Name: Rithik Sarvesh Bharathiraja

UID: 120395246

Course: ENPM693

Task: Homework 5

Task 3.1

The part of the certificate which shows thaa this is a CA's certificate

```
                6c:ed:c8:c2:db:27:22:1a:3d:a0:4f:f9:0c:72:b9:
                f9:b9:fb:91:79:10:ac:a4:94:64:f8:71:fc:2a:b2:
                2a:15:93:1e:de:61:02:bf:9b:05:6f:0a:5e:55:52:
                cd:98:a9:89:7a:0f:3f:9f:9e:97:e1:ea:3d:95:92:
                dc:ec:9c:f0:54:cf:84:23:eb:05:a6:b7:19:18:29:
                a6:b9:81
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Key Identifier:
            73:E8:F7:E8:97:E9:5B:C7:79:36:76:84:1B:3E:61:B9:96:74:E7:6D
        X509v3 Authority Key Identifier:
            keyid:73:E8:F7:E8:97:E9:5B:C7:79:36:76:84:1B:3E:61:B9:96:74:E7:6D

        X509v3 Basic Constraints: critical
            CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
     b6:1a:06:00:31:84:6b:4c:83:01:a6:6a:33:5b:32:1f:c3:93:
     97:da:95:78:46:f0:27:b7:90:1a:c6:47:06:42:fd:4e:2a:65:
     92:5a:b4:a5:6c:db:95:8c:6a:c1:f6:38:16:64:95:57:6c:6b:
     9f:ee:02:ab:fe:10:56:9a:84:5f:dd:fd:67:2d:d2:88:af:0c:
     f9:d5:2d:c3:cf:b5:f0:39:1c:98:91:8b:52:92:f4:0d:4f:10:
     df:72:a4:11:c0:5d:33:6a:50:6c:66:78:6b:7c:8f:4b:68:bd:
     aa:2d:20:1b:fb:72:a8:39:bc:c9:d0:75:e6:e9:b9:6a:63:dc:
     d4:3a:46:29:56:ab:76:5a:c6:18:ef:56:75:13:c0:59:f9:75:
```

The part of the certificate which indicates that this is a self-signed certificate

```
                cd:98:a9:89:7a:0f:3f:9f:9e:97:e1:ea:3d:95:92:
                dc:ec:9c:f0:54:cf:84:23:eb:05:a6:b7:19:18:29:
                a6:b9:81
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Key Identifier:
            73:E8:F7:E8:97:E9:5B:C7:79:36:76:84:1B:3E:61:B9:96:74:E7:6D
        X509v3 Authority Key Identifier:
            keyid:73:E8:F7:E8:97:E9:5B:C7:79:36:76:84:1B:3E:61:B9:96:74:E7:6D

        X509v3 Basic Constraints: critical
            CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
     b6:1a:06:00:31:84:6b:4c:83:01:a6:6a:33:5b:32:1f:c3:93:
     97:da:95:78:46:f0:27:b7:90:1a:c6:47:06:42:fd:4e:2a:65:
     92:5a:b4:a5:6c:db:95:8c:6a:c1:f6:38:16:64:95:57:6c:6b:
```

Parts of RSA algorithm

Public exponent e and the private exponent d

```
    bf:0c:f0:6f:e2:bb:d3:c5:75:c1:49:ce:51:10:3a:
    47:b5:ef:8d:40:c1:92:3e:9c:1c:b4:e0:15:cb:fa:
    1f:dd:f3:28:31:44:ce:06:3a:47:68:99:4f:ab:b6:
    4a:6e:9b:fd:a4:ae:1f:00:0f:c9:c6:3c:ef:50:50:
    b0:2d:0d:e4:7d:6d:c6:de:ec:ee:bb:47:d1:0b:09:
    ae:b4:22:75:34:74:fe:c5:93:d2:1d:ab:bb:86:bd:
    1f:a4:01:8f:88:71:26:a2:ca:cb:97:1d:77:58:93:
    6c:ed:c8:c2:db:27:22:1a:3d:a0:4f:f9:0c:72:b9:
    f9:b9:fb:91:79:10:ac:a4:94:64:f8:71:fc:2a:b2:
    2a:15:93:1e:de:61:02:bf:9b:05:6f:0a:5e:55:52:
    cd:98:a9:89:7a:0f:3f:9f:9e:97:e1:ea:3d:95:92:
    dc:ec:9c:f0:54:cf:84:23:eb:05:a6:b7:19:18:29:
    a6:b9:81
publicExponent: 65537 (0x10001)
privateExponent:
    19:3e:1d:26:83:36:b1:01:ea:f9:53:57:d8:af:23:
    ba:ed:25:51:6c:cb:d8:02:42:6e:ef:7f:7e:72:c8:
    a3:44:c6:cc:ab:d1:cd:1e:94:af:48:59:52:2a:8e:
    19:1c:93:f3:62:a2:47:54:95:fe:e2:aa:2d:98:85:
    80:dd:24:77:70:46:d0:1b:80:85:21:4e:fd:53:50:
    24:23:1f:40:69:2b:17:44:33:24:4c:1b:48:e6:1f:
    2f:5b:f0:87:d5:e9:ff:be:c7:eb:c2:7f:3b:c4:bd:
    58:18:ab:67:6c:85:8e:d8:ed:29:22:72:c8:35:fc:
    26:c3:c6:f5:2a:71:8b:78:a5:24:03:d7:26:8b:29:
    fa:13:7d:c2:39:83:e9:9c:0a:89:ae:b0:a4:7d:db:
    eb:61:d4:cb:47:82:e3:1a:37:66:b8:d9:0e:80:d9:
    e7:d0:a1:24:1a:d3:fd:94:30:7a:99:78:49:38:5a:
    03:7d:88:7c:01:89:8d:bf:da:7e:27:bb:e5:13:6f:
    5f:71:f7:1e:9b:e8:b8:7e:83:37:25:dd:e2:18:89:
    80:bc:36:73:c4:b7:fe:c9:aa:14:34:97:90:b3:10:
    32:96:2e:22:f5:04:6d:9c:ce:92:0a:da:ce:bc:ee:
    67:2b:34:eb:eb:a3:26:4c:2b:24:39:c0:7b:43:11:
    e4:27:8a:01:96:92:69:39:92:7a:9f:c2:0b:0f:15:
    40:33:d4:45:1c:5b:87:95:ce:6a:56:1b:10:70:f6:
```

Prime p

```
    e4:27:8a:01:96:92:69:39:92:7a:9f:c2:0b:0f:15:
    40:33:d4:45:1c:5b:87:95:ce:6a:56:1b:10:70:f6:
    d6:53:14:31:60:28:f0:f2:af:01:5b:60:54:c9:63:
    e4:4b:0d:b5:a6:f6:9f:e1:de:5b:dd:b7:04:4c:f6:
    aa:03:3d:43:31:27:a3:1f:f7:ce:6b:c6:6d:5b:0a:
    88:bb:69:e4:de:17:b0:d2:82:c8:90:51:e3:0f:8b:
    09:36:0b:c5:6f:85:d3:0d:6a:8d:91:8d:25:86:7e:
    d8:8a:d5:1b:da:89:07:48:2d:a8:4c:db:24:88:ac:
    5d:d1:56:c1:d9:24:e6:a0:f2:fd:e9:6a:71:3b:bf:
    11:5e:5e:ed:d7:a7:17:5f:66:03:34:ea:26:c7:f8:
    35:9c:b8:a7:e1:40:b8:c6:6a:4c:ad:0c:72:65:8a:
    13:80:d4:41:3f:1e:eb:39:68:9f:8f:6f:8f:c6:9f:
    0d:a9:64:40:59:1a:2b:f9:6a:96:14:7a:65:bc:1d:
    17:69:b6:a8:71:5f:c4:93:d5:7d:9c:ff:d5:20:9b:
    6c:de:d6:1d:72:16:f2:c3:f1:36:48:62:56:af:bc:
    d4:83:6d:cb:4f:62:c6:04:8c:84:1f:92:a4:06:8d:
    e0:a7:3c:e7:2e:69:3c:df:37:17:22:76:91:f1:b2:
    ae:b9
prime1:
    00:fa:39:a0:82:96:66:f5:70:17:52:18:3d:3e:34:
    c0:47:83:35:c6:54:3d:05:f0:c2:84:1f:15:9d:dd:
    2b:d1:12:6e:2e:c6:7d:9f:e2:ee:1d:3e:7a:2f:7a:
    68:ce:18:6e:c6:b5:77:96:d0:30:cd:a4:99:08:00:
    d2:e4:02:d5:de:a3:06:12:c2:7b:dd:61:e0:c8:0a:
    9c:0e:2b:d3:53:49:cd:c0:2a:83:db:be:52:8a:ba:
    ac:87:f2:86:30:e0:96:06:c6:63:53:ee:3b:13:3d:
    f6:5e:a5:f3:af:eb:0f:10:6e:9f:a2:cc:d9:08:90:
    40:e0:c5:61:80:0e:ab:d0:8f:b4:fb:1a:d0:c1:4a:
    31:e3:be:00:b9:26:3f:86:ae:01:dd:c5:f6:f7:bb:
    25:c9:8f:77:af:9a:8d:64:40:b4:06:88:d6:cc:b8:
    8e:de:aa:44:ac:8e:3d:88:ba:27:75:72:cd:cb:8d:
    72:f5:48:b0:18:ef:fb:04:ce:52:4e:e1:2f:7b:fe:
    76:10:1e:9c:12:71:36:8a:ed:ec:b9:a4:a7:e5:0a:
    02:d6:c8:76:0d:20:08:ad:57:a4:37:b2:07:d9:c2:
```

