Teammates: Ron Gassner, Lucas Yao

Course name: **CSCI 360: Cryptography and Cryptanalysis**

Professor: Matluba Khodjaeva

Project 3 Report

In this report, we detail the secure communication process between Lucas (Bob) and Ron (Alice) utilizing the certificate method. Both entities generated a pair of keys, including public and private keys, for their encryption and decryption operations. Additionally, both Lucas and Ron also created a pair of keys specifically for the Certificate Authority (CA) to facilitate the secure exchange of certificates.

The communication process involved Ron (Alice) encrypting a message using his private key and Lucas (Bob) decrypting the message using Ron's (Alice's) public key, ensuring confidentiality and integrity during transmission. Furthermore, the use of certificates issued by the CA added an extra layer of trust and authentication, allowing Lucas and Ron to verify each other's identities securely.

Overall, the implementation of the certificate method facilitated a robust and secure communication channel between Lucas (Bob) and Ron (Alice), ensuring that sensitive information exchanged between them remained protected from unauthorized access or tampering.

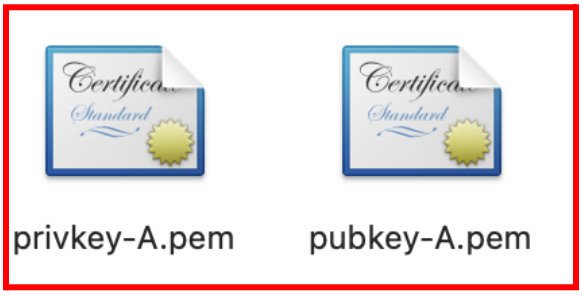
Ron Gassner(Alice):

- Step1. a - I generated my private key using the RSA algorithm.

```
Last login: Thu Mar 21 10:52:34 on ttys002
ron@rons-mbp ~ % openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -pkeyopt rsa_keygen_pubexp:3 -out privkey-A.pem
.................+++++
.......+++++
```

- Step 1. b - From the private key I generated the public key that match it.

```
ron@rons-mbp ~ % openssl pkey -in privkey-A.pem -pubout -out pubkey-A.pem
ron@rons-mbp ~ %
```



- I repeated the same process and generated the two keys for the CA.

```
ron@rons-mbp ~ % openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -p
keyopt rsa_keygen_pubexp:3 -out privkey-c.pem
.....................................................................++
+++
.....................+++++
ron@rons-mbp ~ %
```

```
ron@rons-mbp ~ % openssl pkey -in privkey-A.pem -pubout -out pubkey-c.pem
ron@rons-mbp ~ %
```

