CPS 633 Section 09

Public-Key Infrastructure (PKI) Lab

Group 18

Roxie Reginold (501087897)
Hetu Virajkumar Patel (501215707)
Sayyada Aisha Mehvish (501106795)

To set up the CA directory structure, we created the following directories and files:

```
mkdir demoCA
mkdir demoCA/certs
mkdir demoCA/crl
mkdir demoCA/newcerts
touch demoCA/index.txt
echo 1000 > demoCA/serial
```

Task 1: Becoming a Certificate Authority (CA)

- What part of the certificate indicates this is a CA's certificate?

```
        X509v3 Basic Constraints: critical
            CA:TRUE
```

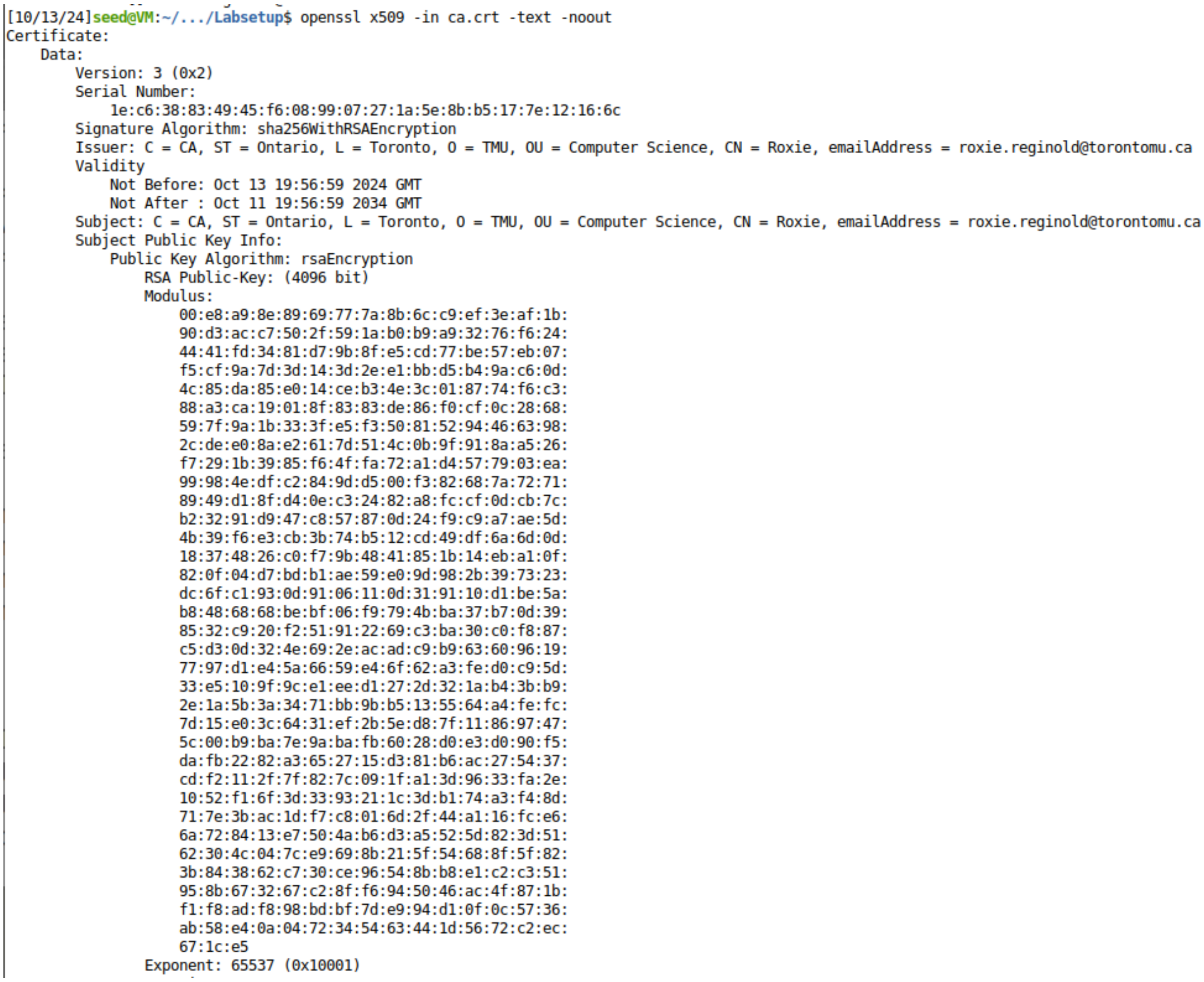
- What part of the certificate indicates this is a self-signed certificate?

```
Issuer: C = CA, ST = Ontario, L = Toronto, O = TMU, OU = Computer Science, CN = Roxie,
emailAddress = roxie.reginold@torontomu.ca
      Validity
         Not Before: Oct 13 19:56:59 2024 GMT
         Not After : Oct 11 19:56:59 2034 GMT
      Subject: C = CA, ST = Ontario, L = Toronto, O = TMU, OU = Computer Science, CN = Roxie,
emailAddress = roxie.reginold@torontomu.ca
```

We would check the issuer and the subject lines. In this case they are the same so this certificate is self-signed,

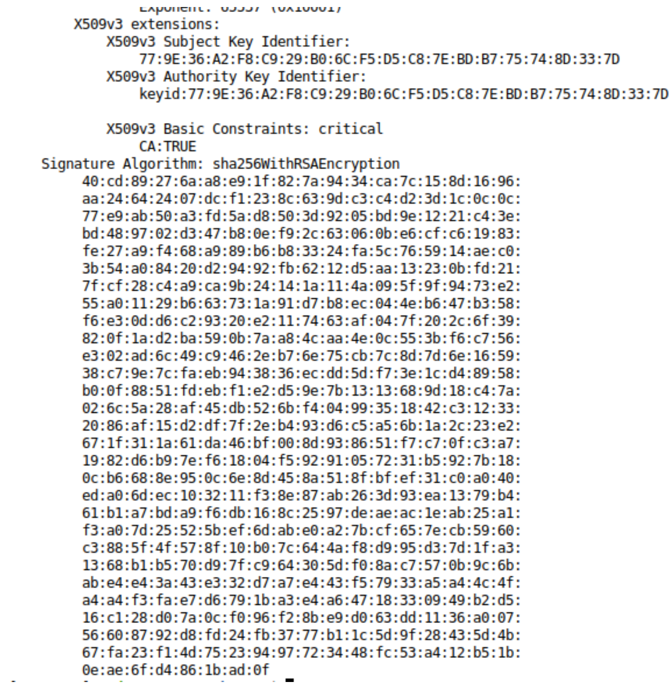
- In the RSA algorithm, we have a
  - public exponent e,
  - a private exponent d,
  - a modulus n, and
  - two secret numbers p and q, such that n = pq.

Output for openssl x509 -in ca.crt -text -noout (contents of certificate)



```
[10/13/24]seed@VM:~/.../Labsetup$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            1e:c6:38:83:49:45:f6:08:99:07:27:1a:5e:8b:b5:17:7e:12:16:6c
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = CA, ST = Ontario, L = Toronto, O = TMU, OU = Computer Science, CN = Roxie, emailAddress = roxie.reginold@torontomu.ca
        Validity
            Not Before: Oct 13 19:56:59 2024 GMT
            Not After : Oct 11 19:56:59 2034 GMT
        Subject: C = CA, ST = Ontario, L = Toronto, O = TMU, OU = Computer Science, CN = Roxie, emailAddress = roxie.reginold@torontomu.ca
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:e8:a9:8e:89:69:77:7a:8b:6c:c9:ef:3e:af:1b:
                    90:d3:ac:c7:50:2f:59:1a:b0:b9:a9:32:76:f6:24:
                    44:41:fd:34:81:d7:9b:8f:e5:cd:77:be:57:eb:07:
                    f5:cf:9a:7d:3d:14:3d:2e:e1:bb:d5:b4:9a:c6:0d:
                    4c:85:da:85:e0:14:ce:b3:4e:3c:01:87:74:f6:c3:
                    88:a3:ca:19:01:8f:83:83:de:86:f0:cf:0c:28:68:
                    59:7f:9a:1b:33:3f:e5:f3:50:81:52:94:46:63:98:
                    2c:de:e0:8a:e2:61:7d:51:4c:0b:9f:91:8a:a5:26:
                    f7:29:1b:39:85:f6:4f:fa:72:a1:d4:57:79:03:ea:
                    99:98:4e:df:c2:84:9d:d5:00:f3:82:68:7a:72:71:
                    89:49:d1:8f:d4:0e:c3:24:82:a8:fc:cf:0d:cb:7c:
                    b2:32:91:d9:47:c8:57:87:0d:24:f9:c9:a7:ae:5d:
                    4b:39:f6:e3:cb:3b:74:b5:12:cd:49:df:6a:6d:0d:
                    18:37:48:26:c0:f7:9b:48:41:85:1b:14:eb:a1:0f:
                    82:0f:04:d7:bd:b1:ae:59:e0:9d:98:2b:39:73:23:
                    dc:6f:c1:93:0d:91:06:11:0d:31:91:10:d1:be:5a:
                    b8:48:68:68:be:bf:06:f9:79:4b:ba:37:b7:0d:39:
                    85:32:c9:20:f2:51:91:22:69:c3:ba:30:c0:f8:87:
                    c5:d3:0d:32:4e:69:2e:ac:ad:c9:b9:63:60:96:19:
                    77:97:d1:e4:5a:66:59:e4:6f:62:a3:fe:d0:c9:5d:
                    33:e5:10:9f:9c:e1:ee:d1:27:2d:32:1a:b4:3b:b9:
                    2e:1a:5b:3a:34:71:bb:9b:b5:13:55:64:a4:fe:fc:
                    7d:15:e0:3c:64:31:ef:2b:5e:d8:7f:11:86:97:47:
                    5c:00:b9:ba:7e:9a:ba:fb:60:28:d0:e3:d0:90:f5:
                    da:fb:22:82:a3:65:27:15:d3:81:b6:ac:27:54:37:
                    cd:f2:11:2f:7f:82:7c:09:1f:a1:3d:96:33:fa:2e:
                    10:52:f1:6f:3d:33:93:21:1c:3d:b1:74:a3:f4:8d:
                    71:7e:3b:ac:1d:f7:c8:01:6d:2f:44:a1:16:fc:e6:
                    6a:72:84:13:e7:50:4a:b6:d3:a5:52:5d:82:3d:51:
                    62:30:4c:04:7c:e9:69:8b:21:5f:54:68:8f:5f:82:
                    3b:84:38:62:c7:30:ce:96:54:8b:b8:e1:c2:c3:51:
                    95:8b:67:32:67:c2:8f:f6:94:50:46:ac:4f:87:1b:
                    f1:f8:ad:f8:98:bd:bf:7d:e9:94:d1:0f:0c:57:36:
                    ab:58:e4:0a:04:72:34:54:63:44:1d:56:72:c2:ec:
                    67:1c:e5
                Exponent: 65537 (0x10001)
```