Prime q

```
    76:10:1e:9c:12:71:36:8a:ed:ec:b9:a4:a7:e5:0a:
    02:d6:c8:76:0d:20:08:ad:57:a4:37:b2:07:d9:c2:
    cc:68:54:fa:15:cc:c6:09:25:e5:3f:61:02:12:36:
    5c:b4:97:5c:71:31:de:2f:52:57:39:35:84:22:2c:
    2b:2b
prime2:
    00:e0:69:2a:37:fe:55:de:a9:8b:65:87:d0:40:5f:
    fb:9d:db:3d:d4:55:2b:4d:8b:cb:b8:f0:cc:11:85:
    bf:62:05:e6:b8:10:8d:e6:c1:56:5b:70:7d:91:cb:
    f7:37:bd:4d:0e:22:ce:2b:f5:6d:33:74:7c:d8:4d:
    9e:a6:e8:61:2b:7a:dc:3e:6d:ab:10:53:01:6b:4f:
    6e:fc:1b:ff:63:39:8f:16:e2:39:fe:fb:2b:e2:87:
    c8:ac:11:8c:39:02:7d:e8:94:55:58:77:f9:98:53:
    3d:66:4a:35:fd:89:a2:0f:8a:f8:88:b0:88:02:7c:
    a8:24:04:5b:59:d3:3d:2b:b0:3a:84:af:ae:87:fd:
    0f:01:ae:0c:9a:ef:44:af:ba:15:b5:59:e7:ab:11:
    d8:fd:a6:1b:79:d0:39:d8:29:5f:9e:c7:4f:44:e7:
    c2:8e:3b:7a:5e:b1:29:93:21:38:87:cd:2c:69:8c:
    eb:92:09:9f:07:0c:d0:d3:b7:df:25:c6:2c:24:b3:
    1e:37:23:c5:29:f1:a3:8b:88:82:e9:82:ae:b5:7b:
    65:f4:a6:5e:46:05:fc:8c:bc:da:fe:5e:f1:8d:49:
    ec:7d:f3:fb:8e:40:c5:1a:e4:5a:59:08:4f:08:4a:
    88:f2:00:a2:b8:0d:98:78:b2:9e:a9:9e:2f:35:6a:
    a8:03
exponent1:
    00:d6:80:d2:25:40:33:90:d1:7f:5c:63:e5:14:4f:
    7a:49:93:a4:64:99:50:1a:a8:92:c7:5a:32:58:bb:
    01:d5:df:7b:ce:e3:5f:4b:d1:e8:97:ef:38:25:3d:
    45:5c:ef:ba:fe:e3:0f:5a:9c:ac:49:8d:81:96:47:
    c6:81:aa:20:97:13:9f:a0:33:52:a5:ac:43:5a:99:
    25:c0:4c:37:83:9d:b0:20:bd:11:7e:2d:c0:6a:a6:
    ae:42:78:58:2a:cc:4c:30:10:9f:93:92:94:d7:e0:
    f5:33:9c:05:b3:d7:c8:79:28:ab:f6:8e:ae:ba:d5:
    96:98:58:fc:45:1f:ce:90:22:b1:5d:d5:56:01:6c:
```

Modulo n

```
[04/18/24]seed@VM:~/Workspace$ openssl rsa -in ca.key -text -noout
Enter pass phrase for ca.key:
RSA Private-Key: (4096 bit, 2 primes)
modulus:
    00:db:59:37:59:48:79:cb:bf:81:d7:58:c4:76:e7:
    19:87:0e:55:14:c6:f3:55:22:18:12:87:db:00:02:
    69:b3:78:d7:1d:13:91:3d:b8:c7:c9:0c:09:51:64:
    46:ff:7a:d7:bd:f7:5d:f4:26:32:7d:57:45:2f:68:
    95:20:33:3b:48:de:10:b6:8e:b7:fe:6e:cb:7a:34:
    ba:ce:14:12:db:49:a3:d3:2b:bb:96:57:d4:b8:f8:
    77:aa:91:ae:41:cc:0f:ab:93:5e:c9:b4:79:dd:83:
    43:2b:0a:5e:a3:0f:94:4f:82:f4:0d:d5:e8:54:7a:
    12:7d:96:6d:54:4b:72:2e:a4:fc:27:22:cc:25:d2:
    ce:25:40:6b:2e:e2:8a:ba:f5:36:07:3c:d6:5b:98:
    8e:0f:89:9c:a6:e0:19:57:ad:ce:79:86:79:c4:30:
    59:5c:7a:c5:70:59:e2:8d:13:02:9b:41:33:7b:3c:
    53:39:36:83:12:bc:c7:04:de:22:02:ed:43:d8:9a:
    63:9e:8f:76:9e:01:be:07:2b:81:61:51:6e:50:75:
    b3:9a:5d:3f:9b:e8:3b:50:e8:be:8d:90:ee:0d:cd:
    63:1a:37:8e:42:c5:87:63:16:9c:c7:5c:f7:29:32:
    bf:fc:86:48:56:5e:df:af:0e:5f:76:38:81:6d:14:
    10:d1:17:9a:7a:e9:f7:3b:e9:56:ac:17:fa:92:b9:
    db:3e:69:15:b5:8b:11:d0:a5:27:6e:48:1b:70:db:
    d3:db:95:35:67:0a:15:78:67:35:69:01:df:1a:d7:
    c4:b3:7c:c5:ab:27:78:da:50:30:0d:e2:3d:56:5e:
    22:02:d1:05:5d:ae:5c:c1:a6:7c:32:ba:01:7f:79:
    bf:0c:f0:6f:e2:bb:d3:c5:75:c1:49:ce:51:10:3a:
    47:b5:ef:8d:40:c1:92:3e:9c:1c:b4:e0:15:cb:fa:
```

