e0:d0:69:e5:fb:15:b6:a7:93:29:f0:c7:7c:26:bc:
    50:5d:6c:82:cb:2f:08:37:04:0d:a8:69:94:1a:5b:
    9c:79:6b:e7:e2:0a:5d:f0:e6:52:34:8d:f3:f4:69:
    87:80:0d:24:5e:7f:29:15
coefficient:
    36:a0:6e:7e:97:5a:87:0c:72:b1:c4:24:1b:2d:50:
    ea:96:d3:d0:f8:d6:ca:29:be:d9:6b:e3:fa:5e:a5:
    e8:41:02:39:19:be:8a:fa:6d:5e:61:b3:56:fc:80:
    13:49:72:a8:db:00:1b:4d:01:2b:bf:7a:50:fc:99:
    7f:8f:3c:08:df:ab:12:d9:a5:44:5f:7b:e7:c6:c2:
    08:35:e6:fa:dc:ab:8d:2f:69:77:62:aa:c5:8d:22:
    31:50:f1:65:71:24:84:02:05:5b:e9:d7:68:b9:50:
    3f:29:86:df:41:09:65:b0:be:6d:67:ff:e7:7e:42:
    8f:56:72:ee:15:ee:f5:e9
writing RSA key
-----BEGIN PRIVATE KEY-----
```

2. **Comparison of the same/different values observed across the extra generated keys**
    i. Which values are constant?
        1. publicExponent
    ii. Which ones vary?
        1. Modulus, privateExponent, prime1, prime2, exponent1, exponent2
    iii. What do these values represent?
        1. Modulus
            a. Used both in the public and private keys, determines size of the keys and the range of values that they can be encrypted/decrypted
            b. Public exponent
                i. Simplifies encryption process, fixed value used in public key of RSA key pair.
            c. Private exponent
                i. Unique to each key pair, secret key used for decryption
            d. Prime factors
                i. These are a kept secret, multiplied to produce the modulus back into its prime components.
            e. Exponents

i. Involves using Chinese Remainder Theorem optimization for RSA decryption

(10 points)

3. **Discussion of the differences between FTP and SFTP.**
   i. Why would you want one over the other?
      1. FTP is File Transfer Prototcol and is an older protocol used to transfer files over a network. It is usually not secure by default and is usually used when you just want to transfer files quickly. Where as SFTP is designed for both secure file transfer and encryption. Overall, you want to use FTP if security is something you don't care about and or you want speed, whereas SFTP is much more secure and offers lots of security.
   ii. Why did we need to specify our private key?
      1. When using SFTP, it is necessary to specify the key for being able to remote into the server. FTP doesn't need this. You need a public and private key in this instance in order to prove your identity and gain access to the server.
   iii. What protection does this offer?
      1. FTP offers no protection (except a password). SFTP offers strong authentication (public/private key pairs) and secure communication (encrypted data).

   (10 points)

4. **Screenshot of the five messages [netid]1.txt, [netid]2.txt, … [netid]5.txt**
   (10 points)

5. **Discussion on hash verification**
   i. What is known about the message?
      1. The hash was signed and the signature is stored in the sha256 file, with the lab09_public_key.pem being the key pair to the private key to encrypt the message.
   ii. What is the message protected against and what is it vulnerable to?

1. The message is protected against modifications because each key has the associated signature sha256 and should correlate to lab09_public_key.pem. This creates a unique hash value. However, its vulnerable to many things such as the key being changed or generating false signatures. If the file is messed with it could become hard to verify if the message is authentic. Can be intercepted with a MITM attack.

(10 points)

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).**
   (10 points)
   - It's protected against unauthorized access during transmission and the use of public key encryption (asymmetric) makes sure that the holder of the private key can decrypt and read the message. Any tampering would result in a decryption failure. It's vulnerable against key compromises, such as the public key; the attacker can use their own private key to decrypt the message. On top of that if the attacker (eve) gets their hands on the message during transmission and has a corresponding private key, it won't matter if the message is encrypted.