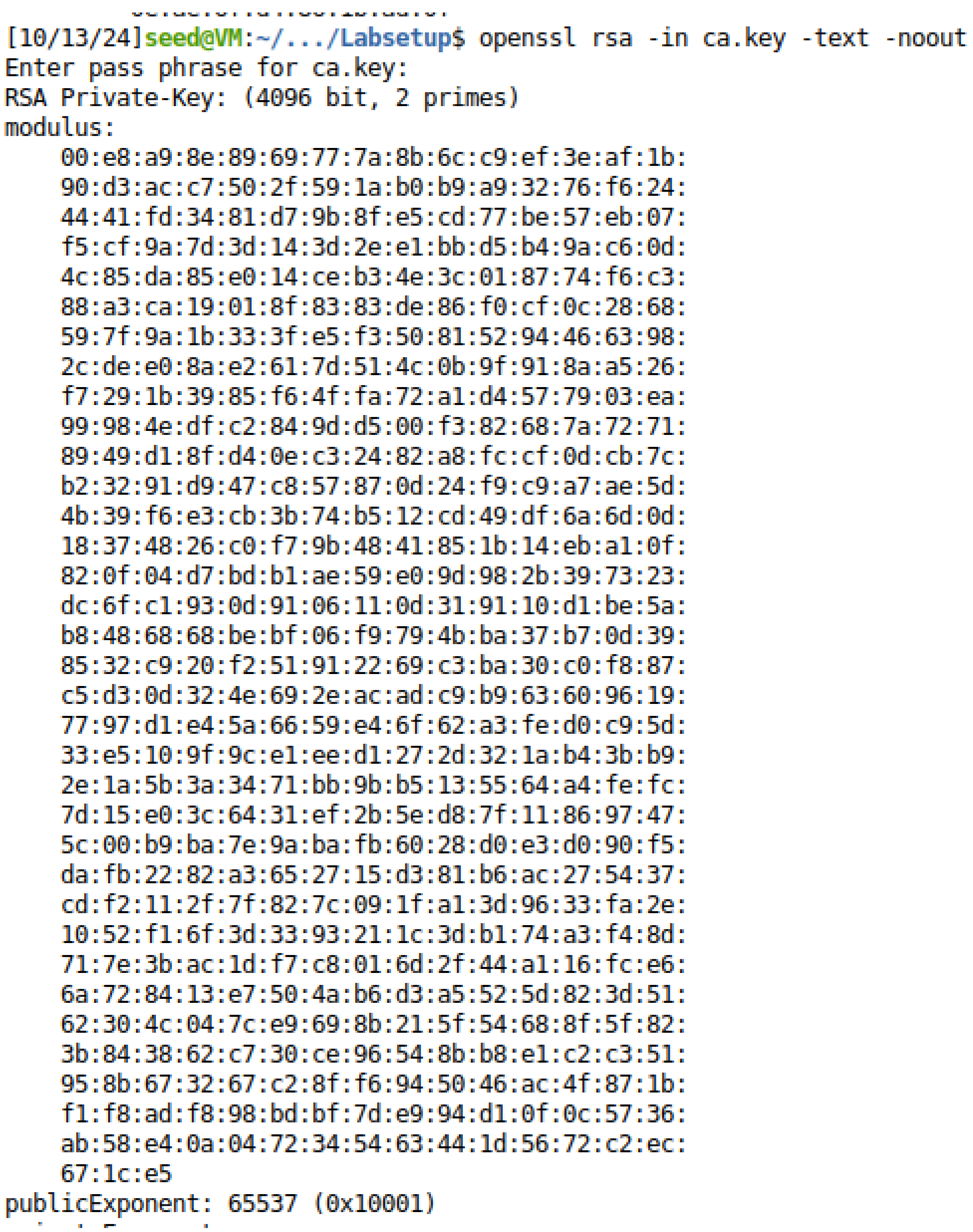
The certificate contains the Modulus n and the public exponent (e = 65537).



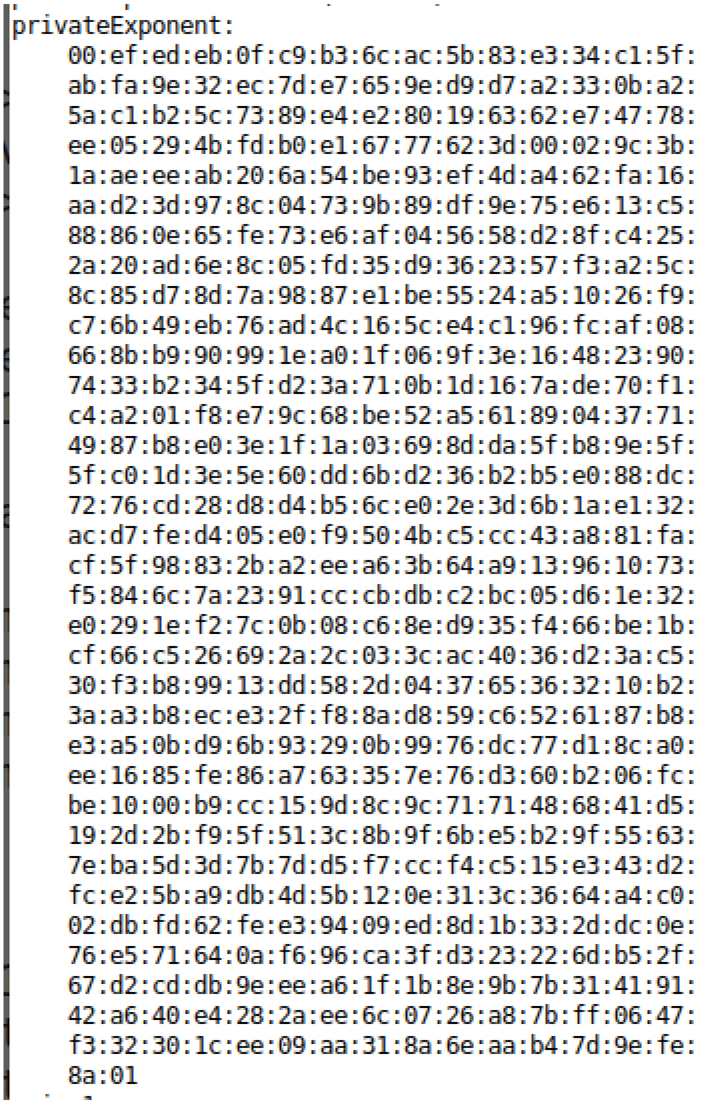
```
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                77:9E:36:A2:F8:C9:29:B0:6C:F5:D5:C8:7E:BD:B7:75:74:8D:33:7D
            X509v3 Authority Key Identifier:
                keyid:77:9E:36:A2:F8:C9:29:B0:6C:F5:D5:C8:7E:BD:B7:75:74:8D:33:7D

            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         40:cd:89:27:6a:a8:e9:1f:82:7a:94:34:ca:7c:15:8d:16:96:
         aa:24:64:24:07:dc:f1:23:8c:63:9d:c3:c4:d2:3d:1c:0c:0c:
         77:e9:ab:50:a3:fd:5a:d8:50:3d:92:05:bd:9e:12:21:c4:3e:
         bd:48:97:02:d3:47:b8:0e:f9:2c:63:06:0b:e6:cf:c6:19:83:
         fe:27:a9:f4:68:a9:89:b6:b8:33:24:fa:5c:76:59:14:ae:c0:
         3b:54:a0:84:20:d2:94:92:fb:62:12:d5:aa:13:23:0b:fd:21:
         7f:cf:28:c4:a9:ca:9b:24:14:1a:11:4a:09:5f:9f:94:73:e2:
         55:a0:11:29:b6:63:73:1a:91:d7:b8:ec:04:4e:b6:47:b3:58:
         f6:e3:0d:d6:c2:93:20:e2:11:74:63:af:04:7f:20:2c:6f:39:
         82:0f:1a:d2:ba:59:0b:7a:a8:4c:aa:4e:0c:55:3b:f6:c7:56:
         e3:02:ad:6c:49:c9:46:2e:b7:6e:75:cb:7c:8d:7d:6e:16:59:
         38:c7:9e:7c:fa:eb:94:38:36:ec:dd:5d:f7:3e:1c:d4:89:58:
         b0:0f:88:51:fd:eb:f1:e2:d5:9e:7b:13:13:68:9d:18:c4:7a:
         02:6c:5a:28:af:45:db:52:6b:f4:04:99:35:18:42:c3:12:33:
         20:86:af:15:d2:df:7f:2e:b4:93:d6:c5:a5:6b:1a:2c:23:e2:
         67:1f:31:1a:61:da:46:bf:00:8d:93:86:51:f7:c7:0f:c3:a7:
         19:82:d6:b9:7e:f6:18:04:f5:92:91:05:72:31:b5:92:7b:18:
         0c:b6:68:8e:95:0c:6e:8d:45:8a:51:8f:bf:ef:31:c0:a0:40:
         ed:a0:6d:ec:10:32:11:f3:8e:87:ab:26:3d:93:ea:13:79:b4:
         61:b1:a7:bd:a9:f6:db:16:8c:25:97:de:ae:ac:1e:ab:25:a1:
         f3:a0:7d:25:52:5b:ef:6d:ab:e0:a2:7b:cf:65:7e:cb:59:60:
         c3:88:5f:4f:57:8f:10:b0:7c:64:4a:f8:d9:95:d3:7d:1f:a3:
         13:68:b1:b5:70:d9:7f:c9:64:30:5d:f0:8a:c7:57:0b:9c:6b:
         ab:e4:e4:3a:43:e3:32:d7:a7:e4:43:f5:79:33:a5:a4:4c:4f:
         a4:a4:f3:fa:e7:d6:79:1b:a3:e4:a6:47:18:33:09:49:b2:d5:
         16:c1:28:d0:7a:0c:f0:96:f2:8b:e9:d0:63:dd:11:36:a0:07:
         56:60:87:92:d8:fd:24:fb:37:77:b1:1c:5d:9f:28:43:5d:4b:
         67:fa:23:f1:4d:75:23:94:97:72:34:48:fc:53:a4:12:b5:1b:
         0e:ae:6f:d4:86:1b:ad:0f
```

Output of openssl rsa -in ca.key -text -noout

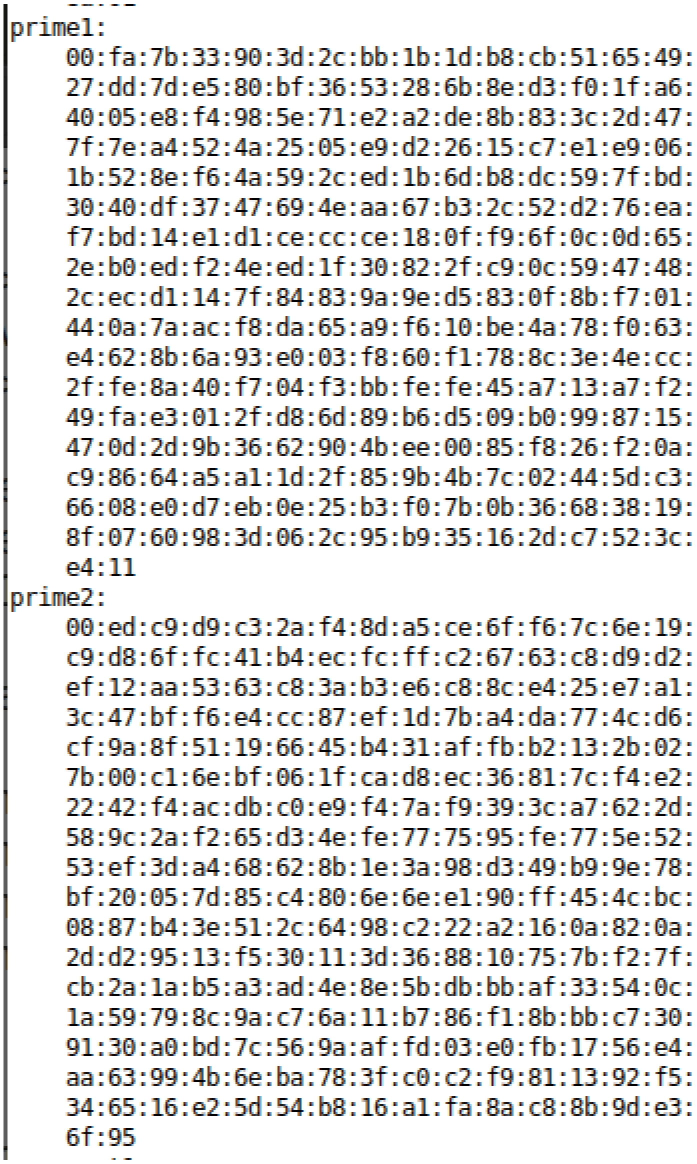
The private key contains the modulus n , public exponent e , private exponent e, prime1 which is p and prime2 which is q.