Screenshots of ca.crt

```
[04/18/24]seed@VM:~/Workspace$ openssl req -x509 -config MyOpenssl.cnf -newkey rsa:4096 -sha256 -days 3650 -keyout ca.key -out ca.crt -subj "
/CN=www.modelCA.com/O=Model CA LTD./C=US" -passout pass:dees
Generating a RSA private key
.....................................................................................++++
.............................++++
writing new private key to 'ca.key'
-----
[04/18/24]seed@VM:~/Workspace$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            7b:3b:c3:c3:ed:c1:2d:3e:58:ab:06:90:7d:53:85:e6:12:fb:07:6a
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: Apr 18 20:18:50 2024 GMT
            Not After : Apr 16 20:18:50 2034 GMT
        Subject: CN = www.modelCA.com, O = Model CA LTD., C = US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:db:59:37:59:48:79:cb:bf:81:d7:58:c4:76:e7:
                    19:87:0e:55:14:c6:f3:55:22:18:12:87:db:00:02:
                    69:b3:78:d7:1d:13:91:3d:b8:c7:c9:0c:09:51:64:
                    46:ff:7a:d7:bd:f7:5d:f4:26:32:7d:57:45:2f:68:
                    95:20:33:3b:48:de:10:b6:8e:b7:fe:6e:cb:7a:34:
                    ba:ce:14:12:db:49:a3:d3:2b:bb:96:57:d4:b8:f8:
                    77:aa:91:ae:41:cc:0f:ab:93:5e:c9:b4:79:dd:83:
                    43:2b:0a:5e:a3:0f:94:4f:82:f4:0d:d5:e8:54:7a:
                    12:7d:96:6d:54:4b:72:2e:a4:fc:27:22:cc:25:d2:
                    ce:25:40:6b:2e:e2:8a:ba:f5:36:07:3c:d6:5b:98:
                    8e:0f:89:9c:a6:e0:19:57:ad:ce:79:86:79:c4:30:
                    [illegible]

                    63:9e:8f:76:9e:01:be:07:2b:81:61:51:6e:50:75:
                    b3:9a:5d:3f:9b:e8:3b:50:e8:be:8d:90:ee:0d:cd:
                    63:1a:37:8e:42:c5:87:63:16:9c:c7:5c:f7:29:32:
                    bf:fc:86:48:56:5e:df:af:0e:5f:76:38:81:6d:14:
                    10:d1:17:9a:7a:e9:f7:3b:e9:56:ac:17:fa:92:b9:
                    db:3e:69:15:b5:8b:11:d0:a5:27:6e:48:1b:70:db:
                    d3:db:95:35:67:0a:15:78:67:35:69:01:df:1a:d7:
                    c4:b3:7c:c5:ab:27:78:da:50:30:0d:e2:3d:56:5e:
                    22:02:d1:05:5d:ae:5c:c1:a6:7c:32:ba:01:7f:79:
                    bf:0c:f0:6f:e2:bb:d3:c5:75:c1:49:ce:51:10:3a:
                    47:b5:ef:8d:40:c1:92:3e:9c:1c:b4:e0:15:cb:fa:
                    1f:dd:f3:28:31:44:ce:06:3a:47:68:99:4f:ab:b6:
                    4a:6e:9b:fd:a4:ae:1f:00:0f:c9:c6:3c:ef:50:50:
                    b0:2d:0d:e4:7d:6d:c6:de:ec:ee:bb:47:d1:0b:09:
                    ae:b4:22:75:34:74:fe:c5:93:d2:1d:ab:bb:86:bd:
                    1f:a4:01:8f:88:71:26:a2:ca:cb:97:1d:77:58:93:
                    6c:ed:c8:c2:db:27:22:1a:3d:a0:4f:f9:0c:72:b9:
                    f9:b9:fb:91:79:10:ac:a4:94:64:f8:71:fc:2a:b2:
                    2a:15:93:1e:de:61:02:bf:9b:05:6f:0a:5e:55:52:
                    cd:98:a9:89:7a:0f:3f:9f:9e:97:e1:ea:3d:95:92:
                    dc:ec:9c:f0:54:cf:84:23:eb:05:a6:b7:19:18:29:
                    a6:b9:81
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                73:E8:F7:E8:97:E9:5B:C7:79:36:76:84:1B:3E:61:B9:96:74:E7:6D
            X509v3 Authority Key Identifier:
                keyid:73:E8:F7:E8:97:E9:5B:C7:79:36:76:84:1B:3E:61:B9:96:74:E7:6D

            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         b6:1a:06:00:31:84:6b:4c:83:01:a6:6a:33:5b:32:1f:c3:93:
         97:da:95:78:46:f0:27:b7:90:1a:c6:47:06:42:fd:4e:2a:65:
```

```
        b6:1a:06:00:31:84:6b:4c:83:01:a6:6a:33:5b:32:1f:c3:93:
        97:da:95:78:46:f0:27:b7:90:1a:c6:47:06:42:fd:4e:2a:65:
        92:5a:b4:a5:6c:db:95:8c:6a:c1:f6:38:16:64:95:57:6c:6b:
        9f:ee:02:ab:fe:10:56:9a:84:5f:dd:fd:67:2d:d2:88:af:0c:
        f9:d5:2d:c3:cf:b5:f0:39:1c:98:91:8b:52:92:f4:0d:4f:10:
        df:72:a4:11:c0:5d:33:6a:50:6c:66:78:6b:7c:8f:4b:68:bd:
        aa:2d:20:1b:fb:72:a8:39:bc:c9:d0:75:e6:e9:b9:6a:63:dc:
        d4:3a:46:29:56:ab:76:5a:c6:18:ef:56:75:13:c0:59:f9:75:
        c1:db:7e:c5:62:c3:f9:53:b7:7e:8b:e7:09:fe:a7:4f:31:97:
        a1:7b:fd:c0:e4:4b:ce:06:70:7d:3b:21:ae:d1:22:6c:f6:f7:
        cc:b8:ab:00:a1:3d:40:8d:9f:d6:62:ce:e5:10:04:5a:6f:2a:
        c1:a7:40:5f:3f:c5:db:a9:09:48:5b:41:6e:18:66:aa:95:a4:
        04:45:62:a4:25:6f:a7:86:33:43:de:4f:b3:16:a6:16:e1:45:
        09:69:4c:85:33:f8:b7:5e:38:b9:a8:24:59:51:fc:78:38:cd:
        72:1c:dd:26:a4:9d:89:33:b6:56:6d:15:0b:1a:4d:ff:17:54:
        53:fc:2b:ff:9b:97:f2:25:28:75:65:32:93:15:c6:9b:23:3a:
        a8:b5:99:32:7f:13:96:5b:9b:39:0f:10:a2:2d:24:11:43:fb:
        19:3a:d2:31:e5:8f:8e:0e:a1:1b:53:b0:8d:f6:c5:46:b9:02:
        ce:2e:33:8e:e0:a9:fe:a9:7f:ef:38:07:46:2e:b7:03:c8:6e:
        d9:cf:c0:27:95:0f:10:b6:71:59:64:83:53:eb:95:14:7a:ff:
        9c:6b:99:c5:bb:a9:90:83:d1:e3:4e:ac:9a:9f:d3:e3:4b:6b:
        28:d8:bc:78:ab:a7:10:b7:9f:ef:72:ad:89:9c:f0:6e:aa:99:
        5b:9d:d1:6d:04:60:f0:48:29:0e:00:99:1c:93:68:bc:cc:7c:
        74:cb:86:ff:1e:04:63:8b:70:d1:cb:24:4c:a8:40:3d:2e:21:
        25:a9:02:c5:4b:e5:d3:40:44:23:7e:a0:ad:fd:da:4c:df:8c:
        1b:01:2a:41:d4:3b:94:a2:b5:3b:0a:8b:5a:b7:79:90:19:c8:
        14:1d:cc:d7:77:99:80:54:43:43:51:2b:f5:4f:e2:c1:4c:c9:
        fd:91:b3:3e:70:2a:d2:cf:ec:31:56:16:38:99:f9:6e:f1:6f:
        47:f0:c5:54:f3:f4:97:19
[04/18/24]seed@VM:~/Workspace$ echo "Rithik"
Rithik
[04/18/24]seed@VM:~/Workspace$ echo "120395246"
120395246
[04/18/24]seed@VM:~/Workspace$
```