7. **Screenshot of the signed certificate ([netid]_certificate.pem) when looked at through openssl**

(10 points)

```
cpre331@cpre331:~/labs/lab09$ openssl x509 -in rjlawson_certificate.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 30 (0x1e)
        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: Oct 29 21:22:02 2023 GMT
            Not After : Oct 28 21:22:02 2024 GMT
        Subject: C = US, ST = Iowa, O = 331.com, OU = homework, CN = rjlawson.homework.331.com, emailAddress = rjlawson@homework.331.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:84:98:70:59:33:00:7f:7a:64:d5:b7:d7:35:56:
                    84:09:10:bd:81:50:53:12:42:37:ce:6d:df:78:1c:
                    0e:2e:2c:9f:4a:c0:63:c3:ad:49:73:2f:67:3b:3f:
                    fe:c3:5d:55:04:0e:b3:9d:62:c1:e8:93:30:8d:b8:
                    d9:93:bf:0c:44:46:72:21:68:fa:bf:a8:9b:51:e0:
                    bc:83:32:dd:fe:59:0c:b4:df:f4:18:f2:27:e0:15:
                    f3:67:35:f5:56:99:b0:08:e0:73:ef:0f:d0:ec:b3:
                    7d:93:8c:d8:ee:21:86:15:d3:0a:be:84:36:bd:f8:
                    32:55:c9:7c:b7:83:c7:01:ba:bf:d3:8f:70:ff:3f:
                    c7:85:64:3e:3f:53:af:39:e1:2a:d4:c0:f4:de:e5:
                    7b:75:5e:10:0f:ad:d9:33:a2:2a:d1:32:02:3a:47:
                    87:00:59:4f:ef:04:39:5f:e0:14:44:0b:62:4b:88:
                    78:3f:4f:b9:03:b3:67:37:d2:66:88:54:dd:b3:7f:
                    3d:71:fc:87:78:07:2e:42:b8:f7:3e:34:a3:1d:7f:
                    0f:a2:55:86:dd:68:64:8c:f1:f4:0a:02:03:2d:39:
                    6a:6e:19:40:58:96:ac:9d:2c:1e:2a:82:d0:a8:c9:
                    a0:84:d5:12:06:47:73:2c:a9:b0:a3:2d:fa:9b:08:
                    a2:b1
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                26:BB:3C:B2:B9:18:BB:2A:44:9A:74:AE:D2:C3:5F:E0:CC:59:D9:54
            X509v3 Authority Key Identifier:
                B1:58:E4:C8:15:C0:A2:DB:95:C9:1B:69:AB:0B:64:9B:A9:F3:CB:D9
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        6e:7e:65:3d:55:b0:b3:c3:1d:ec:36:e8:c1:b5:33:69:40:bd:
        c1:65:ea:60:31:49:0b:be:66:74:48:5f:f6:93:d6:63:ad:d3:
        df:7f:3e:6d:ee:ce:3f:29:fd:2c:07:70:ad:1c:07:22:4e:3e:
        f8:cf:37:14:27:26:15:7d:76:3b:05:f4:f8:76:bf:a4:69:2c:
        f4:5c:e6:4b:42:c6:70:8c:ba:ac:72:69:c2:88:21:15:e6:85:
        6d:bf:13:6f:52:1f:7e:0d:a4:86:0b:15:c3:11:a8:bc:22:c9:
        17:55:17:be:5f:04:01:a6:bb:44:02:52:01:aa:1e:df:26:e4:
```


```
    Signature Value:
        6e:7e:65:3d:55:b0:b3:c3:1d:ec:36:e8:c1:b5:33:69:40:bd:
        c1:65:ea:60:31:49:0b:be:66:74:48:5f:f6:93:d6:63:ad:d3:
        df:7f:3e:6d:ee:ce:3f:29:fd:2c:07:70:ad:1c:07:22:4e:3e:
        f8:cf:37:14:27:26:15:7d:76:3b:05:f4:f8:76:bf:a4:69:2c:
        f4:5c:e6:4b:42:c6:70:8c:ba:ac:72:69:c2:88:21:15:e6:85:
        6d:bf:13:6f:52:1f:7e:0d:a4:86:0b:15:c3:11:a8:bc:22:c9:
        17:55:17:be:5f:04:01:a6:bb:44:02:52:01:aa:1e:df:26:e4:
        61:79:b5:3f:43:82:9d:ce:31:b3:6d:fb:49:29:fd:f3:10:4d:
        7f:2b:e8:f8:25:3b:6d:41:5f:ad:b9:79:c8:d2:64:62:28:98:
        e2:01:40:6b:69:ab:36:7e:ac:c6:a7:96:5d:73:67:aa:c9:a5:
        0d:68:9e:da:07:4b:fb:75:93:d9:62:d2:dd:9e:1d:06:ab:43:
        e0:dd:47:d2:40:58:aa:c3:70:55:38:dc:c3:b4:c4:37:aa:ef:
        f8:49:21:f0:e7:19:86:ca:d1:07:e4:c1:47:b1:c2:76:91:f0:
        c5:9d:cc:1a:1a:f5:01:29:48:71:03:2f:d1:25:4a:09:cc:d6:
        3b:a1:cd:90
```


8. **Discussion from step 12**
    i. **Do any parts of the certificate match with your private key? If so, why?**
        1. Yes, because it contains the public key that corresponds to the private key that was held by me. They form the pair and the public key is embedded in the certificate with encryption and signature verification.