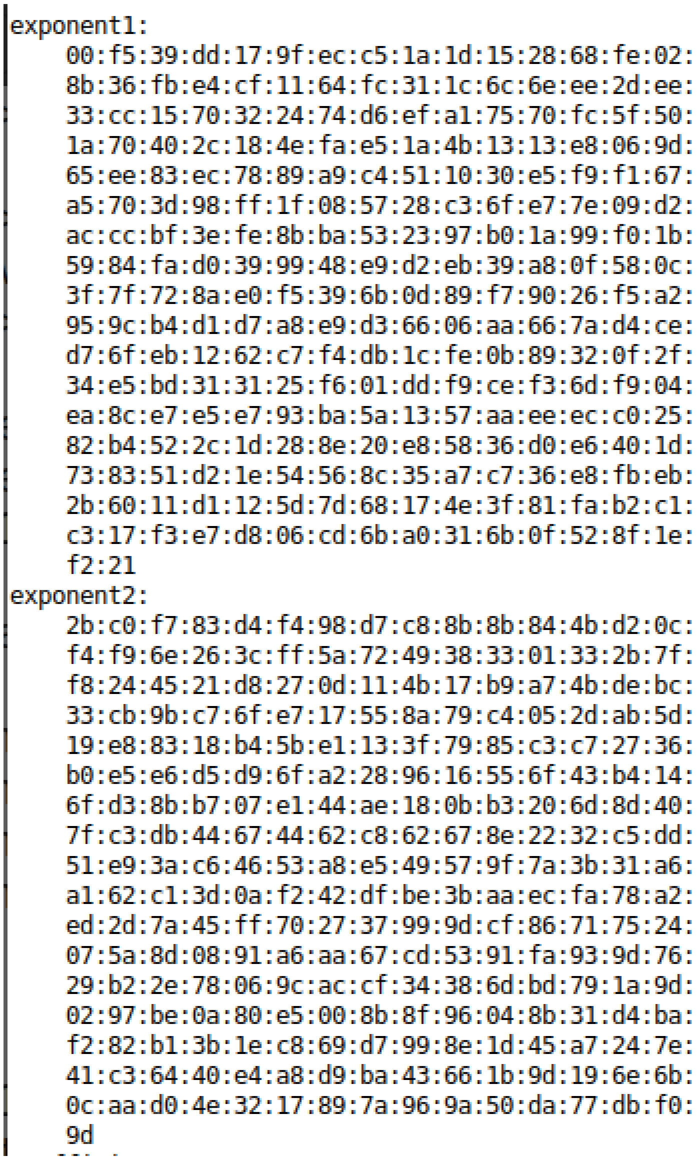
```
[10/13/24]seed@VM:~/.../Labsetup$ openssl rsa -in ca.key -text -noout
Enter pass phrase for ca.key:
RSA Private-Key: (4096 bit, 2 primes)
modulus:
    00:e8:a9:8e:89:69:77:7a:8b:6c:c9:ef:3e:af:1b:
    90:d3:ac:c7:50:2f:59:1a:b0:b9:a9:32:76:f6:24:
    44:41:fd:34:81:d7:9b:8f:e5:cd:77:be:57:eb:07:
    f5:cf:9a:7d:3d:14:3d:2e:e1:bb:d5:b4:9a:c6:0d:
    4c:85:da:85:e0:14:ce:b3:4e:3c:01:87:74:f6:c3:
    88:a3:ca:19:01:8f:83:83:de:86:f0:cf:0c:28:68:
    59:7f:9a:1b:33:3f:e5:f3:50:81:52:94:46:63:98:
    2c:de:e0:8a:e2:61:7d:51:4c:0b:9f:91:8a:a5:26:
    f7:29:1b:39:85:f6:4f:fa:72:a1:d4:57:79:03:ea:
    99:98:4e:df:c2:84:9d:d5:00:f3:82:68:7a:72:71:
    89:49:d1:8f:d4:0e:c3:24:82:a8:fc:cf:0d:cb:7c:
    b2:32:91:d9:47:c8:57:87:0d:24:f9:c9:a7:ae:5d:
    4b:39:f6:e3:cb:3b:74:b5:12:cd:49:df:6a:6d:0d:
    18:37:48:26:c0:f7:9b:48:41:85:1b:14:eb:a1:0f:
    82:0f:04:d7:bd:b1:ae:59:e0:9d:98:2b:39:73:23:
    dc:6f:c1:93:0d:91:06:11:0d:31:91:10:d1:be:5a:
    b8:48:68:68:be:bf:06:f9:79:4b:ba:37:b7:0d:39:
    85:32:c9:20:f2:51:91:22:69:c3:ba:30:c0:f8:87:
    c5:d3:0d:32:4e:69:2e:ac:ad:c9:b9:63:60:96:19:
    77:97:d1:e4:5a:66:59:e4:6f:62:a3:fe:d0:c9:5d:
    33:e5:10:9f:9c:e1:ee:d1:27:2d:32:1a:b4:3b:b9:
    2e:1a:5b:3a:34:71:bb:9b:b5:13:55:64:a4:fe:fc:
    7d:15:e0:3c:64:31:ef:2b:5e:d8:7f:11:86:97:47:
    5c:00:b9:ba:7e:9a:ba:fb:60:28:d0:e3:d0:90:f5:
    da:fb:22:82:a3:65:27:15:d3:81:b6:ac:27:54:37:
    cd:f2:11:2f:7f:82:7c:09:1f:a1:3d:96:33:fa:2e:
    10:52:f1:6f:3d:33:93:21:1c:3d:b1:74:a3:f4:8d:
    71:7e:3b:ac:1d:f7:c8:01:6d:2f:44:a1:16:fc:e6:
    6a:72:84:13:e7:50:4a:b6:d3:a5:52:5d:82:3d:51:
    62:30:4c:04:7c:e9:69:8b:21:5f:54:68:8f:5f:82:
    3b:84:38:62:c7:30:ce:96:54:8b:b8:e1:c2:c3:51:
    95:8b:67:32:67:c2:8f:f6:94:50:46:ac:4f:87:1b:
    f1:f8:ad:f8:98:bd:bf:7d:e9:94:d1:0f:0c:57:36:
    ab:58:e4:0a:04:72:34:54:63:44:1d:56:72:c2:ec:
    67:1c:e5
publicExponent: 65537 (0x10001)
```