Screenshots of ca.key

```
[04/18/24]seed@VM:~/Workspace$ openssl rsa -in ca.key -text -noout
Enter pass phrase for ca.key:
RSA Private-Key: (4096 bit, 2 primes)
modulus:
    00:db:59:37:59:48:79:cb:bf:81:d7:58:c4:76:e7:
    19:87:0e:55:14:c6:f3:55:22:18:12:87:db:00:02:
    69:b3:78:d7:1d:13:91:3d:b8:c7:c9:0c:09:51:64:
    46:ff:7a:d7:bd:f7:5d:f4:26:32:7d:57:45:2f:68:
    95:20:33:3b:48:de:10:b6:8e:b7:fe:6e:cb:7a:34:
    ba:ce:14:12:db:49:a3:d3:2b:bb:96:57:d4:b8:f8:
    77:aa:91:ae:41:cc:0f:ab:93:5e:c9:b4:79:dd:83:
    43:2b:0a:5e:a3:0f:94:4f:82:f4:0d:d5:e8:54:7a:
    12:7d:96:6d:54:4b:72:2e:a4:fc:27:22:cc:25:d2:
    ce:25:40:6b:2e:e2:8a:ba:f5:36:07:3c:d6:5b:98:
    8e:0f:89:9c:a6:e0:19:57:ad:ce:79:86:79:c4:30:
    59:5c:7a:c5:70:59:e2:8d:13:02:9b:41:33:7b:3c:
    53:39:36:83:12:bc:c7:04:de:22:02:ed:43:d8:9a:
    63:9e:8f:76:9e:01:be:07:2b:81:61:51:6e:50:75:
    b3:9a:5d:3f:9b:e8:3b:50:e8:be:8d:90:ee:0d:cd:
    63:1a:37:8e:42:c5:87:63:16:9c:c7:5c:f7:29:32:
    bf:fc:86:48:56:5e:df:af:0e:5f:76:38:81:6d:14:
    10:d1:17:9a:7a:e9:f7:3b:e9:56:ac:17:fa:92:b9:
    db:3e:69:15:b5:8b:11:d0:a5:27:6e:48:1b:70:db:
    d3:db:95:35:67:0a:15:78:67:35:69:01:df:1a:d7:
    c4:b3:7c:c5:ab:27:78:da:50:30:0d:e2:3d:56:5e:
    22:02:d1:05:5d:ae:5c:c1:a6:7c:32:ba:01:7f:79:
    bf:0c:f0:6f:e2:bb:d3:c5:75:c1:49:ce:51:10:3a:
    47:b5:ef:8d:40:c1:92:3e:9c:1c:b4:e0:15:cb:fa:
```

```
    bf:0c:f0:6f:e2:bb:d3:c5:75:c1:49:ce:51:10:3a:
    47:b5:ef:8d:40:c1:92:3e:9c:1c:b4:e0:15:cb:fa:
    1f:dd:f3:28:31:44:ce:06:3a:47:68:99:4f:ab:b6:
    4a:6e:9b:fd:a4:ae:1f:00:0f:c9:c6:3c:ef:50:50:
    b0:2d:0d:e4:7d:6d:c6:de:ec:ee:bb:47:d1:0b:09:
    ae:b4:22:75:34:74:fe:c5:93:d2:1d:ab:bb:86:bd:
    1f:a4:01:8f:88:71:26:a2:ca:cb:97:1d:77:58:93:
    6c:ed:c8:c2:db:27:22:1a:3d:a0:4f:f9:0c:72:b9:
    f9:b9:fb:91:79:10:ac:a4:94:64:f8:71:fc:2a:b2:
    2a:15:93:1e:de:61:02:bf:9b:05:6f:0a:5e:55:52:
    cd:98:a9:89:7a:0f:3f:9f:9e:97:e1:ea:3d:95:92:
    dc:ec:9c:f0:54:cf:84:23:eb:05:a6:b7:19:18:29:
    a6:b9:81
publicExponent: 65537 (0x10001)
privateExponent:
    19:3e:1d:26:83:36:b1:01:ea:f9:53:57:d8:af:23:
    ba:ed:25:51:6c:cb:d8:02:42:6e:ef:7f:7e:72:c8:
    a3:44:c6:cc:ab:d1:cd:1e:94:af:48:59:52:2a:8e:
    19:1c:93:f3:62:a2:47:54:95:fe:e2:aa:2d:98:85:
    80:dd:24:77:70:46:d0:1b:80:85:21:4e:fd:53:50:
    24:23:1f:40:69:2b:17:44:33:24:4c:1b:48:e6:1f:
    2f:5b:f0:87:d5:e9:ff:be:c7:eb:c2:7f:3b:c4:bd:
    58:18:ab:67:6c:85:8e:d8:ed:29:22:72:c8:35:fc:
    26:c3:c6:f5:2a:71:8b:78:a5:24:03:d7:26:8b:29:
    fa:13:7d:c2:39:83:e9:9c:0a:89:ae:b0:a4:7d:db:
    eb:61:d4:cb:47:82:e3:1a:37:66:b8:d9:0e:80:d9:
    e7:d0:a1:24:1a:d3:fd:94:30:7a:99:78:49:38:5a:
    03:7d:88:7c:01:89:8d:bf:da:7e:27:bb:e5:13:6f:
    5f:71:f7:1e:9b:e8:b8:7e:83:37:25:dd:e2:18:89:
    80:bc:36:73:c4:b7:fe:c9:aa:14:34:97:90:b3:10:
    32:96:2e:22:f5:04:6d:9c:ce:92:0a:da:ce:bc:ee:
    67:2b:34:eb:eb:a3:26:4c:2b:24:39:c0:7b:43:11:
    e4:27:8a:01:96:92:69:39:92:7a:9f:c2:0b:0f:15:
    40:33:d4:45:1c:5b:87:95:ce:6a:56:1b:10:70:f6:
```

```
    e4:27:8a:01:96:92:69:39:92:7a:9f:c2:0b:0f:15:
    40:33:d4:45:1c:5b:87:95:ce:6a:56:1b:10:70:f6:
    d6:53:14:31:60:28:f0:f2:af:01:5b:60:54:c9:63:
    e4:4b:0d:b5:a6:f6:9f:e1:de:5b:dd:b7:04:4c:f6:
    aa:03:3d:43:31:27:a3:1f:f7:ce:6b:c6:6d:5b:0a:
    88:bb:69:e4:de:17:b0:d2:82:c8:90:51:e3:0f:8b:
    09:36:0b:c5:6f:85:d3:0d:6a:8d:91:8d:25:86:7e:
    d8:8a:d5:1b:da:89:07:48:2d:a8:4c:db:24:88:ac:
    5d:d1:56:c1:d9:24:e6:a0:f2:fd:e9:6a:71:3b:bf:
    11:5e:5e:ed:d7:a7:17:5f:66:03:34:ea:26:c7:f8:
    35:9c:b8:a7:e1:40:b8:c6:6a:4c:ad:0c:72:65:8a:
    13:80:d4:41:3f:1e:eb:39:68:9f:8f:6f:8f:c6:9f:
    0d:a9:64:40:59:1a:2b:f9:6a:96:14:7a:65:bc:1d:
    17:69:b6:a8:71:5f:c4:93:d5:7d:9c:ff:d5:20:9b:
    6c:de:d6:1d:72:16:f2:c3:f1:36:48:62:56:af:bc:
    d4:83:6d:cb:4f:62:c6:04:8c:84:1f:92:a4:06:8d:
    e0:a7:3c:e7:2e:69:3c:df:37:17:22:76:91:f1:b2:
    ae:b9
prime1:
    00:fa:39:a0:82:96:66:f5:70:17:52:18:3d:3e:34:
    c0:47:83:35:c6:54:3d:05:f0:c2:84:1f:15:9d:dd:
    2b:d1:12:6e:2e:c6:7d:9f:e2:ee:1d:3e:7a:2f:7a:
    68:ce:18:6e:c6:b5:77:96:d0:30:cd:a4:99:08:00:
    d2:e4:02:d5:de:a3:06:12:c2:7b:dd:61:e0:c8:0a:
    9c:0e:2b:d3:53:49:cd:c0:2a:83:db:be:52:8a:ba:
    ac:87:f2:86:30:e0:96:06:c6:63:53:ee:3b:13:3d:
    f6:5e:a5:f3:af:eb:0f:10:6e:9f:a2:cc:d9:08:90:
    40:e0:c5:61:80:0e:ab:d0:8f:b4:fb:1a:d0:c1:4a:
    31:e3:be:00:b9:26:3f:86:ae:01:dd:c5:f6:f7:bb:
    25:c9:8f:77:af:9a:8d:64:40:b4:06:88:d6:cc:b8:
    8e:de:aa:44:ac:8e:3d:88:ba:27:75:72:cd:cb:8d:
    72:f5:48:b0:18:ef:fb:04:ce:52:4e:e1:2f:7b:fe:
    76:10:1e:9c:12:71:36:8a:ed:ec:b9:a4:a7:e5:0a:
    02:d6:c8:76:0d:20:08:ad:57:a4:37:b2:07:d9:c2:
```

```
    76:10:1e:9c:12:71:36:8a:ed:ec:b9:a4:a7:e5:0a:
    02:d6:c8:76:0d:20:08:ad:57:a4:37:b2:07:d9:c2:
    cc:68:54:fa:15:cc:c6:09:25:e5:3f:61:02:12:36:
    5c:b4:97:5c:71:31:de:2f:52:57:39:35:84:22:2c:
    2b:2b
prime2:
    00:e0:69:2a:37:fe:55:de:a9:8b:65:87:d0:40:5f:
    fb:9d:db:3d:d4:55:2b:4d:8b:cb:b8:f0:cc:11:85:
    bf:62:05:e6:b8:10:8d:e6:c1:56:5b:70:7d:91:cb:
    f7:37:bd:4d:0e:22:ce:2b:f5:6d:33:74:7c:d8:4d:
    9e:a6:e8:61:2b:7a:dc:3e:6d:ab:10:53:01:6b:4f:
    6e:fc:1b:ff:63:39:8f:16:e2:39:fe:fb:2b:e2:87:
    c8:ac:11:8c:39:02:7d:e8:94:55:58:77:f9:98:53:
    3d:66:4a:35:fd:89:a2:0f:8a:f8:88:b0:88:02:7c:
    a8:24:04:5b:59:d3:3d:2b:b0:3a:84:af:ae:87:fd:
    0f:01:ae:0c:9a:ef:44:af:ba:15:b5:59:e7:ab:11:
    d8:fd:a6:1b:79:d0:39:d8:29:5f:9e:c7:4f:44:e7:
    c2:8e:3b:7a:5e:b1:29:93:21:38:87:cd:2c:69:8c:
    eb:92:09:9f:07:0c:d0:d3:b7:df:25:c6:2c:24:b3:
    1e:37:23:c5:29:f1:a3:8b:88:82:e9:82:ae:b5:7b:
    65:f4:a6:5e:46:05:fc:8c:bc:da:fe:5e:f1:8d:49:
    ec:7d:f3:fb:8e:40:c5:1a:e4:5a:59:08:4f:08:4a:
    88:f2:00:a2:b8:0d:98:78:b2:9e:a9:9e:2f:35:6a:
    a8:03
exponent1:
    00:d6:80:d2:25:40:33:90:d1:7f:5c:63:e5:14:4f:
    7a:49:93:a4:64:99:50:1a:a8:92:c7:5a:32:58:bb:
    01:d5:df:7b:ce:e3:5f:4b:d1:e8:97:ef:38:25:3d:
    45:5c:ef:ba:fe:e3:0f:5a:9c:ac:49:8d:81:96:47:
    c6:81:aa:20:97:13:9f:a0:33:52:a5:ac:43:5a:99:
    25:c0:4c:37:83:9d:b0:20:bd:11:7e:2d:c0:6a:a6:
    ae:42:78:58:2a:cc:4c:30:10:9f:93:92:94:d7:e0:
    f5:33:9c:05:b3:d7:c8:79:28:ab:f6:8e:ae:ba:d5:
    96:98:58:fc:45:1f:ce:90:22:b1:5d:d5:56:01:6c:
```

```
    f5:33:9c:05:b3:d7:c8:79:28:ab:f6:8e:ae:ba:d5:
    96:98:58:fc:45:1f:ce:90:22:b1:5d:d5:56:01:6c:
    ce:29:d2:76:a2:41:b4:91:8a:d7:94:bb:21:04:ab:
    4d:30:65:a9:8f:42:e9:54:78:d7:1b:06:f1:44:5c:
    2e:35:99:36:f7:c9:93:dc:82:e0:52:a1:90:e3:9f:
    25:5e:39:ea:a3:e6:0d:84:c8:2d:ec:ea:c3:9f:02:
    bb:49:04:44:7c:d6:ca:8f:fc:78:43:88:70:59:3a:
    e4:c6:24:e0:76:4d:f0:c2:50:70:39:42:87:d2:58:
    58:8c:53:d4:73:1d:b0:e2:a4:b6:ca:47:29:d4:5c:
    ff:c9:dc:3b:65:d9:ff:03:08:0e:37:bf:b5:be:e9:
    a8:33
exponent2:
    00:82:a1:14:ff:55:20:9d:25:6a:4c:66:bb:75:cd:
    a9:85:21:2b:23:9f:94:3e:66:a2:e6:fb:dc:7e:52:
    b1:ae:18:ab:4d:f7:ec:f2:27:16:e2:d1:5f:76:f0:
    18:ef:2c:55:5f:66:29:47:73:6c:e6:a7:e7:48:6e:
    1e:6d:20:15:f8:1e:63:78:3f:94:75:43:2c:2f:50:
    24:d5:c2:62:6e:5b:02:0d:1b:11:11:79:19:f9:9a:
    7a:d8:96:ba:5e:31:32:23:a1:bc:f0:6b:9e:31:ea:
    3a:72:81:be:5d:e0:b1:22:85:0d:d9:5b:91:40:89:
    59:c2:e5:7a:5b:96:58:24:47:48:39:16:9e:ec:f0:
    04:bd:40:98:7b:d3:cd:d2:d0:ea:74:0f:6a:88:ad:
    31:f7:ac:aa:8f:c5:02:f6:ee:56:87:f1:93:16:14:
    26:af:6e:b5:f3:cb:02:dd:6f:58:1d:cc:f4:0e:59:
    06:83:92:f0:2c:45:6c:85:e1:a1:96:b6:7d:d9:bb:
    1e:5a:90:8a:e3:b8:92:2f:d5:fe:06:79:98:c3:71:
    9a:4e:c8:4d:56:4b:83:d0:54:da:d1:79:68:f8:8a:
    d0:8c:1c:eb:10:ca:69:32:17:3c:f4:58:9e:d0:bf:
    ba:69:cc:ae:eb:9e:96:63:a3:ee:31:e4:2f:ac:d3:
    72:0b
coefficient:
    00:f4:b0:02:8a:08:b3:49:fa:c1:9c:ff:09:92:13:
    a9:8e:ed:47:0f:6e:2f:63:7e:23:50:6a:1c:aa:83:
    dd:24:0f:93:b6:63:ee:f0:8e:1f:fe:d5:fb:ce:1e:
```

```
    59:c2:e5:7a:5b:96:58:24:47:48:39:16:9e:ec:f0:
    04:bd:40:98:7b:d3:cd:d2:d0:ea:74:0f:6a:88:ad:
    31:f7:ac:aa:8f:c5:02:f6:ee:56:87:f1:93:16:14:
    26:af:6e:b5:f3:cb:02:dd:6f:58:1d:cc:f4:0e:59:
    06:83:92:f0:2c:45:6c:85:e1:a1:96:b6:7d:d9:bb:
    1e:5a:90:8a:e3:b8:92:2f:d5:fe:06:79:98:c3:71:
    9a:4e:c8:4d:56:4b:83:d0:54:da:d1:79:68:f8:8a:
    d0:8c:1c:eb:10:ca:69:32:17:3c:f4:58:9e:d0:bf:
    ba:69:cc:ae:eb:9e:96:63:a3:ee:31:e4:2f:ac:d3:
    72:0b
coefficient:
    00:f4:b0:02:8a:08:b3:49:fa:c1:9c:ff:09:92:13:
    a9:8e:ed:47:0f:6e:2f:63:7e:23:50:6a:1c:aa:83:
    dd:24:0f:93:b6:63:ee:f0:8e:1f:fe:d5:fb:ce:1e:
    bf:f9:20:bc:2d:ee:1b:29:91:db:fc:6e:67:11:4a:
    73:69:72:ea:11:88:53:c8:c1:f5:b8:1e:93:92:35:
    20:95:75:85:7c:1b:32:9f:f9:f3:5a:b8:95:d2:2f:
    e9:20:24:78:5b:57:b7:ba:2c:a8:9f:1b:e0:10:d2:
    85:45:26:4c:f7:d1:97:59:63:9b:38:50:10:63:99:
    aa:ab:aa:df:bc:bb:7c:6a:2e:d4:cb:cf:8a:dc:26:
    5d:ab:77:8a:46:3e:8d:68:66:ba:a1:d0:8d:b2:7b:
    fd:69:85:4b:7d:37:50:25:ec:5b:e6:e1:a3:ac:80:
    45:f1:8e:4c:1f:cd:82:f4:41:42:0a:f6:95:ab:94:
    0d:71:d9:9a:03:82:f3:e6:47:74:88:6e:08:65:e2:
    89:fe:9e:0b:83:df:eb:51:ef:c7:cf:e3:6f:6a:d8:
    03:7e:0d:19:f0:d2:bb:a0:d6:cb:b8:44:79:7b:27:
    c7:6a:65:99:be:7b:55:63:cd:b7:f7:b4:be:75:5c:
    89:64:47:2d:86:63:c2:a1:a5:ee:70:7a:41:bf:4b:
    e8:58
[04/18/24]seed@VM:~/Workspace$ echo "Rithik "
Rithik
[04/18/24]seed@VM:~/Workspace$ echo "120395246"
120395246
[04/18/24]seed@VM:~/Workspace$
```