- I tried the “Aside:” note, trying to see if I can see Alice’s (my keys) and the CA’s keys in plain text and it worked!

```
ron@rons-mbp ~ % openssl pkey -in  privkey-A.pem -text -noout
RSA Private-Key: (2048 bit)
modulus:
    00:c3:08:04:c4:53:83:41:97:a5:8c:80:54:b0:0d:
    87:4d:47:89:cb:37:d6:48:22:a9:93:18:a8:da:54:
    5e:fa:41:ef:29:29:f5:d3:be:ec:bb:c2:cf:4e:e8:
    2a:3f:ac:e0:5e:9e:01:3c:6b:71:75:b5:62:55:53:
    38:23:39:1f:79:2c:07:b1:d4:f1:d3:ea:bc:49:d8:
    76:01:62:df:2b:b1:23:2c:37:6e:6f:eb:d6:d0:be:
    f4:ac:fb:d1:c4:22:99:c2:45:81:71:7f:d1:f1:82:
    31:0f:c4:1e:81:bd:1a:0e:9d:29:46:81:78:04:c1:
    ce:a2:0c:cf:48:bc:f2:3c:ae:87:b0:0d:5c:89:bd:
    fe:74:db:22:c6:2d:5b:63:df:b6:3c:af:ed:cb:07:
    54:d6:fd:bf:04:ef:f7:63:8a:59:c8:f4:ff:aa:fa:
    16:91:7d:f6:a2:7b:bd:67:98:7d:e4:2a:93:94:ef:
    07:33:20:d3:39:ac:6a:22:28:2a:0e:55:6d:7d:5d:
    3d:4b:d8:c7:ed:bb:d1:f5:b5:31:f5:c5:8f:2c:88:
    77:6b:ca:5d:b0:39:6a:a9:b0:55:f2:be:8c:cb:29:
    a3:25:99:8c:32:5a:54:1d:ec:26:97:6d:d2:3d:14:
    3a:cc:a3:86:ca:87:a6:b5:69:1c:c2:18:5a:68:18:
    fe:89
publicExponent: 3 (0x3)
privateExponent:
    00:82:05:58:82:e2:57:81:0f:c3:b3:00:38:75:5e:
    5a:33:85:06:87:7a:8e:da:c1:c6:62:10:70:91:8d:
    94:a6:d6:9f:70:c6:a3:e2:7f:48:7d:2c:8a:34:9a:
    c6:d5:1d:ea:e9:be:ab:7d:9c:f6:4e:78:ec:38:e2:
    25:6c:d0:bf:a6:1d:5a:76:8d:f6:8d:47:28:31:3a:
    f9:56:41:ea:1d:20:c2:1d:7a:49:9f:f2:8f:35:d4:
    a3:1d:fd:36:82:c1:bb:d6:d9:00:f6:55:36:a1:01:
    76:0a:82:bf:01:28:bc:09:be:1b:84:56:50:03:2b:
    df:16:b3:34:db:28:a1:7d:c8:85:cf:4e:e1:4c:83:
    7e:d9:d9:cb:79:e0:ab:fb:76:8e:c0:62:0d:70:19:
    1d:55:cb:4b:7e:c3:97:31:33:f3:e2:37:d4:5d:8d:
    2a:38:46:6f:49:97:c6:21:9c:f6:08:30:fb:3f:d0:
    c8:3b:86:65:87:25:04:30:54:66:00:41:99:e0:a2:
    bc:28:17:d6:90:97:99:78:54:5b:fa:12:a9:1a:d2:
    6a:79:16:76:83:39:55:73:b6:04:2c:1a:cf:6c:53:
    3b:eb:60:d7:87:44:73:15:40:5f:8d:3b:16:1c:3a:
    a9:ae:a6:24:6b:d1:7a:ab:bc:df:8e:63:4e:79:e0:
    5f:ab
prime1:
    00:e3:c0:a4:87:41:4f:8e:de:42:08:08:3f:25:55:
    59:fd:cf:4a:14:c6:ca:2b:82:2e:c0:76:e2:52:54:
    ec:6d:37:82:1c:a4:83:0a:61:27:55:6d:71:4b:8a:
    f5:ac:8b:e2:33:bd:79:b4:00:54:7e:65:c1:b1:20:
    e5:45:fb:4b:53:93:8f:18:3d:18:c3:54:1c:97:4c:
    24:3b:a6:f1:80:a5:7b:a3:63:fe:31:cc:71:82:1c:
    61:58:4a:f9:59:49:27:b6:90:8f:27:60:c7:ec:15:
    41:66:8a:12:e3:da:c4:19:06:85:5c:eb:c9:84:b6:
    52:68:8e:cf:33:24:46:c4:11
prime2:
    00:db:38:72:83:55:a9:31:4f:d2:69:87:1d:34:15:
    53:e2:4c:d2:c4:dc:17:7d:54:1e:0d:4f:e8:42:44:
    cf:fe:be:1f:24:7a:23:4c:db:ec:fa:46:a6:c8:aa:
    37:60:4b:fe:e6:f7:bc:26:d9:82:bc:89:33:32:b8:
    c4:4b:12:a7:b3:18:da:0a:d2:9c:42:c0:bb:d4:75:
    12:6c:57:b8:10:de:d1:34:52:2a:7a:1e:f1:e8:5f:
    bd:f7:65:9c:fc:5f:85:12:b3:f9:21:86:ab:bb:68:
    ca:30:b9:82:4d:37:f8:23:40:24:f3:3d:03:e9:fd:
    7b:64:dd:b4:31:8d:01:aa:f9
exponent1:
    00:97:d5:c3:04:d6:35:09:e9:81:5a:b0:2a:18:e3:
    91:53:df:86:b8:84:86:c7:ac:1f:2a:f9:ec:36:e3:
    48:48:cf:ac:13:18:57:5c:40:c4:e3:9e:4b:87:b1:
    f9:1d:b2:96:cd:28:fb:cd:55:8d:a9:99:2b:cb:6b:
```

```
exponent1:
    00:97:d5:c3:04:d6:35:09:e9:81:5a:b0:2a:18:e3:
    91:53:df:86:b8:84:86:c7:ac:1f:2a:f9:ec:36:e3:
    48:48:cf:ac:13:18:57:5c:40:c4:e3:9e:4b:87:b1:
    f9:1d:b2:96:cd:28:fb:cd:55:8d:a9:99:2b:cb:6b:
    43:83:fc:dc:e2:62:5f:65:7e:10:82:38:13:0f:88:
    18:27:c4:a1:00:6e:52:6c:ed:54:21:32:f6:56:bd:
    96:3a:dc:a6:3b:86:1a:79:b5:b4:c4:eb:2f:f2:b8:
    d6:44:5c:0c:97:e7:2d:66:04:58:e8:9d:31:03:24:
    36:f0:5f:34:cc:c2:d9:d8:0b
exponent2:
    00:92:25:a1:ac:e3:c6:20:df:e1:9b:af:68:cd:63:
    8d:41:88:8c:83:3d:64:fe:38:14:08:df:f0:2c:2d:
    df:ff:29:6a:18:51:6c:dd:e7:f3:51:84:6f:30:71:
    7a:40:32:a9:ef:4f:d2:c4:91:01:d3:06:22:21:d0:
    82:dc:b7:1a:77:65:e6:b1:e1:bd:81:d5:d2:8d:a3:
    61:9d:8f:d0:0b:3f:36:22:e1:71:a6:bf:4b:f0:3f:
    d3:fa:43:bd:fd:95:03:61:cd:50:c1:04:72:7c:f0:
    86:cb:26:56:de:25:50:17:80:18:a2:28:ad:46:a8:
    fc:ed:e9:22:cb:b3:56:71:fb
coefficient:
    00:c6:bd:48:5f:e8:06:0b:de:10:64:3d:b2:ab:5d:
    b8:0b:ab:2d:90:28:7b:48:fc:7f:60:76:bf:43:23:
    9a:4f:e7:3f:01:87:d6:45:6c:c1:97:29:ec:70:dc:
    8f:b2:93:25:d8:85:5b:e7:ac:18:64:99:60:e5:e3:
    37:91:b8:08:6c:89:ca:5f:88:a2:b8:bd:52:c4:2e:
    ba:26:4f:06:9e:ec:a5:58:f7:65:c4:c4:a3:4b:bd:
    13:59:af:08:9f:5a:eb:14:ec:fe:35:62:a6:50:f0:
    b8:c0:9f:41:cb:a3:a6:0c:56:79:c2:4d:7c:7e:e1:
    7a:61:ec:2c:d5:34:e2:03:48
ron@rons-mbp ~ %
```

```
ron@rons-mbp ~ % openssl pkey -pubin -in pubkey-A.pem -text -noout
RSA Public-Key: (2048 bit)
Modulus:
    00:c3:08:04:c4:53:83:41:97:a5:8c:80:54:b0:0d:
    87:4d:47:89:cb:37:d6:48:22:a9:93:18:a8:da:54:
    5e:fa:41:ef:29:29:f5:d3:be:ec:bb:c2:cf:4e:e8:
    2a:3f:ac:e0:5e:9e:01:3c:6b:71:75:b5:62:55:53:
    38:23:39:1f:79:2c:07:b1:d4:f1:d3:ea:bc:49:d8:
    76:01:62:df:2b:b1:23:2c:37:6e:6f:eb:d6:d0:be:
    f4:ac:fb:d1:c4:22:99:c2:45:81:71:7f:d1:f1:82:
    31:0f:c4:1e:81:bd:1a:0e:9d:29:46:81:78:04:c1:
    ce:a2:0c:cf:48:bc:f2:3c:ae:87:b0:0d:5c:89:bd:
    fe:74:db:22:c6:2d:5b:63:df:b6:3c:af:ed:cb:07:
    54:d6:fd:bf:04:ef:f7:63:8a:59:c8:f4:ff:aa:fa:
    16:91:7d:f6:a2:7b:bd:67:98:7d:e4:2a:93:94:ef:
    07:33:20:d3:39:ac:6a:22:28:2a:0e:55:6d:7d:5d:
    3d:4b:d8:c7:ed:bb:d1:f5:b5:31:f5:c5:8f:2c:88:
    77:6b:ca:5d:b0:39:6a:a9:b0:55:f2:be:8c:cb:29:
    a3:25:99:8c:32:5a:54:1d:ec:26:97:6d:d2:3d:14:
    3a:cc:a3:86:ca:87:a6:b5:69:1c:c2:18:5a:68:18:
    fe:89
Exponent: 3 (0x3)
ron@rons-mbp ~ %
```

```
ron@rons-mbp ~ % openssl pkey -in  privkey-C.pem -text -noout
RSA Private-Key: (2048 bit)
modulus:
    00:e5:df:de:d0:c7:92:03:ea:4e:36:2d:a3:00:e0:
    21:da:42:9d:0e:3b:b4:f4:4d:fe:aa:8e:de:ed:d8:
    73:ab:7d:40:d9:33:55:4f:85:be:c5:87:3d:a3:1b:
    a3:1d:b7:c1:85:50:fa:5e:1a:40:3a:04:40:08:55:
    62:2f:61:28:f1:19:72:15:c6:ba:6c:25:53:5d:a9:
    cb:39:32:80:45:1f:3c:6b:fd:83:76:e0:fe:42:e1:
    4e:8d:1a:68:fd:9a:a7:4e:6e:c4:69:ef:cb:31:19:
    df:5d:a1:3b:6d:4e:0d:6b:85:e3:59:95:33:d7:79:
    59:23:68:9c:6d:0c:92:81:76:d1:1e:0c:10:fe:11:
    f3:27:68:0a:36:25:65:52:7d:8b:23:6a:df:1d:c8:
    50:ba:81:3e:fc:fc:0d:20:9c:0d:bb:56:61:2d:b7:
    68:f7:a7:a5:55:a4:1a:2e:50:a8:c4:db:44:13:f4:
    e1:ea:d5:e5:3b:da:72:5b:fe:fe:ac:10:a9:0e:7d:
    db:e3:e8:a2:f6:0f:18:c8:27:4a:e9:ef:89:8c:80:
    32:a1:7a:1c:16:b4:75:93:3b:95:9d:7e:3a:03:78:
    39:ef:f1:bc:0c:6a:05:bd:6b:09:98:c9:93:78:30:
    a0:47:b1:c1:cd:13:ed:70:44:6e:cd:3d:fe:65:2a:
    93:03
publicExponent: 3 (0x3)
privateExponent:
    00:99:3f:e9:e0:85:0c:02:9c:34:24:1e:6c:ab:40:
    16:91:81:be:09:7d:23:4d:89:54:71:b4:94:9e:90:
    4d:1c:fe:2b:3b:77:8e:35:03:d4:83:af:7e:6c:bd:
    17:69:25:2b:ae:35:fc:3e:bc:2a:d1:58:2a:b0:38:
    ec:1f:96:1b:4b:66:4c:0e:84:7c:48:18:e2:3e:71:
    32:26:21:aa:d8:bf:7d:9d:53:ac:f9:eb:54:2c:96:
    34:5e:11:9b:53:bc:6f:89:9f:2d:9b:f5:32:20:bb:
    ea:3e:6b:7c:f3:89:5e:47:ae:97:91:0e:22:8f:a6:
    3b:6c:f0:68:48:b3:0c:56:4d:f2:5c:84:37:ba:58:
    02:2a:10:24:fa:8b:d8:a7:71:e0:79:75:2f:57:ef:
    13:53:28:b3:f0:2c:21:32:c9:b3:62:28:b8:b2:b4:
    a6:6f:f6:c3:83:70:1f:71:21:ab:fd:88:db:18:93:
    df:2c:c3:68:91:e4:84:35:fc:4a:9b:88:05:d2:64:
    71:fd:6d:46:f9:bc:e1:87:ac:43:8b:0f:fd:f6:86:
    fc:0d:bc:5f:a2:82:d7:20:20:5c:ff:e1:02:b7:46:
    4a:0c:6c:4a:9b:27:2b:33:95:b5:69:d0:16:75:fc:
    df:b4:ca:a1:37:f0:9a:2b:2c:9e:51:60:b3:bd:51:
    e6:db
prime1:
    00:fc:af:7f:c8:ab:dd:72:b0:7b:e6:d4:a1:8d:21:
    6e:25:1f:0e:c8:a9:d8:43:42:4c:69:17:e1:54:b9:
    72:d0:d2:e5:00:b9:c5:5e:9f:b8:e6:c2:27:e4:da:
    06:92:1b:fa:a5:25:51:3b:55:be:88:98:90:33:31:
    7b:b8:93:d1:e0:20:35:d9:45:d0:94:09:d4:07:fe:
    37:8d:60:82:13:17:54:94:dd:dd:88:5f:86:a2:fd:
    19:bf:ef:c3:c1:5d:5e:2b:03:12:09:42:b1:d2:f6:
    0e:46:8c:19:a2:71:b6:21:d7:a7:44:14:7c:27:84:
    c4:95:6a:6a:71:46:0f:64:1f
prime2:
    00:e8:e3:c5:f4:ba:b0:7d:37:d3:eb:e9:b2:13:35:
    e4:95:4e:2c:4f:70:09:70:7b:77:c7:fc:d8:86:9a:
    fa:af:d5:34:4b:67:e3:10:af:fc:99:4e:54:06:2a:
    97:94:ac:93:56:49:c5:d7:d1:f2:3f:c8:73:78:d9:
```

```
prime2:
    00:e8:e3:c5:f4:ba:b0:7d:37:d3:eb:e9:b2:13:35:
    e4:95:4e:2c:4f:70:09:70:7b:77:c7:fc:d8:86:9a:
    fa:af:d5:34:4b:67:e3:10:af:fc:99:4e:54:06:2a:
    97:94:ac:93:56:49:c5:d7:d1:f2:3f:c8:73:78:d9:
    88:d6:2e:f2:c0:32:b1:57:a1:f4:24:75:9f:be:7e:
    6d:58:38:d5:79:83:61:23:af:02:04:43:69:8f:e5:
    f1:4a:2d:e8:f4:93:30:9f:da:3d:42:e0:fd:71:f9:
    fc:32:ed:f7:cf:55:7f:2e:e0:da:8b:e4:ae:de:aa:
    bc:eb:e8:c2:7f:83:20:54:9d
exponent1:
    00:a8:74:ff:db:1d:3e:4c:75:a7:ef:38:6b:b3:6b:
    9e:c3:6a:09:db:1b:e5:82:2c:32:f0:ba:96:38:7b:
    a1:e0:8c:98:ab:26:83:94:6a:7b:44:81:6f:ed:e6:
    af:0c:12:a7:18:c3:8b:7c:e3:d4:5b:10:60:22:20:
    fd:25:b7:e1:40:15:79:3b:83:e0:62:b1:38:05:54:
    25:08:eb:01:62:0f:8d:b8:93:e9:05:95:04:6c:a8:
    bb:d5:4a:82:80:e8:e9:72:02:0c:06:2c:76:8c:a4:
    09:84:5d:66:6c:4b:ce:c1:3a:6f:82:b8:52:c5:03:
    2d:b8:f1:9c:4b:84:0a:42:bf
exponent2:
    00:9b:42:83:f8:7c:75:a8:cf:e2:9d:46:76:b7:79:
    43:0e:34:1d:8a:4a:b0:f5:a7:a5:2f:fd:e5:af:11:
    fc:75:38:cd:87:9a:97:60:75:53:10:de:e2:ae:c7:
    0f:b8:73:0c:e4:31:2e:8f:e1:4c:2a:85:a2:50:91:
    05:e4:1f:4c:80:21:cb:8f:c1:4d:6d:a3:bf:d4:54:
    48:e5:7b:38:fb:ac:eb:6d:1f:56:ad:82:46:5f:ee:
    a0:dc:1e:9b:4d:b7:75:bf:e6:d3:81:eb:53:a1:51:
    52:cc:9e:a5:34:e3:aa:1f:40:91:b2:98:74:94:71:
    d3:47:f0:81:aa:57:6a:e3:13
coefficient:
    00:dc:33:eb:a6:58:7c:29:e8:a9:25:14:36:8c:e4:
    ab:d3:25:d1:0b:bc:46:36:8b:fa:db:98:7e:fc:81:
    30:72:98:7d:a6:48:c9:ea:a7:fb:20:23:62:03:86:
    72:32:33:0a:a7:80:e4:37:b2:e3:18:e5:07:3a:89:
    d0:ac:8e:ec:38:50:ef:ff:0a:d1:23:57:23:cb:da:
    6c:86:4a:cf:38:b3:ee:5a:28:05:59:26:47:93:99:
    ed:3c:c8:82:c3:ca:e4:62:7c:dc:f8:c0:3d:86:f1:
    df:cc:bb:45:ce:ea:c8:7c:a1:d8:b9:69:fe:83:99:
    34:ab:d2:3c:61:ee:6f:30:0b
ron@rons-mbp ~ % %
```

```
ron@rons-mbp ~ % openssl pkey -pubin -in pubkey-C.pem -text -noout
RSA Public-Key: (2048 bit)
Modulus:
    00:c3:08:04:c4:53:83:41:97:a5:8c:80:54:b0:0d:
    87:4d:47:89:cb:37:d6:48:22:a9:93:18:a8:da:54:
    5e:fa:41:ef:29:29:f5:d3:be:ec:bb:c2:cf:4e:e8:
    2a:3f:ac:e0:5e:9e:01:3c:6b:71:75:b5:62:55:53:
    38:23:39:1f:79:2c:07:b1:d4:f1:d3:ea:bc:49:d8:
    76:01:62:df:2b:b1:23:2c:37:6e:6f:eb:d6:d0:be:
    f4:ac:fb:d1:c4:22:99:c2:45:81:71:7f:d1:f1:82:
    31:0f:c4:1e:81:bd:1a:0e:9d:29:46:81:78:04:c1:
    ce:a2:0c:cf:48:bc:f2:3c:ae:87:b0:0d:5c:89:bd:
    fe:74:db:22:c6:2d:5b:63:df:b6:3c:af:ed:cb:07:
    54:d6:fd:bf:04:ef:f7:63:8a:59:c8:f4:ff:aa:fa:
    16:91:7d:f6:a2:7b:bd:67:98:7d:e4:2a:93:94:ef:
    07:33:20:d3:39:ac:6a:22:28:2a:0e:55:6d:7d:5d:
    3d:4b:d8:c7:ed:bb:d1:f5:b5:31:f5:c5:8f:2c:88:
    77:6b:ca:5d:b0:39:6a:a9:b0:55:f2:be:8c:cb:29:
    a3:25:99:8c:32:5a:54:1d:ec:26:97:6d:d2:3d:14:
    3a:cc:a3:86:ca:87:a6:b5:69:1c:c2:18:5a:68:18:
    fe:89
Exponent: 3 (0x3)
ron@rons-mbp ~ %
```