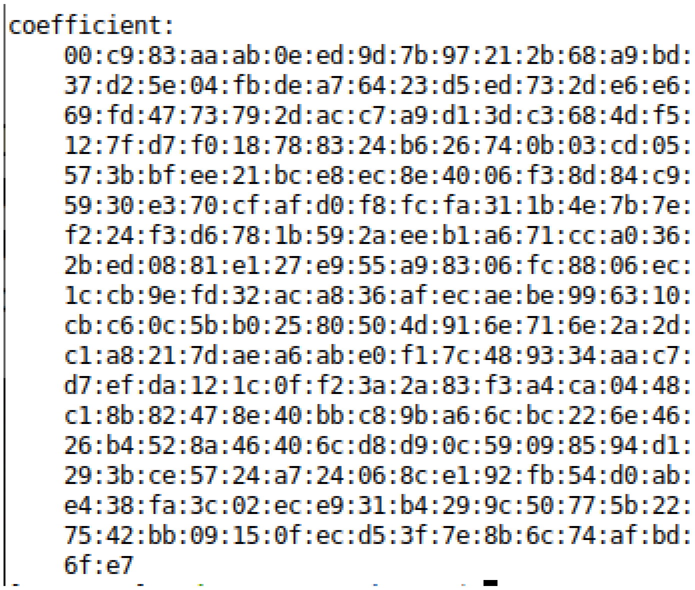
```
privateExponent:
    00:ef:ed:eb:0f:c9:b3:6c:ac:5b:83:e3:34:c1:5f:
    ab:fa:9e:32:ec:7d:e7:65:9e:d9:d7:a2:33:0b:a2:
    5a:c1:b2:5c:73:89:e4:e2:80:19:63:62:e7:47:78:
    ee:05:29:4b:fd:b0:e1:67:77:62:3d:00:02:9c:3b:
    1a:ae:ee:ab:20:6a:54:be:93:ef:4d:a4:62:fa:16:
    aa:d2:3d:97:8c:04:73:9b:89:df:9e:75:e6:13:c5:
    88:86:0e:65:fe:73:e6:af:04:56:58:d2:8f:c4:25:
    2a:20:ad:6e:8c:05:fd:35:d9:36:23:57:f3:a2:5c:
    8c:85:d7:8d:7a:98:87:e1:be:55:24:a5:10:26:f9:
    c7:6b:49:eb:76:ad:4c:16:5c:e4:c1:96:fc:af:08:
    66:8b:b9:90:99:1e:a0:1f:06:9f:3e:16:48:23:90:
    74:33:b2:34:5f:d2:3a:71:0b:1d:16:7a:de:70:f1:
    c4:a2:01:f8:e7:9c:68:be:52:a5:61:89:04:37:71:
    49:87:b8:e0:3e:1f:1a:03:69:8d:da:5f:b8:9e:5f:
    5f:c0:1d:3e:5e:60:dd:6b:d2:36:b2:b5:e0:88:dc:
    72:76:cd:28:d8:d4:b5:6c:e0:2e:3d:6b:1a:e1:32:
    ac:d7:fe:d4:05:e0:f9:50:4b:c5:cc:43:a8:81:fa:
    cf:5f:98:83:2b:a2:ee:a6:3b:64:a9:13:96:10:73:
    f5:84:6c:7a:23:91:cc:cb:db:c2:bc:05:d6:1e:32:
    e0:29:1e:f2:7c:0b:08:c6:8e:d9:35:f4:66:be:1b:
    cf:66:c5:26:69:2a:2c:03:3c:ac:40:36:d2:3a:c5:
    30:f3:b8:99:13:dd:58:2d:04:37:65:36:32:10:b2:
    3a:a3:b8:ec:e3:2f:f8:8a:d8:59:c6:52:61:87:b8:
    e3:a5:0b:d9:6b:93:29:0b:99:76:dc:77:d1:8c:a0:
    ee:16:85:fe:86:a7:63:35:7e:76:d3:60:b2:06:fc:
    be:10:00:b9:cc:15:9d:8c:9c:71:71:48:68:41:d5:
    19:2d:2b:f9:5f:51:3c:8b:9f:6b:e5:b2:9f:55:63:
    7e:ba:5d:3d:7b:7d:d5:f7:cc:f4:c5:15:e3:43:d2:
    fc:e2:5b:a9:db:4d:5b:12:0e:31:3c:36:64:a4:c0:
    02:db:fd:62:fe:e3:94:09:ed:8d:1b:33:2d:dc:0e:
    76:e5:71:64:0a:f6:96:ca:3f:d3:23:22:6d:b5:2f:
    67:d2:cd:db:9e:ee:a6:1f:1b:8e:9b:7b:31:41:91:
    42:a6:40:e4:28:2a:ee:6c:07:26:a8:7b:ff:06:47:
    f3:32:30:1c:ee:09:aa:31:8a:6e:aa:b4:7d:9e:fe:
    8a:01
```



```
prime1:
    00:fa:7b:33:90:3d:2c:bb:1b:1d:b8:cb:51:65:49:
    27:dd:7d:e5:80:bf:36:53:28:6b:8e:d3:f0:1f:a6:
    40:05:e8:f4:98:5e:71:e2:a2:de:8b:83:3c:2d:47:
    7f:7e:a4:52:4a:25:05:e9:d2:26:15:c7:e1:e9:06:
    1b:52:8e:f6:4a:59:2c:ed:1b:6d:b8:dc:59:7f:bd:
    30:40:df:37:47:69:4e:aa:67:b3:2c:52:d2:76:ea:
    f7:bd:14:e1:d1:ce:cc:ce:18:0f:f9:6f:0c:0d:65:
    2e:b0:ed:f2:4e:ed:1f:30:82:2f:c9:0c:59:47:48:
    2c:ec:d1:14:7f:84:83:9a:9e:d5:83:0f:8b:f7:01:
    44:0a:7a:ac:f8:da:65:a9:f6:10:be:4a:78:f0:63:
    e4:62:8b:6a:93:e0:03:f8:60:f1:78:8c:3e:4e:cc:
    2f:fe:8a:40:f7:04:f3:bb:fe:fe:45:a7:13:a7:f2:
    49:fa:e3:01:2f:d8:6d:89:b6:d5:09:b0:99:87:15:
    47:0d:2d:9b:36:62:90:4b:ee:00:85:f8:26:f2:0a:
    c9:86:64:a5:a1:1d:2f:85:9b:4b:7c:02:44:5d:c3:
    66:08:e0:d7:eb:0e:25:b3:f0:7b:0b:36:68:38:19:
    8f:07:60:98:3d:06:2c:95:b9:35:16:2d:c7:52:3c:
    e4:11
prime2:
    00:ed:c9:d9:c3:2a:f4:8d:a5:ce:6f:f6:7c:6e:19:
    c9:d8:6f:fc:41:b4:ec:fc:ff:c2:67:63:c8:d9:d2:
    ef:12:aa:53:63:c8:3a:b3:e6:c8:8c:e4:25:e7:a1:
    3c:47:bf:f6:e4:cc:87:ef:1d:7b:a4:da:77:4c:d6:
    cf:9a:8f:51:19:66:45:b4:31:af:fb:b2:13:2b:02:
    7b:00:c1:6e:bf:06:1f:ca:d8:ec:36:81:7c:f4:e2:
    22:42:f4:ac:db:c0:e9:f4:7a:f9:39:3c:a7:62:2d:
    58:9c:2a:f2:65:d3:4e:fe:77:75:95:fe:77:5e:52:
    53:ef:3d:a4:68:62:8b:1e:3a:98:d3:49:b9:9e:78:
    bf:20:05:7d:85:c4:80:6e:6e:e1:90:ff:45:4c:bc:
    08:87:b4:3e:51:2c:64:98:c2:22:a2:16:0a:82:0a:
    2d:d2:95:13:f5:30:11:3d:36:88:10:75:7b:f2:7f:
    cb:2a:1a:b5:a3:ad:4e:8e:5b:db:bb:af:33:54:0c:
    1a:59:79:8c:9a:c7:6a:11:b7:86:f1:8b:bb:c7:30:
    91:30:a0:bd:7c:56:9a:af:fd:03:e0:fb:17:56:e4:
    aa:63:99:4b:6e:ba:78:3f:c0:c2:f9:81:13:92:f5:
    34:65:16:e2:5d:54:b8:16:a1:fa:8a:c8:8b:9d:e3:
    6f:95
```

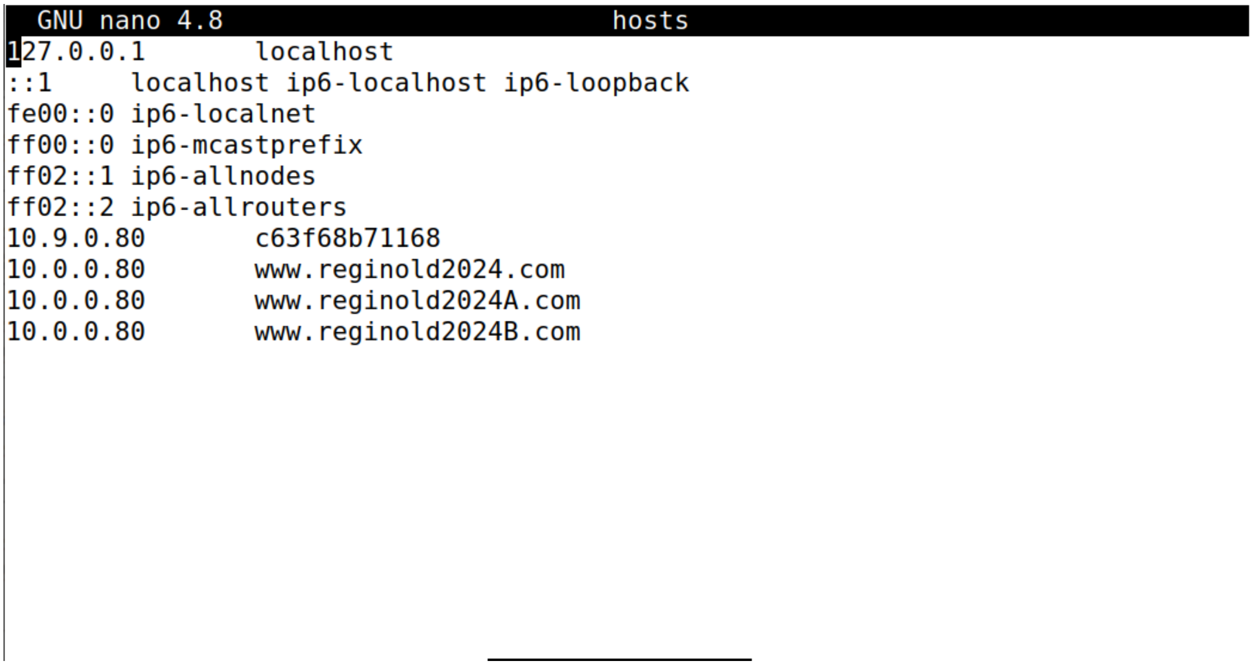


```
exponent1:
    00:f5:39:dd:17:9f:ec:c5:1a:1d:15:28:68:fe:02:
    8b:36:fb:e4:cf:11:64:fc:31:1c:6c:6e:ee:2d:ee:
    33:cc:15:70:32:24:74:d6:ef:a1:75:70:fc:5f:50:
    1a:70:40:2c:18:4e:fa:e5:1a:4b:13:13:e8:06:9d:
    65:ee:83:ec:78:89:a9:c4:51:10:30:e5:f9:f1:67:
    a5:70:3d:98:ff:1f:08:57:28:c3:6f:e7:7e:09:d2:
    ac:cc:bf:3e:fe:8b:ba:53:23:97:b0:1a:99:f0:1b:
    59:84:fa:d0:39:99:48:e9:d2:eb:39:a8:0f:58:0c:
    3f:7f:72:8a:e0:f5:39:6b:0d:89:f7:90:26:f5:a2:
    95:9c:b4:d1:d7:a8:e9:d3:66:06:aa:66:7a:d4:ce:
    d7:6f:eb:12:62:c7:f4:db:1c:fe:0b:89:32:0f:2f:
    34:e5:bd:31:31:25:f6:01:dd:f9:ce:f3:6d:f9:04:
    ea:8c:e7:e5:e7:93:ba:5a:13:57:aa:ee:ec:c0:25:
    82:b4:52:2c:1d:28:8e:20:e8:58:36:d0:e6:40:1d:
    73:83:51:d2:1e:54:56:8c:35:a7:c7:36:e8:fb:eb:
    2b:60:11:d1:12:5d:7d:68:17:4e:3f:81:fa:b2:c1:
    c3:17:f3:e7:d8:06:cd:6b:a0:31:6b:0f:52:8f:1e:
    f2:21
exponent2:
    2b:c0:f7:83:d4:f4:98:d7:c8:8b:8b:84:4b:d2:0c:
    f4:f9:6e:26:3c:ff:5a:72:49:38:33:01:33:2b:7f:
    f8:24:45:21:d8:27:0d:11:4b:17:b9:a7:4b:de:bc:
    33:cb:9b:c7:6f:e7:17:55:8a:79:c4:05:2d:ab:5d:
    19:e8:83:18:b4:5b:e1:13:3f:79:85:c3:c7:27:36:
    b0:e5:e6:d5:d9:6f:a2:28:96:16:55:6f:43:b4:14:
    6f:d3:8b:b7:07:e1:44:ae:18:0b:b3:20:6d:8d:40:
    7f:c3:db:44:67:44:62:c8:62:67:8e:22:32:c5:dd:
    51:e9:3a:c6:46:53:a8:e5:49:57:9f:7a:3b:31:a6:
    a1:62:c1:3d:0a:f2:42:df:be:3b:aa:ec:fa:78:a2:
    ed:2d:7a:45:ff:70:27:37:99:9d:cf:86:71:75:24:
    07:5a:8d:08:91:a6:aa:67:cd:53:91:fa:93:9d:76:
    29:b2:2e:78:06:9c:ac:cf:34:38:6d:bd:79:1a:9d:
    02:97:be:0a:80:e5:00:8b:8f:96:04:8b:31:d4:ba:
    f2:82:b1:3b:1e:c8:69:d7:99:8e:1d:45:a7:24:7e:
    41:c3:64:40:e4:a8:d9:ba:43:66:1b:9d:19:6e:6b:
    0c:aa:d0:4e:32:17:89:7a:96:9a:50:da:77:db:f0:
    9d
```