Task 3.2

Screenshots of server.csr

```
[04/21/24]seed@VM:~/Workspace$ openssl req -newkey rsa:2048 -sha256 -keyout server.key -out server.csr -subj "/CN=www.bank32.com/O=Bank32 Inc
./C=US" -passout pass:dees -addext "subjectAltName = DNS:www.bank32.com, DNS:www.bank32A.com, DNS:www.bank32B.com"
Generating a RSA private key
...+++++
.................................+++++
writing new private key to 'server.key'
-----
[04/21/24]seed@VM:~/Workspace$ echo "Rithik Sarvesh Bharathiraja - 120395246"
Rithik Sarvesh Bharathiraja - 120395246
[04/21/24]seed@VM:~/Workspace$ openssl req -in server.csr -text -noout
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = www.bank32.com, O = Bank32 Inc., C = US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:da:ae:39:d5:f3:9b:3f:ec:94:d5:80:5f:65:5a:
                    e4:40:d2:62:3c:46:fe:1f:75:ca:95:47:c5:d7:b7:
                    bc:9f:08:8d:4b:ba:71:e1:17:40:90:67:0e:d9:7e:
                    61:5c:b6:65:a4:ae:39:95:d4:17:99:b7:df:93:84:
                    31:cb:a4:28:d0:85:52:8a:7e:d0:a1:e0:fc:c3:1a:
                    10:e0:4d:19:3f:f2:5f:63:2d:4f:a1:8c:9f:59:63:
                    2a:9b:ca:4a:0f:d2:5d:a5:e9:da:95:7a:bb:bd:ec:
                    16:56:3a:5e:3b:0c:7c:3e:16:12:93:28:ed:cc:c6:
                    37:df:01:c2:f9:8c:69:e3:67:8e:37:d6:01:51:04:
                    f9:62:ec:3c:d3:ac:61:fc:3b:ed:20:86:f7:60:41:
                    16:41:b4:48:a4:a8:99:69:a4:e1:2e:c4:d1:24:80:
                    5f:9b:a0:12:02:24:c0:02:ea:e9:38:e0:9e:c6:88:
                    cc:cf:dc:68:82:9d:4b:bc:5b:d7:77:db:3a:ea:cd:
                    f4:1d:7a:93:b5:08:a6:f0:12:d9:e5:a8:58:dc:b8:
                    2a:b4:92:d6:56:a0:8b:7c:34:47:ff:56:45:02:90:
                    bb:bf:79:67:c3:26:87:3d:83:80:1b:f6:68:0b:6e:
```

```
                37:df:01:c2:f9:8c:69:e3:67:8e:37:d6:01:51:04:
                f9:62:ec:3c:d3:ac:61:fc:3b:ed:20:86:f7:60:41:
                16:41:b4:48:a4:a8:99:69:a4:e1:2e:c4:d1:24:80:
                5f:9b:a0:12:02:24:c0:02:ea:e9:38:e0:9e:c6:88:
                cc:cf:dc:68:82:9d:4b:bc:5b:d7:77:db:3a:ea:cd:
                f4:1d:7a:93:b5:08:a6:f0:12:d9:e5:a8:58:dc:b8:
                2a:b4:92:d6:56:a0:8b:7c:34:47:ff:56:45:02:90:
                bb:bf:79:67:c3:26:87:3d:83:80:1b:f6:68:0b:6e:
                7f:44:5f:39:22:df:30:68:66:0c:ef:50:40:dc:7b:
                09:ed
            Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Subject Alternative Name:
                DNS:www.bank32.com, DNS:www.bank32A.com, DNS:www.bank32B.com
    Signature Algorithm: sha256WithRSAEncryption
         85:0e:fa:f9:17:fc:67:84:e3:9e:db:7d:68:09:bc:94:39:a1:
         b1:01:c9:78:29:ef:86:53:a1:41:26:1a:7b:b8:78:85:18:75:
         b3:68:73:92:ad:58:b3:11:67:fa:57:86:53:32:ae:ee:36:6c:
         bd:0d:49:0b:51:e1:aa:c8:0b:cf:21:08:93:4c:2f:d4:5d:dc:
         16:04:fd:0d:49:1c:e2:88:0b:51:c0:df:7d:07:d2:3e:c6:89:
         b9:87:5b:68:ab:a9:68:80:8d:34:18:89:27:52:84:c0:40:17:
         76:6e:10:4b:eb:4d:fb:a5:19:52:9f:24:de:63:25:0f:f1:4f:
         be:85:d6:9c:78:5c:36:36:51:b1:68:ed:15:7c:52:26:9d:04:
         39:e5:f2:98:2d:99:ec:7f:fe:c0:ae:b8:46:5c:1d:58:17:28:
         7b:c9:f1:49:df:6c:93:a9:f1:a5:d2:47:29:a8:7d:bd:cb:a5:
         d1:e1:81:e3:e5:51:f3:f0:69:b0:86:ca:77:43:c5:21:29:f5:
         1d:1f:9e:9e:e4:6b:85:e8:83:5a:0e:13:89:a7:8c:13:d0:ed:
         de:d8:d4:3b:65:d7:f1:6a:4a:be:48:22:97:e4:42:e5:f1:bf:
         b7:16:42:4f:b4:17:e8:70:89:bf:a6:69:c0:1e:64:af:ef:55:
         35:7d:0c:95
[04/21/24]seed@VM:~/Workspace$ echo "Rithik Sarvesh Bharathiraja - 120395246"
Rithik Sarvesh Bharathiraja - 120395246
[04/21/24]seed@VM:~/Workspace$
```