- Step 1. c - I generated a certificate signing request.

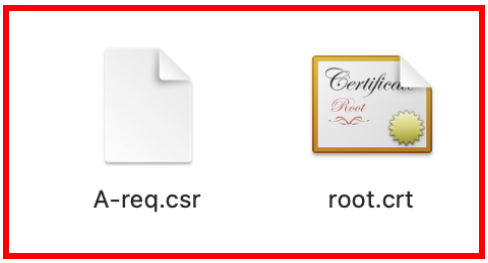
```
ron@rons-mbp ~ % openssl req -new -key privkey-A.pem -out A-req.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:New York
Locality Name (eg, city) []:New York
Organization Name (eg, company) []:John Jay
Organizational Unit Name (eg, section) []:CSCI
Common Name (eg, fully qualified host name) []:Ron
Email Address []:ron.gassner@jjay.cuny.edu

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:pass
ron@rons-mbp ~ %
```

- I tried the :”Aside:” note again and generated a self-sign certificate for the CA.
- After I tried to see the certificate as text.

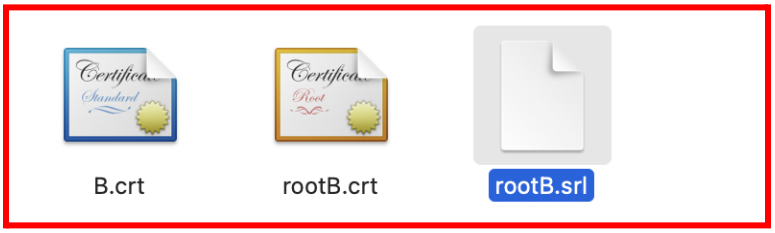
```
ron@rons-mbp ~ % openssl req -x509 -new -nodes -key privkey-c.pem -sha256 -days 1024 -out root.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:New York
Locality Name (eg, city) []:New York
Organization Name (eg, company) []:John Jay
Organizational Unit Name (eg, section) []:CSCI
Common Name (eg, fully qualified host name) []:CA
Email Address []:c.a@jjay.cuny.edu
ron@rons-mbp ~ %
```

```
ron@rons-mbp ~ % openssl x509 -in root.crt -text -noout
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            a6:b2:d4:d2:9d:10:2d:d7
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=New York, L=New York, O=John Jay, OU=CSCI, CN=CA/emailAddress=c.a@jjay.cuny.edu
        Validity
            Not Before: Mar 28 17:04:08 2024 GMT
            Not After : Jan 16 17:04:08 2027 GMT
        Subject: C=US, ST=New York, L=New York, O=John Jay, OU=CSCI, CN=CA/emailAddress=c.a@jjay.cuny.edu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:e5:df:de:d0:c7:92:03:ea:4e:36:2d:a3:00:e0:
                    21:da:42:9d:0e:3b:b4:f4:4d:fe:aa:8e:de:ed:d8:
                    73:ab:7d:40:d9:33:55:4f:85:be:c5:87:3d:a3:1b:
                    a3:1d:b7:c1:85:50:fa:5e:1a:40:3a:04:40:08:55:
                    62:2f:61:28:f1:19:72:15:c6:ba:6c:25:53:5d:a9:
                    cb:39:32:80:45:1f:3c:6b:fd:83:76:e0:fe:42:e1:
                    4e:8d:1a:68:fd:9a:a7:4e:6e:c4:69:ef:cb:31:19:
                    df:5d:a1:3b:6d:4e:0d:6b:85:e3:59:95:33:d7:79:
                    59:23:68:9c:6d:0c:92:81:76:d1:1e:0c:10:fe:11:
                    f3:27:68:0a:36:25:65:52:7d:8b:23:6a:df:1d:c8:
                    50:ba:81:3e:fc:fc:0d:20:9c:0d:bb:56:61:2d:b7:
                    68:f7:a7:a5:55:a4:1a:2e:50:a8:c4:db:44:13:f4:
                    e1:ea:d5:e5:3b:da:72:5b:fe:fe:ac:10:a9:0e:7d:
                    db:e3:e8:a2:f6:0f:18:c8:27:4a:e9:ef:89:8c:80:
                    32:a1:7a:1c:16:b4:75:93:3b:95:9d:7e:3a:03:78:
                    39:ef:f1:bc:0c:6a:05:bd:6b:09:98:c9:93:78:30:
                    a0:47:b1:c1:cd:13:ed:70:44:6e:cd:3d:fe:65:2a:
                    93:03
                Exponent: 3 (0x3)
    Signature Algorithm: sha256WithRSAEncryption
         c5:52:7e:82:4d:b1:f0:8b:f6:1f:71:9e:10:5a:b8:01:23:0b:
         e2:88:40:4e:3a:60:eb:ed:18:e4:80:2e:cd:62:5b:15:46:c4:
         5b:97:24:a0:8f:f7:f7:22:71:40:ef:fa:71:bb:df:1f:92:d5:
         ba:6c:3c:2f:64:a1:e9:ba:a0:28:aa:02:05:43:ce:13:0e:dc:
         94:4c:d6:a8:bc:63:23:10:28:ab:c8:a7:10:fb:42:d8:db:90:
         4d:38:14:be:73:31:01:44:73:83:e5:ae:00:7f:25:5d:fe:62:
         c1:aa:fa:dd:78:6f:44:85:80:31:8d:d2:fd:07:fc:25:02:3d:
         b7:06:93:1b:cd:39:1b:81:b4:c9:c6:b4:02:c0:c5:a0:0d:76:
         e0:34:cd:1d:70:d7:3d:93:0e:bc:76:ce:98:f6:5a:9b:93:ab:
         11:59:d2:2c:fc:12:c7:3b:6c:a2:be:66:ec:32:d7:18:24:22:
         7b:e0:4b:c1:6e:58:52:1f:98:34:1b:dd:e2:0c:3e:23:30:3e:
         a0:f5:f1:f7:9f:09:bd:3c:f4:ff:d0:8a:a3:1f:6e:23:d0:23:
         e2:70:7a:3e:09:95:70:cd:2a:c3:71:8c:17:65:f3:f5:3f:dd:
         cd:51:cd:2e:a9:c5:a9:83:82:c7:ad:61:38:16:df:d6:4e:e1:
         b4:18:b8:1e
ron@rons-mbp ~ %
```