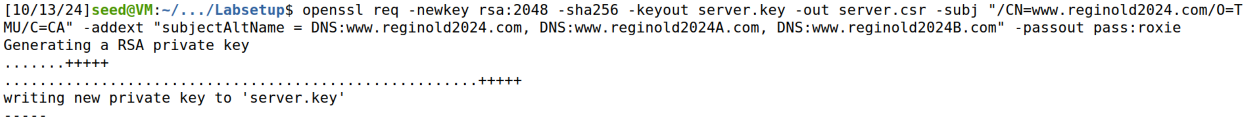


```
coefficient:
    00:c9:83:aa:ab:0e:ed:9d:7b:97:21:2b:68:a9:bd:
    37:d2:5e:04:fb:de:a7:64:23:d5:ed:73:2d:e6:e6:
    69:fd:47:73:79:2d:ac:c7:a9:d1:3d:c3:68:4d:f5:
    12:7f:d7:f0:18:78:83:24:b6:26:74:0b:03:cd:05:
    57:3b:bf:ee:21:bc:e8:ec:8e:40:06:f3:8d:84:c9:
    59:30:e3:70:cf:af:d0:f8:fc:fa:31:1b:4e:7b:7e:
    f2:24:f3:d6:78:1b:59:2a:ee:b1:a6:71:cc:a0:36:
    2b:ed:08:81:e1:27:e9:55:a9:83:06:fc:88:06:ec:
    1c:cb:9e:fd:32:ac:a8:36:af:ec:ae:be:99:63:10:
    cb:c6:0c:5b:b0:25:80:50:4d:91:6e:71:6e:2a:2d:
    c1:a8:21:7d:ae:a6:ab:e0:f1:7c:48:93:34:aa:c7:
    d7:ef:da:12:1c:0f:f2:3a:2a:83:f3:a4:ca:04:48:
    c1:8b:82:47:8e:40:bb:c8:9b:a6:6c:bc:22:6e:46:
    26:b4:52:8a:46:40:6c:d8:d9:0c:59:09:85:94:d1:
    29:3b:ce:57:24:a7:24:06:8c:e1:92:fb:54:d0:ab:
    e4:38:fa:3c:02:ec:e9:31:b4:29:9c:50:77:5b:22:
    75:42:bb:09:15:0f:ec:d5:3f:7e:8b:6c:74:af:bd:
    6f:e7
```

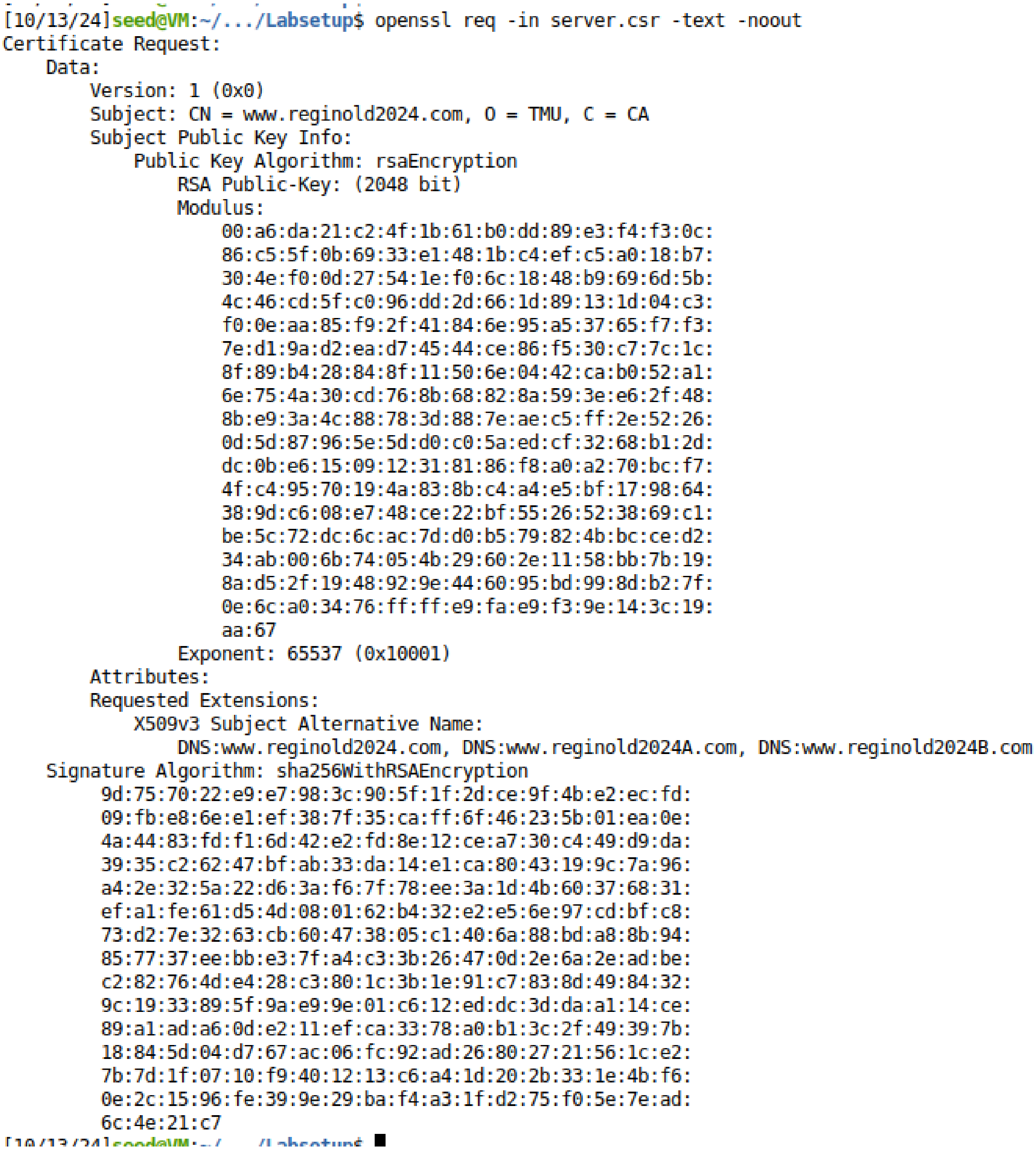
Task 2: Generating a Certificate Request for Your Web Server



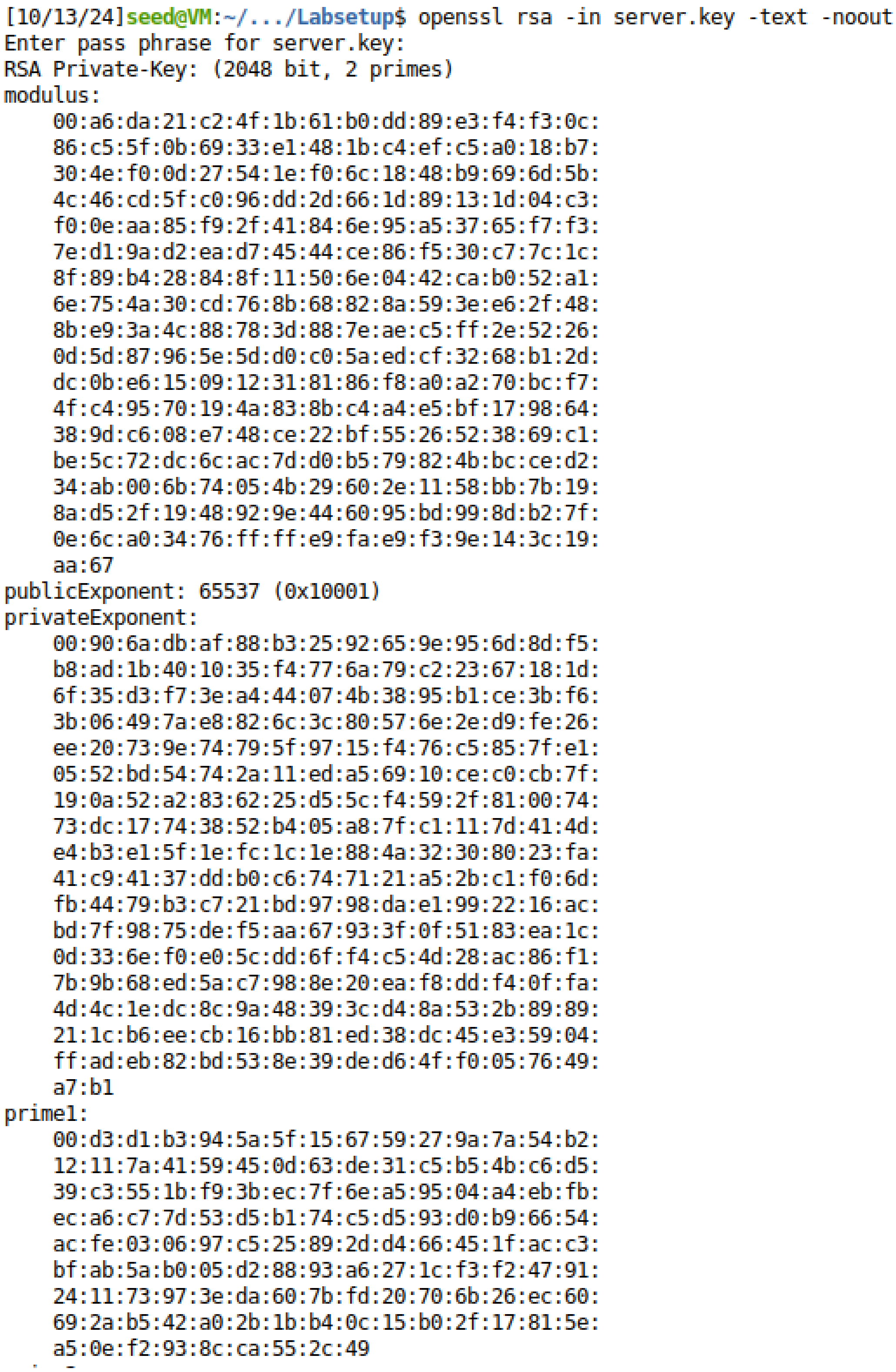
```
  GNU nano 4.8                         hosts
127.0.0.1       localhost
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.9.0.80       c63f68b71168
10.0.0.80       www.reginold2024.com
10.0.0.80       www.reginold2024A.com
10.0.0.80       www.reginold2024B.com
```