Screenshots of server.key

```
[04/18/24]seed@VM:~/Workspace$ echo "Rithik"
Rithik
[04/18/24]seed@VM:~/Workspace$ echo 120395246
120395246
[04/18/24]seed@VM:~/Workspace$ openssl rsa -in server.key -text -noout
Enter pass phrase for server.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
    00:b1:ac:f8:a5:03:5c:30:82:a8:92:b2:ca:e4:42:
    9e:b2:5c:6a:28:89:06:0b:10:71:96:59:ff:7a:38:
    0c:a5:97:70:54:ff:6b:1b:16:2b:08:8d:40:62:4b:
    71:72:18:13:9b:8a:7b:d2:60:69:73:b4:3f:55:f5:
    b4:d0:05:e0:f7:c2:1c:d6:31:ff:2c:a5:b6:13:30:
    35:4c:0f:0e:d1:0f:39:92:8b:c2:67:13:fc:a4:9a:
    d4:cf:b1:86:b5:c6:40:09:44:93:f1:b2:a8:95:c9:
    fb:1f:b0:cc:df:ab:54:e6:73:b1:5d:44:2b:c5:b5:
    ba:d6:b8:b4:7b:9d:5e:20:db:e7:5f:26:93:70:a2:
    c3:eb:47:86:0f:14:7f:68:b7:33:ef:e9:33:e6:c1:
    c0:25:6f:20:4c:e8:8b:da:51:37:d9:b2:d4:e2:19:
    b9:8a:b0:b4:16:07:81:e2:c9:f6:33:d4:f5:37:e2:
    4e:6e:1f:c1:de:f1:5d:73:aa:01:f2:b9:e8:e1:cc:
    7a:f0:f1:44:c8:db:4d:f2:5f:b0:d7:f2:31:40:75:
    3c:a2:0c:c8:ce:d5:f1:d7:8c:d5:bb:f3:5f:b1:ad:
    93:ec:a3:5a:e5:01:2f:30:c4:75:93:b4:aa:96:7d:
    e8:ca:10:f1:71:3a:49:29:e2:be:3a:46:92:af:1c:
    f6:23
publicExponent: 65537 (0x10001)
privateExponent:
    2c:02:45:20:52:61:be:5e:4e:b4:ef:76:53:ed:b0:
    73:4b:72:bc:11:9c:9e:96:f7:1b:9f:b5:29:27:c2:
    f2:2d:3d:94:c0:23:5e:75:32:39:8f:0b:38:8d:a9:
    4e:f2:69:c0:e8:1f:5d:6f:a6:0f:13:c1:70:60:48:
    e6:11:de:b4:5f:af:56:da:d1:72:d4:a4:f1:c1:ca:
```

```
    78:f9:08:f6:09:f1:20:97:dd:81:d5:85:e6:15:ea:
    6e:8f:17:9d:5a:d0:5a:e0:d3:3e:73:68:ec:a8:39:
    d7:56:9a:91:f9:07:4c:79:5e:3e:d1:1c:79:f8:d0:
    42:89:db:af:37:26:3e:9d:70:11:4c:28:bc:ed:96:
    e3:85:06:db:16:c1:d6:b4:ff:57:15:e6:47:17:43:
    b2:e6:5f:31:e5:8b:47:b6:e9:8b:d9:89:e1:8e:75:
    3b:c1:71:d0:45:03:fd:35:38:d0:d6:61:b9:3a:c2:
    63:51:71:f6:8f:b7:2c:98:86:0e:2e:e2:e7:50:0e:
    ce:41:8c:52:2a:2e:cf:75:f6:c0:48:56:f1:73:08:
    d7:a7:64:ef:5d:1c:b9:c7:2e:7c:b1:8d:e5:af:e6:
    e9
prime1:
    00:e7:95:52:bb:ac:2a:72:b7:f2:63:25:88:dd:22:
    10:19:32:45:b8:58:28:85:b6:ce:6f:fe:25:42:74:
    8f:23:da:23:c8:0f:96:89:00:b2:5f:60:16:a1:ad:
    ae:f9:e1:b3:9e:37:8c:ec:d0:1e:e4:31:31:71:c2:
    0e:4d:e1:c3:eb:56:9b:a7:d5:aa:09:34:82:36:68:
    c1:ba:6c:34:05:ff:19:e9:35:de:f3:67:27:1e:71:
    6e:c4:49:73:f1:03:e1:c7:ad:12:0c:3e:04:04:f4:
    44:7e:5a:43:86:b6:e3:b2:fa:a4:28:14:04:80:e0:
    8e:05:5f:c9:e8:79:6d:fe:af
prime2:
    00:c4:68:9f:e3:b0:54:31:fb:6b:6f:e4:de:34:00:
    76:d5:fa:aa:09:d9:fd:f3:25:06:8f:c5:b4:94:dc:
    c0:18:97:74:86:18:4a:83:8d:6a:bf:00:41:c3:57:
    23:f1:43:b6:5d:26:e2:2a:9f:98:56:ae:29:f1:21:
    66:b1:f4:ef:87:60:01:94:7a:a9:91:4f:c3:f6:a7:
    22:c3:a7:ba:e9:53:5b:de:3b:5f:59:1a:61:ba:8e:
    41:fb:94:12:e2:39:9d:d7:58:7e:b4:74:53:9e:4f:
    ca:61:f4:45:94:31:73:69:19:af:0b:55:d4:2d:a4:
    e9:2a:05:ff:27:b8:d9:3c:cd
exponent1:
    00:9e:8a:29:83:75:8f:f1:cd:60:50:e3:e7:58:8b:
    f3:3d:6c:9f:32:5e:98:0f:42:60:fd:66:9d:97:6b:
```

```
    41:fb:94:12:e2:39:9d:d7:58:7e:b4:74:53:9e:4f:
    ca:61:f4:45:94:31:73:69:19:af:0b:55:d4:2d:a4:
    e9:2a:05:ff:27:b8:d9:3c:cd
exponent1:
    00:9e:8a:29:83:75:8f:f1:cd:60:50:e3:e7:58:8b:
    f3:3d:6c:9f:32:5e:98:0f:42:60:fd:66:9d:97:6b:
    38:7b:30:e1:82:1a:b9:d1:bc:fa:60:34:e6:09:75:
    5f:ee:8d:c7:6b:af:57:f8:df:59:e6:9a:8e:e0:f4:
    1a:da:d2:8e:4f:d4:90:e7:4b:6d:06:b4:3d:d8:85:
    ca:ea:97:1c:de:66:10:15:09:de:42:00:02:55:e3:
    0e:13:ae:bd:82:e8:47:6f:6d:5a:87:ab:05:11:67:
    30:64:d7:e2:96:9d:2a:30:e3:49:f2:6e:11:cf:30:
    eb:c9:5e:14:59:e4:97:9a:dd
exponent2:
    00:9a:2d:1a:dd:cb:cb:bb:d4:85:b8:b7:2a:ea:1d:
    37:2b:af:72:0c:fb:af:0a:4f:95:40:04:cd:45:51:
    a8:05:65:d6:95:70:ba:05:5c:5c:60:04:9e:9a:ed:
    6b:8c:77:3f:cf:0d:b7:da:07:9f:b8:e3:4c:8f:39:
    4d:f9:01:b1:89:4e:06:cf:7c:1e:61:b0:00:bf:3c:
    e1:e0:3e:69:4d:c1:1e:cb:6b:45:e4:96:fe:02:48:
    ab:69:06:0a:70:c5:13:af:38:8b:75:b2:1e:f5:95:
    e2:e3:53:b1:ce:ab:a6:d1:e8:d4:6c:8c:7a:5b:3e:
    29:bd:d0:29:44:10:29:8f:3d
coefficient:
    00:dd:bd:ed:9f:35:d9:f9:54:11:eb:ee:4a:d5:28:
    84:35:27:fc:7d:2e:f8:06:d9:5c:cc:e0:9a:4f:8d:
    81:10:50:a3:89:92:6f:9b:3a:cd:e1:2d:4e:cf:d8:
    b0:31:77:42:87:44:8d:af:cd:4f:5e:4d:c9:92:2c:
    32:c2:7b:57:31:9a:53:15:88:d8:3e:91:51:ca:ef:
    f3:30:d1:8f:b4:ed:b5:c5:62:08:b0:6b:fb:68:7e:
    13:33:8b:c5:36:e1:51:df:57:c3:6c:79:97:5e:4b:
    32:3c:95:af:e9:b0:5c:58:7a:93:ec:fc:38:20:19:
    a7:c7:99:c6:a1:09:3a:b8:68
[04/18/24]seed@VM:~/Workspace$
```