- Step 1. d - As my own CA, I generated and signed a certificate for Alice (who is also me)
- The certificate will be valid for 500 days, and I used the sha256 algorithm to hash it.

```
ron@rons-mbp ~ % openssl x509 -req -in A-req.csr -CA root.crt -CAkey privkey-c.pem -CAcreateserial -out A.crt -days 500 -sha256
Signature ok
subject=/C=US/ST=New York/L=New York/O=John Jay/OU=CSCI/CN=Ron/emailAddress=ron.gassner@jjay.cuny.edu
Getting CA Private Key
ron@rons-mbp ~ %
```

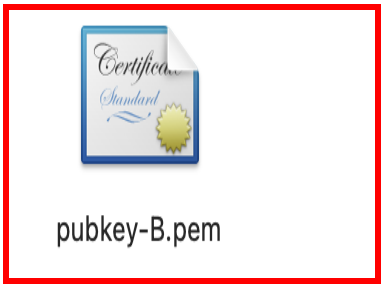


- Step 2. a - I verified Bob's (Lucas's) public certificate

```
ron@rons-mbp ~ % openssl verify -CAfile rootB.crt B.crt
B.crt: OK
ron@rons-mbp ~ %
```

- Step 2. b - I extracted Bob's (Lucase's) public key.

```
ron@rons-mbp ~ % openssl x509 -pubkey -in B.crt -noout > pubkey-B.pem
ron@rons-mbp ~ %
```



- Step 2. c - I tried to encrypt the text file ABOstory.text using Bob's (Lucas's) public key, but it did not work.

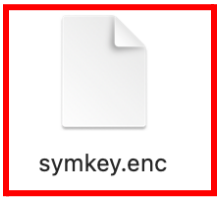
```
ron@rons-mbp ~ % openssl pkeyutl -encrypt -in ABOstory.text -pubin -inkey pubkey-B.pem -out ciphertext.bin
Public Key operation error
7902240448:error:04FFF06E:rsa routines:CRYPTO_internal:data too large for key size:/AppleInternal/Library/BuildRoots/5ad84cef-5dac-11ee-99ed-c6501008687b/Library/Caches/com.apple.xbs/Sources/libressl/libressl-3.3/crypto/rsa/rsa_pk1.c:151:
ron@rons-mbp ~ %
```

- Step 3. a - So, I generated a symmetric key.

```
ron@rons-mbp ~ % openssl rand -base64 32 -out symkey.pem
ron@rons-mbp ~ %
```

- Step 3. b - I encrypted symkey.pem using Bob's (Lucas's) public key.

```
ron@rons-mbp ~ % openssl pkeyutl -encrypt -in symkey.pem -pubin -inkey pubkey-B.pem -out symkey.enc
```



- Step 3. c - Then, I hashed symkey.pem and encrypted it using my own (Alice's) private key.

```
ron@rons-mbp ~ % openssl dgst -sha1 -sign privkey-A.pem -out signature.bin symkey.pem
```

- Eventually, after Bob (Lucas) was able to decrypt symkey.enc using his private key, and verified my identity with the certificate he extracted my (Alice's) public key. I was able to encrypt the ABOstory.text using the symmetric key and send it to Bob (Lucas) so he can encrypt it.

```
ron@rons-mbp ~ % openssl enc -aes-256-cbc -pass file:symkey.pem -p -md sha256 -in ABOstory.text -out ciphertext.bin
salt=D968A6BDE63BB532
key=CB6402B8CEBE845B9B92225DEE4A224CAF39F20583645B03501E0F456E5E47E8
iv =93057972545B35E1F8C8AD2EC4C4A95D
ron@rons-mbp ~ %
```

Lucas(Bob):