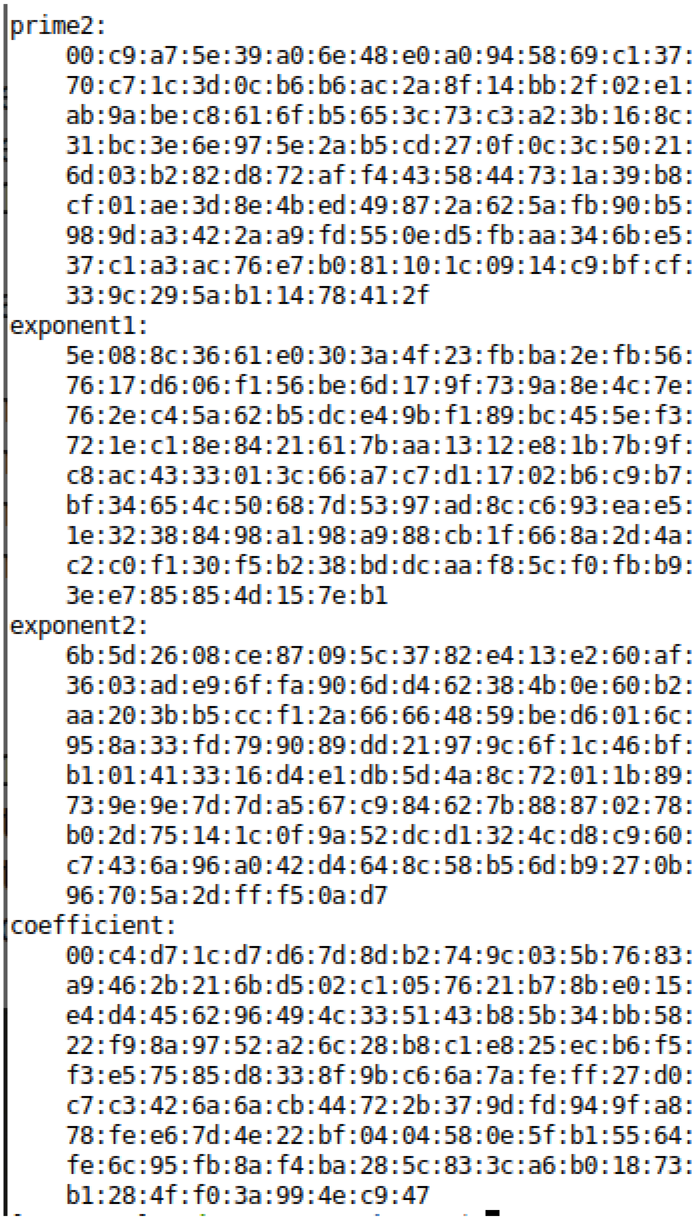
```
[10/13/24]seed@VM:~/.../Labsetup$ openssl req -newkey rsa:2048 -sha256 -keyout server.key -out server.csr -subj "/CN=www.reginold2024.com/O=T
MU/C=CA" -addext "subjectAltName = DNS:www.reginold2024.com, DNS:www.reginold2024A.com, DNS:www.reginold2024B.com" -passout pass:roxie
Generating a RSA private key
.......+++++
.....................................................+++++
writing new private key to 'server.key'
-----
```



```
[10/13/24]seed@VM:~/.../Labsetup$ openssl req -in server.csr -text -noout
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = www.reginold2024.com, O = TMU, C = CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:a6:da:21:c2:4f:1b:61:b0:dd:89:e3:f4:f3:0c:
                    86:c5:5f:0b:69:33:e1:48:1b:c4:ef:c5:a0:18:b7:
                    30:4e:f0:0d:27:54:1e:f0:6c:18:48:b9:69:6d:5b:
                    4c:46:cd:5f:c0:96:dd:2d:66:1d:89:13:1d:04:c3:
                    f0:0e:aa:85:f9:2f:41:84:6e:95:a5:37:65:f7:f3:
                    7e:d1:9a:d2:ea:d7:45:44:ce:86:f5:30:c7:7c:1c:
                    8f:89:b4:28:84:8f:11:50:6e:04:42:ca:b0:52:a1:
                    6e:75:4a:30:cd:76:8b:68:82:8a:59:3e:e6:2f:48:
                    8b:e9:3a:4c:88:78:3d:88:7e:ae:c5:ff:2e:52:26:
                    0d:5d:87:96:5e:5d:d0:c0:5a:ed:cf:32:68:b1:2d:
                    dc:0b:e6:15:09:12:31:81:86:f8:a0:a2:70:bc:f7:
                    4f:c4:95:70:19:4a:83:8b:c4:a4:e5:bf:17:98:64:
                    38:9d:c6:08:e7:48:ce:22:bf:55:26:52:38:69:c1:
                    be:5c:72:dc:6c:ac:7d:d0:b5:79:82:4b:bc:ce:d2:
                    34:ab:00:6b:74:05:4b:29:60:2e:11:58:bb:7b:19:
                    8a:d5:2f:19:48:92:9e:44:60:95:bd:99:8d:b2:7f:
                    0e:6c:a0:34:76:ff:ff:e9:fa:e9:f3:9e:14:3c:19:
                    aa:67
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Subject Alternative Name:
                DNS:www.reginold2024.com, DNS:www.reginold2024A.com, DNS:www.reginold2024B.com
    Signature Algorithm: sha256WithRSAEncryption
         9d:75:70:22:e9:e7:98:3c:90:5f:1f:2d:ce:9f:4b:e2:ec:fd:
         09:fb:e8:6e:e1:ef:38:7f:35:ca:ff:6f:46:23:5b:01:ea:0e:
         4a:44:83:fd:f1:6d:42:e2:fd:8e:12:ce:a7:30:c4:49:d9:da:
         39:35:c2:62:47:bf:ab:33:da:14:e1:ca:80:43:19:9c:7a:96:
         a4:2e:32:5a:22:d6:3a:f6:7f:78:ee:3a:1d:4b:60:37:68:31:
         ef:a1:fe:61:d5:4d:08:01:62:b4:32:e2:e5:6e:97:cd:bf:c8:
         73:d2:7e:32:63:cb:60:47:38:05:c1:40:6a:88:bd:a8:8b:94:
         85:77:37:ee:bb:e3:7f:a4:c3:3b:26:47:0d:2e:6a:2e:ad:be:
         c2:82:76:4d:e4:28:c3:80:1c:3b:1e:91:c7:83:8d:49:84:32:
         9c:19:33:89:5f:9a:e9:9e:01:c6:12:ed:dc:3d:da:a1:14:ce:
         89:a1:ad:a6:0d:e2:11:ef:ca:33:78:a0:b1:3c:2f:49:39:7b:
         18:84:5d:04:d7:67:ac:06:fc:92:ad:26:80:27:21:56:1c:e2:
         7b:7d:1f:07:10:f9:40:12:13:c6:a4:1d:20:2b:33:1e:4b:f6:
         0e:2c:15:96:fe:39:9e:29:ba:f4:a3:1f:d2:75:f0:5e:7e:ad:
         6c:4e:21:c7
[10/13/24]seed@VM:~/.../Labsetup$ █
```

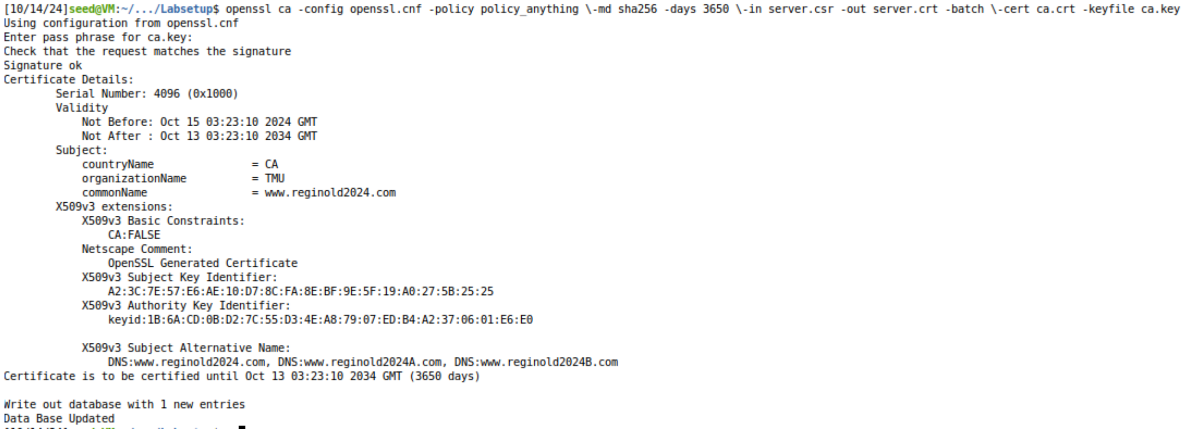


```
[10/13/24]seed@VM:~/.../Labsetup$ openssl rsa -in server.key -text -noout
Enter pass phrase for server.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
    00:a6:da:21:c2:4f:1b:61:b0:dd:89:e3:f4:f3:0c:
    86:c5:5f:0b:69:33:e1:48:1b:c4:ef:c5:a0:18:b7:
    30:4e:f0:0d:27:54:1e:f0:6c:18:48:b9:69:6d:5b:
    4c:46:cd:5f:c0:96:dd:2d:66:1d:89:13:1d:04:c3:
    f0:0e:aa:85:f9:2f:41:84:6e:95:a5:37:65:f7:f3:
    7e:d1:9a:d2:ea:d7:45:44:ce:86:f5:30:c7:7c:1c:
    8f:89:b4:28:84:8f:11:50:6e:04:42:ca:b0:52:a1:
    6e:75:4a:30:cd:76:8b:68:82:8a:59:3e:e6:2f:48:
    8b:e9:3a:4c:88:78:3d:88:7e:ae:c5:ff:2e:52:26:
    0d:5d:87:96:5e:5d:d0:c0:5a:ed:cf:32:68:b1:2d:
    dc:0b:e6:15:09:12:31:81:86:f8:a0:a2:70:bc:f7:
    4f:c4:95:70:19:4a:83:8b:c4:a4:e5:bf:17:98:64:
    38:9d:c6:08:e7:48:ce:22:bf:55:26:52:38:69:c1:
    be:5c:72:dc:6c:ac:7d:d0:b5:79:82:4b:bc:ce:d2:
    34:ab:00:6b:74:05:4b:29:60:2e:11:58:bb:7b:19:
    8a:d5:2f:19:48:92:9e:44:60:95:bd:99:8d:b2:7f:
    0e:6c:a0:34:76:ff:ff:e9:fa:e9:f3:9e:14:3c:19:
    aa:67
publicExponent: 65537 (0x10001)
privateExponent:
    00:90:6a:db:af:88:b3:25:92:65:9e:95:6d:8d:f5:
    b8:ad:1b:40:10:35:f4:77:6a:79:c2:23:67:18:1d:
    6f:35:d3:f7:3e:a4:44:07:4b:38:95:b1:ce:3b:f6:
    3b:06:49:7a:e8:82:6c:3c:80:57:6e:2e:d9:fe:26:
    ee:20:73:9e:74:79:5f:97:15:f4:76:c5:85:7f:e1:
    05:52:bd:54:74:2a:11:ed:a5:69:10:ce:c0:cb:7f:
    19:0a:52:a2:83:62:25:d5:5c:f4:59:2f:81:00:74:
    73:dc:17:74:38:52:b4:05:a8:7f:c1:11:7d:41:4d:
    e4:b3:e1:5f:1e:fc:1c:1e:88:4a:32:30:80:23:fa:
    41:c9:41:37:dd:b0:c6:74:71:21:a5:2b:c1:f0:6d:
    fb:44:79:b3:c7:21:bd:97:98:da:e1:99:22:16:ac:
    bd:7f:98:75:de:f5:aa:67:93:3f:0f:51:83:ea:1c:
    0d:33:6e:f0:e0:5c:dd:6f:f4:c5:4d:28:ac:86:f1:
    7b:9b:68:ed:5a:c7:98:8e:20:ea:f8:dd:f4:0f:fa:
    4d:4c:1e:dc:8c:9a:48:39:3c:d4:8a:53:2b:89:89:
    21:1c:b6:ee:cb:16:bb:81:ed:38:dc:45:e3:59:04:
    ff:ad:eb:82:bd:53:8e:39:de:d6:4f:f0:05:76:49:
    a7:b1
prime1:
    00:d3:d1:b3:94:5a:5f:15:67:59:27:9a:7a:54:b2:
    12:11:7a:41:59:45:0d:63:de:31:c5:b5:4b:c6:d5:
    39:c3:55:1b:f9:3b:ec:7f:6e:a5:95:04:a4:eb:fb:
    ec:a6:c7:7d:53:d5:b1:74:c5:d5:93:d0:b9:66:54:
    ac:fe:03:06:97:c5:25:89:2d:d4:66:45:1f:ac:c3:
    bf:ab:5a:b0:05:d2:88:93:a6:27:1c:f3:f2:47:91:
    24:11:73:97:3e:da:60:7b:fd:20:70:6b:26:ec:60:
    69:2a:b5:42:a0:2b:1b:b4:0c:15:b0:2f:17:81:5e:
    a5:0e:f2:93:8c:ca:55:2c:49
```