Task 3.3

Screenshots of server.crt

```
[04/18/24]seed@VM:~/Workspace$ openssl ca -config MyOpenssl.cnf -policy policy_anything -md sha256 -days 3650 -in server.csr -out server.crt
-batch -cert ca.crt -keyfile ca.key
Using configuration from MyOpenssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Apr 18 22:06:11 2024 GMT
            Not After : Apr 16 22:06:11 2034 GMT
        Subject:
            countryName               = US
            organizationName          = Bank32 Inc.
            commonName                = www.bank32.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                F0:FF:65:96:0E:53:74:4F:FB:82:71:F5:E9:1B:81:97:15:EB:6F:D2
            X509v3 Authority Key Identifier:
                keyid:73:E8:F7:E8:97:E9:5B:C7:79:36:76:84:1B:3E:61:B9:96:74:E7:6D

Certificate is to be certified until Apr 16 22:06:11 2034 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
[04/18/24]seed@VM:~/Workspace$ openssl x509 -in server.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
```

```
Data Base Updated
[04/18/24]seed@VM:~/Workspace$ openssl x509 -in server.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: Apr 18 22:06:11 2024 GMT
            Not After : Apr 16 22:06:11 2034 GMT
        Subject: C = US, O = Bank32 Inc., CN = www.bank32.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:b1:ac:f8:a5:03:5c:30:82:a8:92:b2:ca:e4:42:
                    9e:b2:5c:6a:28:89:06:0b:10:71:96:59:ff:7a:38:
                    0c:a5:97:70:54:ff:6b:1b:16:2b:08:8d:40:62:4b:
                    71:72:18:13:9b:8a:7b:d2:60:69:73:b4:3f:55:f5:
                    b4:d0:05:e0:f7:c2:1c:d6:31:ff:2c:a5:b6:13:30:
                    35:4c:0f:0e:d1:0f:39:92:8b:c2:67:13:fc:a4:9a:
                    d4:cf:b1:86:b5:c6:40:09:44:93:f1:b2:a8:95:c9:
                    fb:1f:b0:cc:df:ab:54:e6:73:b1:5d:44:2b:c5:b5:
                    ba:d6:b8:b4:7b:9d:5e:20:db:e7:5f:26:93:70:a2:
                    c3:eb:47:86:0f:14:7f:68:b7:33:ef:e9:33:e6:c1:
                    c0:25:6f:20:4c:e8:8b:da:51:37:d9:b2:d4:e2:19:
                    b9:8a:b0:b4:16:07:81:e2:c9:f6:33:d4:f5:37:e2:
                    4e:6e:1f:c1:de:f1:5d:73:aa:01:f2:b9:e8:e1:cc:
                    7a:f0:f1:44:c8:db:4d:f2:5f:b0:d7:f2:31:40:75:
                    3c:a2:0c:c8:ce:d5:f1:d7:8c:d5:bb:f3:5f:b1:ad:
                    93:ec:a3:5a:e5:01:2f:30:c4:75:93:b4:aa:96:7d:
```

```
                c0:25:6f:20:4c:e8:8b:da:51:37:d9:b2:d4:e2:19:
                b9:8a:b0:b4:16:07:81:e2:c9:f6:33:d4:f5:37:e2:
                4e:6e:1f:c1:de:f1:5d:73:aa:01:f2:b9:e8:e1:cc:
                7a:f0:f1:44:c8:db:4d:f2:5f:b0:d7:f2:31:40:75:
                3c:a2:0c:c8:ce:d5:f1:d7:8c:d5:bb:f3:5f:b1:ad:
                93:ec:a3:5a:e5:01:2f:30:c4:75:93:b4:aa:96:7d:
                e8:ca:10:f1:71:3a:49:29:e2:be:3a:46:92:af:1c:
                f6:23
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
            F0:FF:65:96:0E:53:74:4F:FB:82:71:F5:E9:1B:81:97:15:EB:6F:D2
        X509v3 Authority Key Identifier:
            keyid:73:E8:F7:E8:97:E9:5B:C7:79:36:76:84:1B:3E:61:B9:96:74:E7:6D

Signature Algorithm: sha256WithRSAEncryption
     2e:e6:2b:d9:69:0d:0c:fe:3d:6c:41:7a:a1:42:91:2c:25:af:
     43:fb:d9:bc:6b:a8:bf:56:8d:8d:21:b1:11:79:db:2e:73:a0:
     fc:f5:18:5e:57:b8:3a:28:ca:29:29:1d:8d:56:c4:80:88:6c:
     4a:04:52:a7:97:47:dc:e7:e4:af:fb:50:0c:75:a8:97:81:c2:
     1d:06:d3:2c:fb:4a:2b:4b:92:0f:0d:f0:d1:e9:42:44:a8:3a:
     b4:1d:01:c6:48:3a:6f:e6:aa:30:58:73:4f:c2:54:3f:f2:2b:
     88:8f:ce:39:a1:1c:1b:4c:44:df:82:dd:67:d8:40:04:38:35:
     68:d2:99:5e:f8:8e:9a:0f:54:99:71:8c:2c:60:3f:ca:aa:d7:
     29:a5:ed:41:4a:f3:a5:8b:95:f9:15:d6:19:8f:2f:24:ee:4b:
     80:3d:de:7e:31:2d:e9:36:05:50:60:93:00:51:9c:7d:66:72:
```

```
    Signature Algorithm: sha256WithRSAEncryption
         2e:e6:2b:d9:69:0d:0c:fe:3d:6c:41:7a:a1:42:91:2c:25:af:
         43:fb:d9:bc:6b:a8:bf:56:8d:8d:21:b1:11:79:db:2e:73:a0:
         fc:f5:18:5e:57:b8:3a:28:ca:29:29:1d:8d:56:c4:80:88:6c:
         4a:04:52:a7:97:47:dc:e7:e4:af:fb:50:0c:75:a8:97:81:c2:
         1d:06:d3:2c:fb:4a:2b:4b:92:0f:0d:f0:d1:e9:42:44:a8:3a:
         b4:1d:01:c6:48:3a:6f:e6:aa:30:58:73:4f:c2:54:3f:f2:2b:
         88:8f:ce:39:a1:1c:1b:4c:44:df:82:dd:67:d8:40:04:38:35:
         68:d2:99:5e:f8:8e:9a:0f:54:99:71:8c:2c:60:3f:ca:aa:d7:
         29:a5:ed:41:4a:f3:a5:8b:95:f9:15:d6:19:8f:2f:24:ee:4b:
         80:3d:de:7e:31:2d:e9:36:05:50:60:93:00:51:9c:7d:66:72:
         33:a8:dd:49:26:a4:fa:74:8a:41:66:27:df:58:38:6c:bd:15:
         37:e9:09:66:91:19:4b:87:76:1f:8d:4d:e5:6d:c6:14:56:d6:
         76:a4:9d:2d:c9:bf:69:2a:8f:ec:9c:a5:e4:18:d2:49:06:1b:
         8f:1a:72:49:51:db:31:7f:21:f2:12:bd:62:80:c4:58:e8:b4:
         27:db:16:b6:5b:3b:9d:34:a2:92:0c:bb:0d:ec:7b:bb:c3:2f:
         7d:4e:45:5f:94:84:1b:dd:47:89:b0:0c:71:08:cf:b4:6a:42:
         a6:02:bc:70:e8:5f:a8:ad:de:9e:a0:b1:58:2a:0f:43:1e:55:
         87:35:93:ac:b0:68:60:69:d8:a8:b9:64:7c:e5:29:86:c4:29:
         e9:79:98:a3:98:df:b7:34:5f:be:c9:f2:fe:0e:85:40:ec:20:
         14:b7:a3:b1:b4:07:41:f7:b1:e2:f8:18:c0:ac:14:65:6f:ec:
         f9:f5:12:8d:0f:e1:38:b1:3e:ee:a3:34:6a:56:ad:d7:34:e3:
         43:5f:24:ee:fd:70:6b:9f:68:3d:46:c4:f9:4d:96:4d:8a:30:
         59:30:7b:2f:0d:d1:ce:05:43:8d:2b:18:bb:13:44:56:57:d0:
         2a:3c:b2:7a:76:74:d5:a7:f3:c9:b0:ac:ec:54:86:19:6d:a8:
         85:a4:3d:17:b2:af:fa:1d:62:be:77:06:f1:17:ef:b6:05:98:
         7b:e6:a2:d7:84:f4:44:6b:09:97:cb:fe:94:e9:3d:e0:ef:8b:
         24:07:20:95:cb:e8:9f:66:c7:63:d6:4f:89:41:4e:d4:49:cd:
         a9:73:e6:41:cd:71:a9:ad:09:71:ea:55:1f:61:53:6d:a8:6f:
         b6:2e:28:14:e6:4b:a6:30
[04/18/24]seed@VM:~/Workspace$ echo "Rithik Sarvesh Bharathiraja - 120395246"
Rithik Sarvesh Bharathiraja - 120395246
[04/18/24]seed@VM:~/Workspace$
```