- Step 1. a - I generated my private key.
- For the private key, I used the RSA algorithm, set opt to value, set the size of the key to 2048 bits, and set the public exponent e to 3. It outputs the file privkey-B.pem.
- Step 1. b - then, I generated a public key from privkey-B.pem, and output a public key as pubkey-B.pem.
- I viewed the keys in plain text.

- ```
  Last login: Mon Mar 18 17:13:07 on ttys002
  (base) ------------------------------------------------------------------------
  ~ » ls                                                    lucasyao@lucass-mbp
  Applications                     Music
  Applications (Parallels)         Parallels
  Debian 11.x 64-bit Arm.vmwarevm Pictures
  Desktop                          Public
  Documents                        Virtual Machines.localized
  Downloads                        Windows 11 64-bit Arm.vmwarevm
  Library                          Windows 11.vmwarevm
  Lucas                            dotnet
  Movies                           version
  (base) ------------------------------------------------------------------------
  ~ » cd lucas                                              lucasyao@lucass-mbp
  (base) ------------------------------------------------------------------------
  ~/lucas » openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -pkeyopt rsa_keygen_pubexp:3 -out privkey-B.pem
  ...........................................................................+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
  ...................+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
  (base) ------------------------------------------------------------------------
  ~/lucas » openssl pkey -in privkey-B.pem -pubout 0out pubkey-B.pem
  pkey: Use -help for summary.
  (base) ------------------------------------------------------------------------
  ~/lucas » openssl pkey -in privkey-B.pem -pubout -out pubkey-B.pem
  (base) ------------------------------------------------------------------------
  ~/lucas » openssl pkey -in privkey-B.pem -text -noout     lucasyao@lucass-mbp
  Private-Key: (2048 bit, 2 primes)
  modulus:
      00:e6:6d:27:f2:d8:2a:bc:ab:91:39:ff:d3:15:d1:
      f3:ce:d9:a6:11:f3:8c:56:c9:55:04:59:fd:7c:62:
      ae:3b:b8:38:74:4d:1e:2b:c8:35:bd:d2:78:ee:2b:
      70:97:05:5e:13:40:41:4a:79:b7:40:80:44:97:53:
      c9:64:35:1c:1b:80:95:fa:e2:4a:c7:23:c2:6f:0a:
      3d:e5:be:4a:f7:0c:55:bd:41:e5:05:60:66:41:0f:
      20:93:2c:90:95:ad:c4:d7:40:bd:f9:3b:ba:b5:42:
      17:b4:5d:a9:15:ee:ef:4e:7f:2d:04:16:72:fc:34:
      54:76:d2:2e:48:a3:5c:6d:81:4b:5f:4a:30:86:74:
      49:e6:20:37:16:94:14:ee:01:08:8b:11:8e:57:c0:
      16:51:de:88:a0:d3:a9:ae:2c:fa:51:3a:c4:8f:23:
      f5:d2:fe:c1:7f:9b:82:f3:a8:4e:34:07:a0:8b:b2:
      74:53:59:b8:bf:17:13:69:06:a9:0c:45:bc:af:f7:
      0d:e1:eb:2a:16:5a:1e:a4:6e:4a:01:8f:43:82:7f:
      9e:85:f2:c0:6c:91:f9:a7:5a:1a:02:77:72:fe:b4:
      3d:7b:0f:6a:87:bb:46:f6:44:98:18:d7:05:28:34:
      b8:20:f3:c5:ee:8c:9f:a1:8e:0e:92:5e:cf:c5:be:
      0e:87
  publicExponent: 3 (0x3)
  privateExponent:
      00:99:9e:1a:a1:e5:71:d3:1d:0b:7b:ff:e2:0e:8b:
      f7:df:3b:c4:0b:f7:b2:e4:86:38:ad:91:53:a8:41:
  ```
- ```
      c9:7d:25:7a:f8:33:69:72:85:79:29:36:fb:49:72:
      4b:0f:58:e9:62:2a:d6:31:a6:7a:2b:00:2d:ba:37:
      db:98:23:68:12:55:b9:51:ec:31:da:17:d6:f4:b1:
      7e:99:29:87:4f:5d:8e:7e:2b:ee:03:95:99:80:b4:
      c0:62:1d:b5:b9:1e:83:3a:2b:29:50:d2:7c:78:d6:
      ba:78:3e:70:b9:49:f4:de:ff:73:58:0e:f7:52:cd:
      8d:a4:8c:1e:db:17:92:f3:aa:43:be:e3:6e:1d:0a:
      66:1c:d0:2c:59:67:0b:b8:54:05:b6:2c:7e:b2:a7:
      27:55:d5:9c:88:67:b4:22:64:2f:96:f5:d2:58:ae:
      6a:a7:d1:33:8d:c7:7d:3e:ef:65:86:e5:05:44:45:
      23:91:24:87:f5:6d:63:b0:d5:b4:13:99:b3:fb:d5:
      e0:af:59:90:52:18:a4:eb:46:8f:86:c1:61:2e:a3:
      06:4c:97:d8:61:16:57:47:f9:de:b6:4e:44:ac:5e:
      38:cb:a9:67:6a:43:cf:40:b0:ad:2d:ab:44:59:5b:
      06:8b:40:3e:7e:46:7a:fa:c9:b3:2d:8a:83:d6:78:
      e2:db
  prime1:
      00:f3:02:8b:91:b5:36:31:85:ba:af:0f:c1:37:86:
      a2:ab:46:6f:b3:8a:f5:ac:d1:61:31:62:6b:8b:89:
      f7:14:40:c7:b9:2c:2a:e7:6c:ae:83:3f:c2:f3:a7:
      ef:09:74:7d:57:fc:08:fc:e1:91:e3:7a:97:90:de:
      91:01:06:6c:66:13:53:97:02:1d:cc:41:cc:70:4a:
      f9:f6:00:20:a2:dc:ee:68:d9:b1:31:e7:db:b9:47:
      be:20:43:68:5e:31:e8:b9:32:45:40:6f:43:29:e5:
      3d:c6:46:81:f3:20:60:7f:7b:29:5c:0d:de:07:de:
      89:3a:66:00:e5:58:31:5d:95
  prime2:
      00:f2:be:69:79:a5:ae:7f:35:2d:45:80:b8:4b:d2:
      e0:54:b3:5f:1c:c0:cf:ae:7f:bc:ec:71:cc:8f:f0:
      9f:9e:ae:02:4f:dd:f3:6e:6a:96:70:eb:2d:53:6d:
      52:2c:75:32:c0:a9:41:c2:18:11:09:54:5b:6d:01:
      35:19:e8:72:c8:a2:e2:a5:d8:c7:05:59:68:b6:f8:
      8a:7c:b7:4c:8e:df:9c:ac:39:5d:c9:f3:14:bd:73:
      a5:2b:ad:99:ad:ca:3e:2f:17:4c:0e:f9:12:66:2f:
      fd:ce:0d:d4:2b:81:cb:ae:d4:ea:0c:23:44:df:4a:
      d6:47:68:0e:24:ab:d7:5c:ab
  exponent1:
      00:a2:01:b2:61:23:79:76:59:27:1f:5f:d6:25:04:
      6c:72:2e:f5:22:5c:a3:c8:8b:96:20:ec:47:b2:5b:
      fa:0d:80:85:26:1d:71:ef:9d:c9:ac:d5:2c:a2:6f:
      f4:b0:f8:53:8f:fd:5b:53:41:0b:ec:fc:65:0b:3f:
      0b:56:04:48:44:0c:e2:64:ac:13:dd:81:32:f5:87:
      51:4e:aa:c0:6c:93:49:9b:3b:cb:76:9a:92:7b:85:
      29:6a:d7:9a:e9:76:9b:26:21:83:80:4a:2c:c6:98:
      d3:d9:84:56:a2:15:95:aa:52:1b:92:b3:e9:5a:94:
      5b:7c:44:00:98:e5:76:3e:63
  exponent2:
      00:a1:d4:46:51:19:1e:ff:78:c8:d9:00:7a:dd:37:
      40:38:77:94:bd:d5:df:c9:aa:7d:f2:f6:88:5f:f5:
  ```

```
    5b:7c:44:00:98:e5:76:3e:63
exponent2:
    00:a1:d4:46:51:19:1e:ff:78:c8:d9:00:7a:dd:37:
    40:38:77:94:bd:d5:df:c9:aa:7d:f2:f6:88:5f:f5:
    bf:bf:1e:ac:35:3e:a2:49:9c:64:4b:47:73:8c:f3:
    8c:1d:a3:77:2b:1b:81:2c:10:0b:5b:8d:92:48:ab:
    78:bb:f0:4c:85:c1:ec:6e:90:84:ae:3b:9b:24:a5:
    b1:a8:7a:33:09:ea:68:72:d0:e9:31:4c:b8:7e:4d:
    18:c7:c9:11:1e:86:d4:1f:64:dd:5f:50:b6:ee:ca:
    a9:34:09:38:1d:01:32:74:8d:f1:5d:6c:d8:94:dc:
    8e:da:45:5e:c3:1d:3a:3d:c7
coefficient:
    00:ce:7d:e7:07:8d:5f:87:09:07:0f:39:86:61:ae:
    0c:31:0a:c3:08:cd:54:33:f9:42:bd:79:4e:c4:cc:
    eb:44:8a:13:7c:e2:09:14:f8:b8:7c:bc:01:4e:ea:
    14:af:aa:0a:64:6a:27:62:18:45:f2:3d:9d:32:bd:
    82:16:cc:89:40:a7:ca:2d:2f:a1:29:9d:4e:cf:9c:
    4c:36:1f:38:32:eb:7e:16:c2:e0:3a:2d:0e:e8:8a:
    2d:a2:ec:ef:db:18:5a:9a:8e:34:f9:d1:cc:87:60:
    58:a8:7c:d5:3c:c1:2b:70:06:54:23:bf:e6:ae:a9:
    38:4e:43:6a:43:7a:99:b0:01
(base) ------------------------------------------------------------------------
~/lucas » openssl pkey -pubin -in pubkey-B.pem -text -noout
Public-Key: (2048 bit)
Modulus:
    00:e6:6d:27:f2:d8:2a:bc:ab:91:39:ff:d3:15:d1:
    f3:ce:d9:a6:11:f3:8c:56:c9:55:04:59:fd:7c:62:
    ae:3b:b8:38:74:4d:1e:2b:c8:35:bd:d2:78:ee:2b:
    70:97:05:5e:13:40:41:4a:79:b7:40:80:44:97:53:
    c9:64:35:1c:1b:80:95:fa:e2:4a:c7:23:c2:6f:0a:
    3d:e5:be:4a:f7:0c:55:bd:41:e5:05:60:66:41:0f:
    20:93:2c:90:95:ad:c4:d7:40:bd:f9:3b:ba:b5:42:
    17:b4:5d:a9:15:ee:ef:4e:7f:2d:04:16:72:fc:34:
    54:76:d2:2e:48:a3:5c:6d:81:4b:5f:4a:30:86:74:
    49:e6:20:37:16:94:14:ee:01:08:8b:11:8e:57:c0:
    16:51:de:88:a0:d3:a9:ae:2c:fa:51:3a:c4:8f:23:
    f5:d2:fe:c1:7f:9b:82:f3:a8:4e:34:07:a0:8b:b2:
    74:53:59:b8:bf:17:13:69:06:a9:0c:45:bc:af:f7:
    0d:e1:eb:2a:16:5a:1e:a4:6e:4a:01:8f:43:82:7f:
    9e:85:f2:c0:6c:91:f9:a7:5a:1a:02:77:72:fe:b4:
    3d:7b:0f:6a:87:bb:46:f6:44:98:18:d7:05:28:34:
    b8:20:f3:c5:ee:8c:9f:a1:8e:0e:92:5e:cf:c5:be:
    0e:87
Exponent: 3 (0x3)
(base) ------------------------------------------------------------------------
```