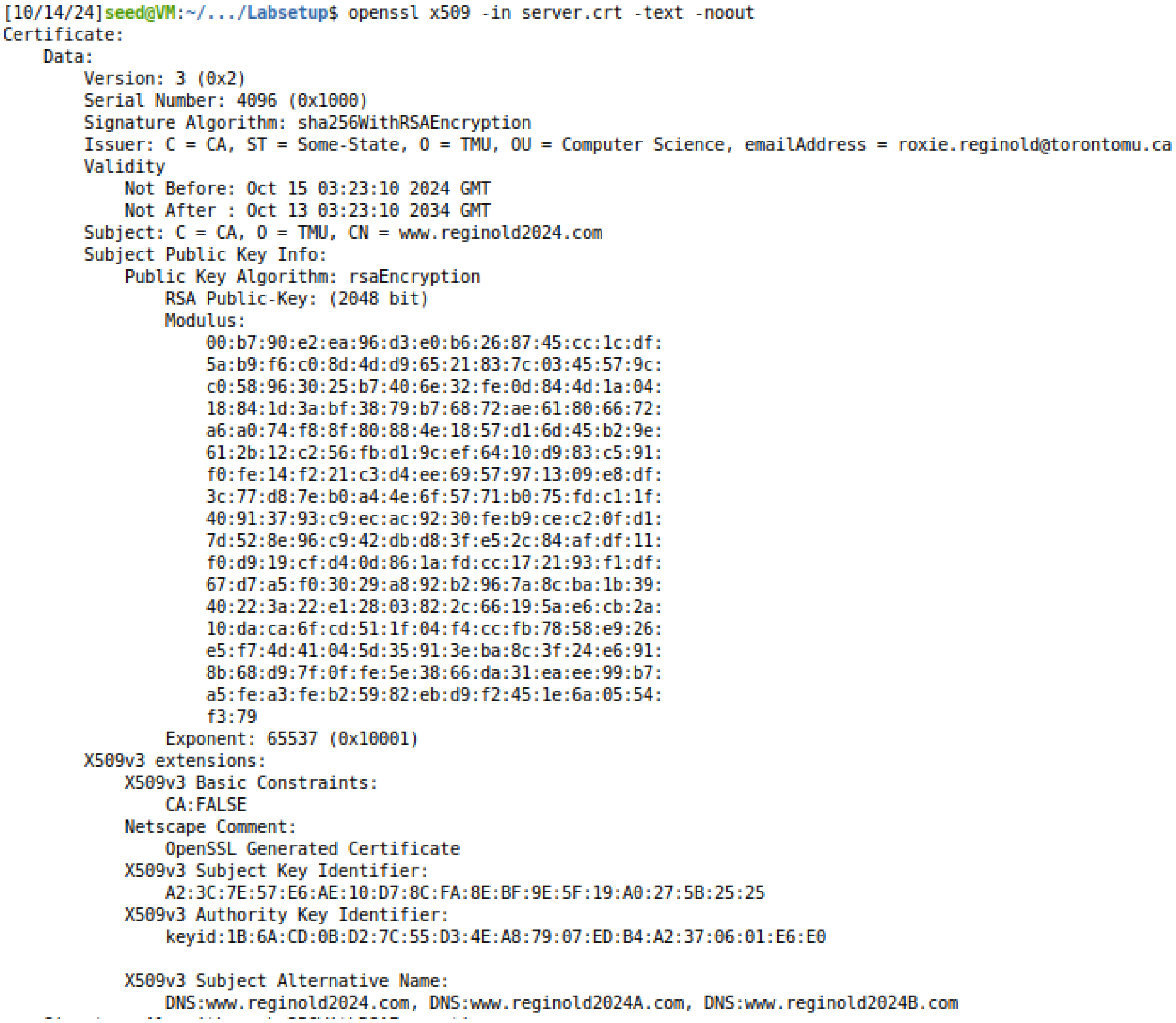


```
prime2:
    00:c9:a7:5e:39:a0:6e:48:e0:a0:94:58:69:c1:37:
    70:c7:1c:3d:0c:b6:b6:ac:2a:8f:14:bb:2f:02:e1:
    ab:9a:be:c8:61:6f:b5:65:3c:73:c3:a2:3b:16:8c:
    31:bc:3e:6e:97:5e:2a:b5:cd:27:0f:0c:3c:50:21:
    6d:03:b2:82:d8:72:af:f4:43:58:44:73:1a:39:b8:
    cf:01:ae:3d:8e:4b:ed:49:87:2a:62:5a:fb:90:b5:
    98:9d:a3:42:2a:a9:fd:55:0e:d5:fb:aa:34:6b:e5:
    37:c1:a3:ac:76:e7:b0:81:10:1c:09:14:c9:bf:cf:
    33:9c:29:5a:b1:14:78:41:2f
exponent1:
    5e:08:8c:36:61:e0:30:3a:4f:23:fb:ba:2e:fb:56:
    76:17:d6:06:f1:56:be:6d:17:9f:73:9a:8e:4c:7e:
    76:2e:c4:5a:62:b5:dc:e4:9b:f1:89:bc:45:5e:f3:
    72:1e:c1:8e:84:21:61:7b:aa:13:12:e8:1b:7b:9f:
    c8:ac:43:33:01:3c:66:a7:c7:d1:17:02:b6:c9:b7:
    bf:34:65:4c:50:68:7d:53:97:ad:8c:c6:93:ea:e5:
    1e:32:38:84:98:a1:98:a9:88:cb:1f:66:8a:2d:4a:
    c2:c0:f1:30:f5:b2:38:bd:dc:aa:f8:5c:f0:fb:b9:
    3e:e7:85:85:4d:15:7e:b1
exponent2:
    6b:5d:26:08:ce:87:09:5c:37:82:e4:13:e2:60:af:
    36:03:ad:e9:6f:fa:90:6d:d4:62:38:4b:0e:60:b2:
    aa:20:3b:b5:cc:f1:2a:66:66:48:59:be:d6:01:6c:
    95:8a:33:fd:79:90:89:dd:21:97:9c:6f:1c:46:bf:
    b1:01:41:33:16:d4:e1:db:5d:4a:8c:72:01:1b:89:
    73:9e:9e:7d:7d:a5:67:c9:84:62:7b:88:87:02:78:
    b0:2d:75:14:1c:0f:9a:52:dc:d1:32:4c:d8:c9:60:
    c7:43:6a:96:a0:42:d4:64:8c:58:b5:6d:b9:27:0b:
    96:70:5a:2d:ff:f5:0a:d7
coefficient:
    00:c4:d7:1c:d7:d6:7d:8d:b2:74:9c:03:5b:76:83:
    a9:46:2b:21:6b:d5:02:c1:05:76:21:b7:8b:e0:15:
    e4:d4:45:62:96:49:4c:33:51:43:b8:5b:34:bb:58:
    22:f9:8a:97:52:a2:6c:28:b8:c1:e8:25:ec:b6:f5:
    f3:e5:75:85:d8:33:8f:9b:c6:6a:7a:fe:ff:27:d0:
    c7:c3:42:6a:6a:cb:44:72:2b:37:9d:fd:94:9f:a8:
    78:fe:e6:7d:4e:22:bf:04:04:58:0e:5f:b1:55:64:
    fe:6c:95:fb:8a:f4:ba:28:5c:83:3c:a6:b0:18:73:
    b1:28:4f:f0:3a:99:4e:c9:47
```

Task 3: Generating a Certificate for your server



```
[10/14/24]seed@VM:~/.../Labsetup$ openssl ca -config openssl.cnf -policy policy_anything \-md sha256 -days 3650 \-in server.csr -out server.crt -batch \-cert ca.crt -keyfile ca.key
Using configuration from openssl.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: Oct 15 03:23:10 2024 GMT
            Not After : Oct 13 03:23:10 2034 GMT
        Subject:
            countryName               = CA
            organizationName          = TMU
            commonName                = www.reginold2024.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                A2:3C:7E:57:E6:AE:10:D7:8C:FA:8E:BF:9E:5F:19:A0:27:5B:25:25
            X509v3 Authority Key Identifier:
                keyid:1B:6A:CD:0B:D2:7C:55:D3:4E:A8:79:07:ED:B4:A2:37:06:01:E6:E0

            X509v3 Subject Alternative Name:
                DNS:www.reginold2024.com, DNS:www.reginold2024A.com, DNS:www.reginold2024B.com
Certificate is to be certified until Oct 13 03:23:10 2034 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
```

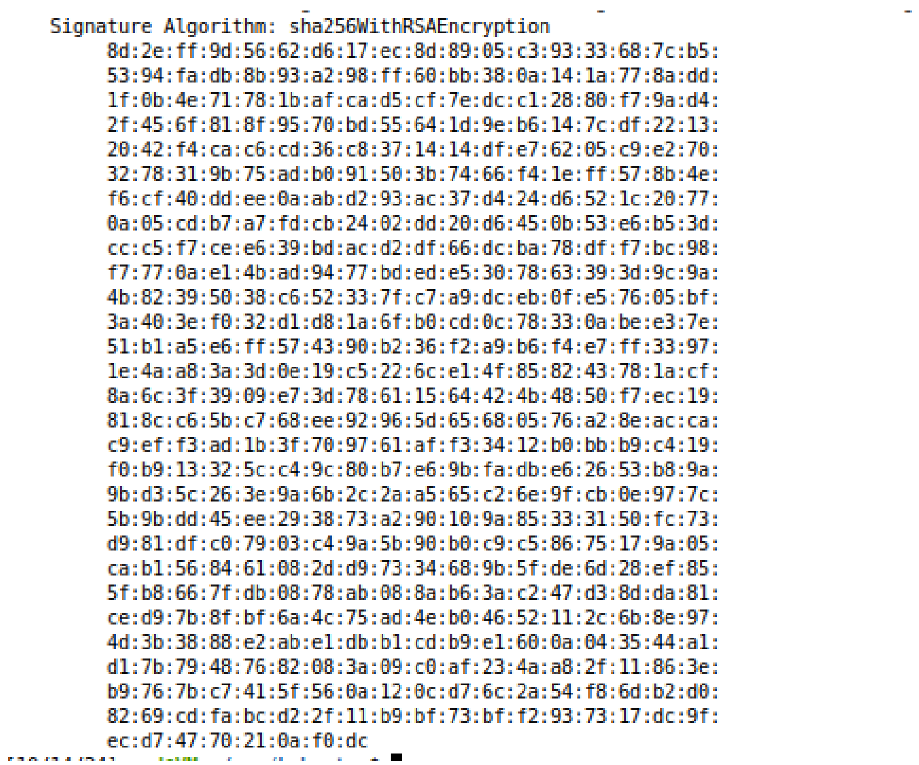


```
[10/14/24]seed@VM:~/.../Labsetup$ openssl x509 -in server.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = CA, ST = Some-State, O = TMU, OU = Computer Science, emailAddress = roxie.reginold@torontomu.ca
        Validity
            Not Before: Oct 15 03:23:10 2024 GMT
            Not After : Oct 13 03:23:10 2034 GMT
        Subject: C = CA, O = TMU, CN = www.reginold2024.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:b7:90:e2:ea:96:d3:e0:b6:26:87:45:cc:1c:df:
                    5a:b9:f6:c0:8d:4d:d9:65:21:83:7c:03:45:57:9c:
                    c0:58:96:30:25:b7:40:6e:32:fe:0d:84:4d:1a:04:
                    18:84:1d:3a:bf:38:79:b7:68:72:ae:61:80:66:72:
                    a6:a0:74:f8:8f:80:88:4e:18:57:d1:6d:45:b2:9e:
                    61:2b:12:c2:56:fb:d1:9c:ef:64:10:d9:83:c5:91:
                    f0:fe:14:f2:21:c3:d4:ee:69:57:97:13:09:e8:df:
                    3c:77:d8:7e:b0:a4:4e:6f:57:71:b0:75:fd:c1:1f:
                    40:91:37:93:c9:ec:ac:92:30:fe:b9:ce:c2:0f:d1:
                    7d:52:8e:96:c9:42:db:d8:3f:e5:2c:84:af:df:11:
                    f0:d9:19:cf:d4:0d:86:1a:fd:cc:17:21:93:f1:df:
                    67:d7:a5:f0:30:29:a8:92:b2:96:7a:8c:ba:1b:39:
                    40:22:3a:22:e1:28:03:82:2c:66:19:5a:e6:cb:2a:
                    10:da:ca:6f:cd:51:1f:04:f4:cc:fb:78:58:e9:26:
                    e5:f7:4d:41:04:5d:35:91:3e:ba:8c:3f:24:e6:91:
                    8b:68:d9:7f:0f:fe:5e:38:66:da:31:ea:ee:99:b7:
                    a5:fe:a3:fe:b2:59:82:eb:d9:f2:45:1e:6a:05:54:
                    f3:79
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                A2:3C:7E:57:E6:AE:10:D7:8C:FA:8E:BF:9E:5F:19:A0:27:5B:25:25
            X509v3 Authority Key Identifier:
                keyid:1B:6A:CD:0B:D2:7C:55:D3:4E:A8:79:07:ED:B4:A2:37:06:01:E6:E0

            X509v3 Subject Alternative Name:
                DNS:www.reginold2024.com, DNS:www.reginold2024A.com, DNS:www.reginold2024B.com
```