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

(10 points)

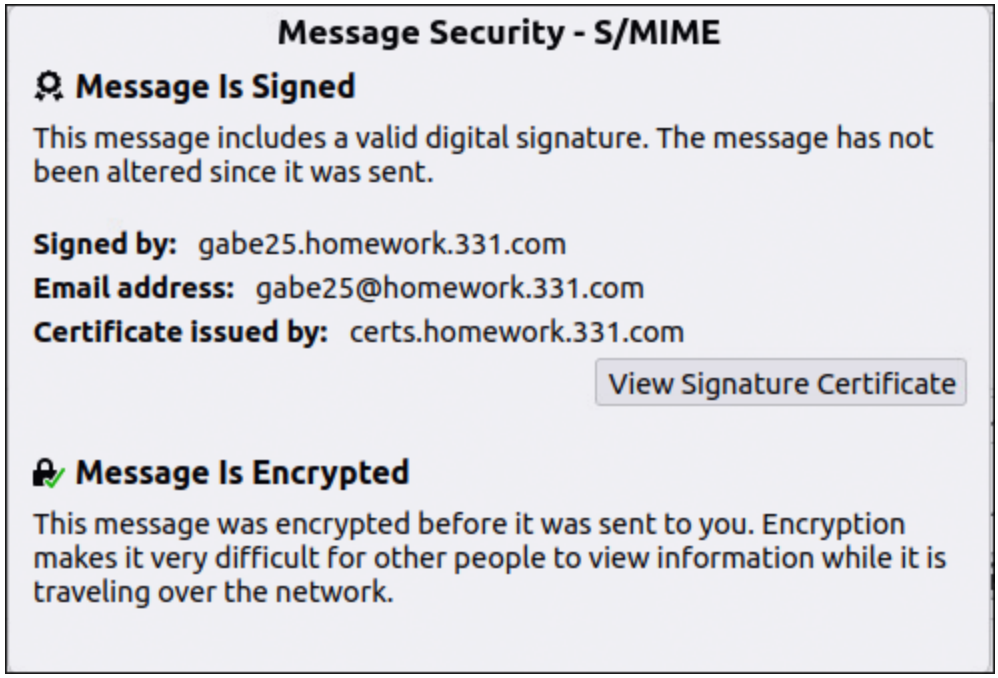
- It required a certificate request which was generated by the owner that includes the public key and information about the subject. Then it is submitted to a trusted CA for verification. Once approved it signs the certificate signing with its private key. This certificate includes the public key and information about the key. The person installs it on the server and is then used. It needs to be submitted for signing to make sure it is trustworthy and the certificate can be validated by the ownership of the associated public key. This makes sure that the requested certificate is the entity it claims to be.

Part 02:

9. **Screenshot of signed and encrypted message received from a classmate**

(10 points)

-



10. **Explain why you couldn't send an encrypted message straight away - why did you need to send a signed-only message first?**

(10 points)

- Well you can't send an encrypted message right away, because you need the other sender's public key and essentially trade key with the other person, but keep the private key to yourself. For the signed-only message, it's just for identity verification, establishing trust, and making sure that encryption capabilities are possible.