- Then, I repeated the process for the same keys in Certificate Authority

```
~/lucas » openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -pkeyopt rsa_keygen_pubexp:3 -out privkey-CA.pem                  127 ↵ lucasyao@lucass-mbp
.............................+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.....................+++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++
.....................................+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.....................................................
.....................................................................................................................................................
.....................................................................................................+++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++*.......+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
(base) ------------------------------------------------------------------------------------------------------------------------------------
~/lucas » openssl pkey -in privkey-CA.pem -pubout 0out pubkey-CA.pem                                                  lucasyao@lucass-mbp
pkey: Use -help for summary.
(base) ------------------------------------------------------------------------------------------------------------------------------------
~/lucas » openssl pkey -in privkey-CA.pem -pubout -out pubkey-CA.pem                                                1 ↵ lucasyao@lucass-mbp
(base) ------------------------------------------------------------------------------------------------------------------------------------
~/lucas » openssl pkey -pubin -in pubkey-CA.pem -text -noout                                                         lucasyao@lucass-mbp
Public-Key: (2048 bit)
Modulus:
    00:c5:c3:dd:75:1e:6b:42:e2:9b:21:02:0a:55:c6:
    80:93:2f:c0:89:3c:35:b7:65:23:20:eb:89:52:a1:
    63:77:72:a9:e6:a4:ff:7b:f9:f4:2e:8d:52:99:62:
    2e:13:c5:92:30:df:6c:8e:a8:ca:48:7f:05:bd:2c:
    e6:8b:6d:70:08:c8:25:9f:74:9f:07:54:89:ba:45:
    9d:0c:e1:24:56:65:32:6a:b8:4b:57:ea:43:26:e8:
    cf:ba:dc:43:96:f5:82:b7:15:1e:9a:ec:f6:b3:43:
    98:77:a6:25:3a:f7:a2:5b:6d:f4:89:d9:31:e5:7b:
    21:0c:65:78:e5:7c:18:48:a8:fb:9e:d7:c4:1a:01:
    e8:87:6d:1a:03:81:a2:58:ff:30:e1:67:b9:56:fc:
    e8:e3:44:ac:a4:48:b2:1b:3d:cc:d1:4c:00:8a:04:
    36:f8:77:0a:58:75:8d:ff:2f:fd:9e:0e:e7:aa:46:
    9d:23:41:6d:f2:cd:4c:10:33:d1:48:63:43:40:71:
    f4:dd:8d:b5:56:9d:12:20:ff:7e:1a:4e:91:2e:f4:
    10:59:86:2c:fd:f4:b4:b5:cf:0f:ed:50:f6:ac:14:
    5f:b7:fa:fc:1a:84:23:4c:df:88:28:52:ea:3b:87:
    8e:76:f1:18:8c:4b:4a:18:1f:8d:ce:e3:58:76:fe:
    68:3d
Exponent: 3 (0x3)
(base) ------------------------------------------------------------------------------------------------------------------------------------
~/lucas » openssl pkey -in privkey-CA.pem -text -noout                                                               lucasyao@lucass-mbp
Private-Key: (2048 bit, 2 primes)
modulus:
    00:c5:c3:dd:75:1e:6b:42:e2:9b:21:02:0a:55:c6:
    80:93:2f:c0:89:3c:35:b7:65:23:20:eb:89:52:a1:
    63:77:72:a9:e6:a4:ff:7b:f9:f4:2e:8d:52:99:62:
    2e:13:c5:92:30:df:6c:8e:a8:ca:48:7f:05:bd:2c:
    e6:8b:6d:70:08:c8:25:9f:74:9f:07:54:89:ba:45:
    9d:0c:e1:24:56:65:32:6a:b8:4b:57:ea:43:26:e8:
```

- Step 1. c -Then, I generated a certificate signing request called B-req.csr :
- I created and processed signing requests
- I generated a new certificate request, and I input some information with my identity info
- It signs the request with my private key

-
```
~/lucas » openssl req -new -key privkey-B.pem -out B-req.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:New York
Locality Name (eg, city) []:New York
Organization Name (eg, company) [Internet Widgits Pty Ltd]:John Jay
Organizational Unit Name (eg, section) []:CSCI
Common Name (e.g. server FQDN or YOUR name) []:Lucas
Email Address []:lu.yao@jjay.cuny.edu

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:pass
An optional company name []:
(base)
```
- Step 1. d - Here, I generated rootB.crt with the prickly-CA.pem
-
```
~/lucas » openssl req -x509 -new -nodes -key privkey-CA.pem -sha256 -days 1024 -out rootB.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:New York
Locality Name (eg, city) []:New York
Organization Name (eg, company) [Internet Widgits Pty Ltd]:John Jay
Organizational Unit Name (eg, section) []:CSCI
Common Name (e.g. server FQDN or YOUR name) []:CA
Email Address []:c.a@jjay.cuny.edu
(base)
```
- Completed self-signature:
-
```
~/lucas » openssl x509 -req -in B-req.csr -CA rootB.crt -CAkey privkey-CA.pem -CAcreateserial -out B.crt -days 500 -sha256
Certificate request self-signature ok
subject=C = US, ST = New York, L = New York, O = John Jay, OU = CSCI, CN = Lucas, emailAddress = lu.yao@jjay.cuny.edu
(base)
```
-

Lucas

Name	Date Modified	Size	Kind
pubkey-A.pem	Today, 10:50 AM	451 bytes	printabl...archive
root.srl	Yesterday, 1:28 PM	17 bytes	Document
root.crt	Yesterday, 1:28 PM	1 KB	certificate
A.crt	Yesterday, 1:28 PM	1 KB	certificate
B.crt	Yesterday, 1:27 PM	1 KB	certificate
rootB.srl	Yesterday, 1:27 PM	41 bytes	Document
rootB.crt	Yesterday, 1:27 PM	1 KB	certificate
B-req.csr	Yesterday, 1:13 PM	1 KB	Document
pubkey-CA.pem	Yesterday, 12:47 PM	451 bytes	printabl...archive
privkey-CA.pem	Yesterday, 12:46 PM	2 KB	printabl...archive
privkey-B.pem	Yesterday, 12:23 PM	2 KB	printabl...archive

- After completing the keys and certificates, Ron and I exchanged our certificates, and I viewed the certificate as text from Ron:

```
(base)
~/lucas » openssl x509 -in A.crt -text -noout              lucasyao@lucass-mbp
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            b1:22:b2:cb:49:4b:05:1c
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = New York, L = New York, O = John Jay, OU = CSCI, CN = CA, emailAddress = c.a@jjay.cuny.edu
        Validity
            Not Before: Mar 28 17:20:18 2024 GMT
            Not After : Aug 10 17:20:18 2025 GMT
        Subject: C = US, ST = New York, L = New York, O = John Jay, OU = CSCI, CN = Ron, emailAddress = ron.gassner@jjay.cuny.edu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c3:08:04:c4:53:83:41:97:a5:8c:80:54:b0:0d:
                    87:4d:47:89:cb:37:d6:48:22:a9:93:18:a8:da:54:
                    5e:fa:41:ef:29:29:f5:d3:be:ec:bb:c2:cf:4e:e8:
                    2a:3f:ac:e0:5e:9e:01:3c:6b:71:75:b5:62:55:53:
                    38:23:39:1f:79:2c:07:b1:d4:f1:d3:ea:bc:49:d8:
                    76:01:62:df:2b:b1:23:2c:37:6e:6f:eb:d6:d0:be:
                    f4:ac:fb:d1:c4:22:99:c2:45:81:71:7f:d1:f1:82:
                    31:0f:c4:1e:81:bd:1a:0e:9d:29:46:81:78:04:c1:
                    ce:a2:0c:cf:48:bc:f2:3c:ae:87:b0:0d:5c:89:bd:
                    fe:74:db:22:c6:2d:5b:63:df:b6:3c:af:ed:cb:07:
                    54:d6:fd:bf:04:ef:f7:63:8a:59:c8:f4:ff:aa:fa:
                    16:91:7d:f6:a2:7b:bd:67:98:7d:e4:2a:93:94:ef:
                    07:33:20:d3:39:ac:6a:22:28:2a:0e:55:6d:7d:5d:
                    3d:4b:d8:c7:ed:bb:d1:f5:b5:31:f5:c5:8f:2c:88:
                    77:6b:ca:5d:b0:39:6a:a9:b0:55:f2:be:8c:cb:29:
                    a3:25:99:8c:32:5a:54:1d:ec:26:97:6d:d2:3d:14:
                    3a:cc:a3:86:ca:87:a6:b5:69:1c:c2:18:5a:68:18:
                    fe:89
                Exponent: 3 (0x3)
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        75:84:7a:27:bb:fe:77:64:be:0c:1c:9c:a7:09:a5:ce:70:4d:
        46:0d:b6:62:29:e0:b3:69:f9:de:9c:e2:79:0b:8a:23:31:a2:
        e6:b8:fd:89:f0:45:a7:f2:82:01:9b:69:ae:4f:e7:c5:3f:6b:
        89:0e:f9:38:c6:a4:72:56:ee:9d:99:4f:ed:49:f7:8a:7f:8f:
        18:e2:20:4a:82:18:f4:6e:0f:f9:d0:e2:19:cf:36:53:ed:71:
        d5:de:72:1e:c5:94:b4:72:58:6d:58:57:14:cc:48:42:35:c6:
        6e:12:9a:b5:14:19:1d:a4:65:88:2f:b9:a0:0e:ae:f8:ee:fc:
        ae:aa:db:24:eb:12:03:5b:06:24:e3:8e:c2:4e:dd:d7:3b:09:
        27:9c:db:66:63:41:a5:c5:f4:cf:6e:5d:33:ae:c1:97:6f:69:
        00:a1:22:1f:a8:ff:82:79:0b:ba:99:f8:35:e0:96:c7:5c:ae:
        28:c2:24:3f:a7:ca:95:a5:b5:46:04:83:e1:80:cd:0e:1b:69:
```

- Step 2. a - I extracted his public key.

```
(base)
~/lucas » openssl x509 -pubkey -in A.crt -noout > pubkey-A.pem
(base)
```

- Step 4. a - I decrypted symkey.enc using my private key.

```
(base)
~/lucas » openssl pkeyutl -decrypt -in symkey.enc -inkey privkey-B.pem -out symkey.pem
(base)
```

- Step 4. b - I verified Ron's public certificate, andI got an OK. I know the certificate can be trusted.

```
(base)
~/lucas »  openssl verify -CAfile root.crt A.crt          lucasyao@lucass-mbp
A.crt: OK
(base)
~/lucas »                                                                  lucasyao@lucas
```

- I verified the message was from Ron, and I decrypted ciphertext.bin with the same symmetric key.

```
(base)
~/lucas » openssl dgst -sha1 -verify pubkey-A.pem -signature signature.bin symkey.pem
Verified OK
(base)
~/lucas » openssl enc -aes-256-cbc -d -pass file:symkey.pem -p -md sha256 -in ciphertext.bin -out largefile.txt
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
salt=D968A6BDE63BB532
key=CB6402B8CEBE845B9B92225DEE4A224CAF39F20583645B03501E0F456E5E47E8
iv =93057972545B35E1F8C8AD2EC4C4A95D
(base)
```

- Step 4. c -Finally, I got the message!