Alternative names are included as shown above:

X509v3 Subject Alternative Name:

DNS:www.reginold2024.com, DNS:www.reginold2024A.com, DNS:www.reginold2024B.com



```
    Signature Algorithm: sha256WithRSAEncryption
         8d:2e:ff:9d:56:62:d6:17:ec:8d:89:05:c3:93:33:68:7c:b5:
         53:94:fa:db:8b:93:a2:98:ff:60:bb:38:0a:14:1a:77:8a:dd:
         1f:0b:4e:71:78:1b:af:ca:d5:cf:7e:dc:c1:28:80:f7:9a:d4:
         2f:45:6f:81:8f:95:70:bd:55:64:1d:9e:b6:14:7c:df:22:13:
         20:42:f4:ca:c6:cd:36:c8:37:14:14:df:e7:62:05:c9:e2:70:
         32:78:31:9b:75:ad:b0:91:50:3b:74:66:f4:1e:ff:57:8b:4e:
         f6:cf:40:dd:ee:0a:ab:d2:93:ac:37:d4:24:d6:52:1c:20:77:
         0a:05:cd:b7:a7:fd:cb:24:02:dd:20:d6:45:0b:53:e6:b5:3d:
         cc:c5:f7:ce:e6:39:bd:ac:d2:df:66:dc:ba:78:df:f7:bc:98:
         f7:77:0a:e1:4b:ad:94:77:bd:ed:e5:30:78:63:39:3d:9c:9a:
         4b:82:39:50:38:c6:52:33:7f:c7:a9:dc:eb:0f:e5:76:05:bf:
         3a:40:3e:f0:32:d1:d8:1a:6f:b0:cd:0c:78:33:0a:be:e3:7e:
         51:b1:a5:e6:ff:57:43:90:b2:36:f2:a9:b6:f4:e7:ff:33:97:
         1e:4a:a8:3a:3d:0e:19:c5:22:6c:e1:4f:85:82:43:78:1a:cf:
         8a:6c:3f:39:09:e7:3d:78:61:15:64:42:4b:48:50:f7:ec:19:
         81:8c:c6:5b:c7:68:ee:92:96:5d:65:68:05:76:a2:8e:ac:ca:
         c9:ef:f3:ad:1b:3f:70:97:61:af:f3:34:12:b0:bb:b9:c4:19:
         f0:b9:13:32:5c:c4:9c:80:b7:e6:9b:fa:db:e6:26:53:b8:9a:
         9b:d3:5c:26:3e:9a:6b:2c:2a:a5:65:c2:6e:9f:cb:0e:97:7c:
         5b:9b:dd:45:ee:29:38:73:a2:90:10:9a:85:33:31:50:fc:73:
         d9:81:df:c0:79:03:c4:9a:5b:90:b0:c9:c5:86:75:17:9a:05:
         ca:b1:56:84:61:08:2d:d9:73:34:68:9b:5f:de:6d:28:ef:85:
         5f:b8:66:7f:db:08:78:ab:08:8a:b6:3a:c2:47:d3:8d:da:81:
         ce:d9:7b:8f:bf:6a:4c:75:ad:4e:b0:46:52:11:2c:6b:8e:97:
         4d:3b:38:88:e2:ab:e1:db:b1:cd:b9:e1:60:0a:04:35:44:a1:
         d1:7b:79:48:76:82:08:3a:09:c0:af:23:4a:a8:2f:11:86:3e:
         b9:76:7b:c7:41:5f:56:0a:12:0c:d7:6c:2a:54:f8:6d:b2:d0:
         82:69:cd:fa:bc:d2:2f:11:b9:bf:73:bf:f2:93:73:17:dc:9f:
         ec:d7:47:70:21:0a:f0:dc
```

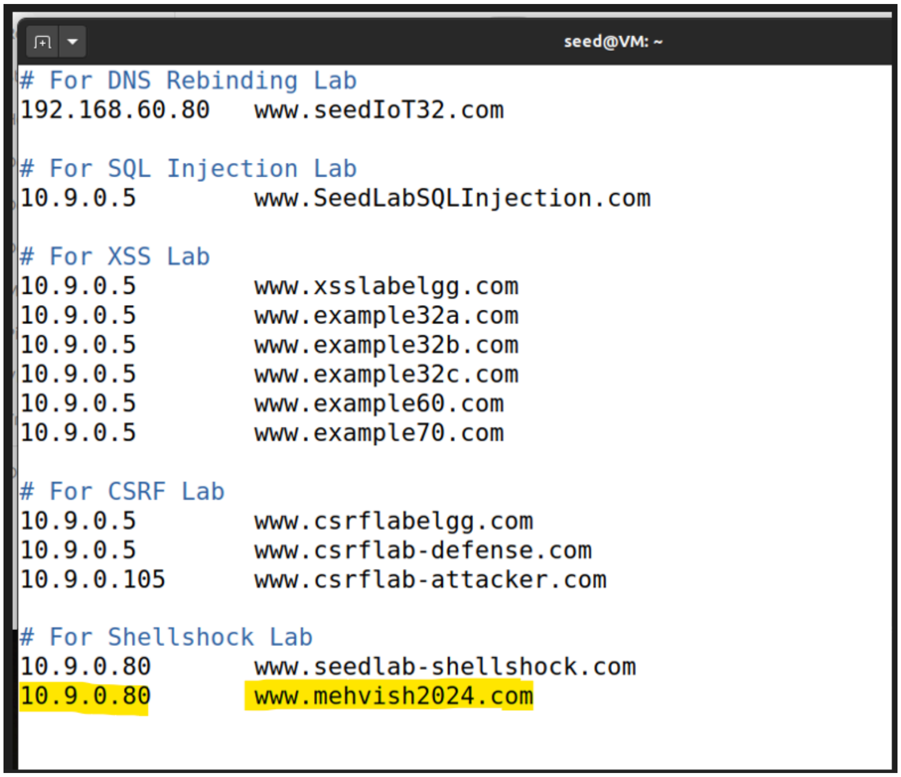
Task 4: Deploying Certificate in an Apache-Based HTTPS Website

Initial Setup:

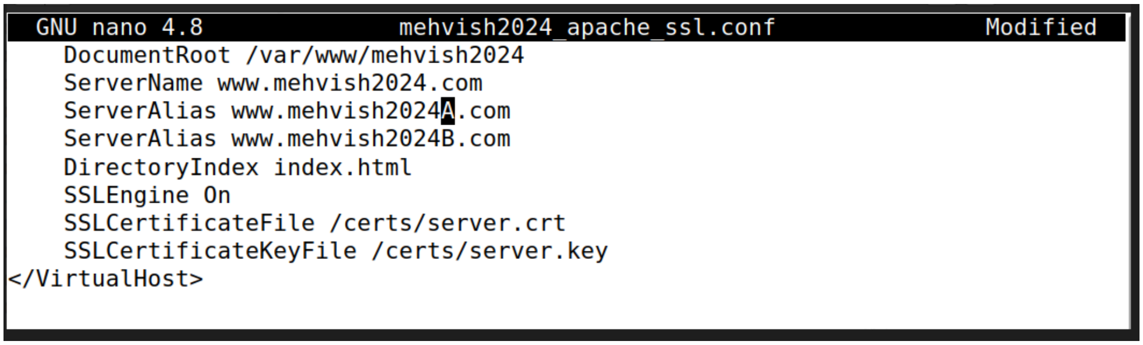
• Modified /etc/hosts file to add the custom website name
• Created a new apache_ssl.conf (A new VirtualHost configuration file) file based on the bank32 example in /etc/apache2/sites-available/
• Updated ServerName, ServerAlias, SSLCertificateFile, and SSLCertificateKeyFile in the conf file

File Transfer:

• Used the shared volume to transfer necessary files between VM and container.
• Copied the certificate and private key files to the /certs directory in the container



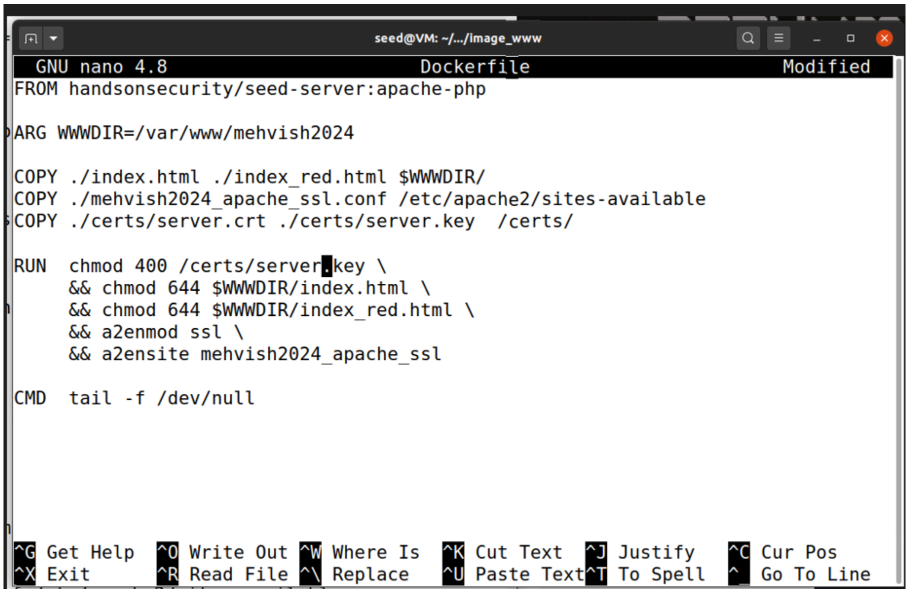
```
# For DNS Rebinding Lab
192.168.60.80   www.seedIoT32.com

# For SQL Injection Lab
10.9.0.5        www.SeedLabSQLInjection.com

# For XSS Lab
10.9.0.5        www.xsslabelgg.com
10.9.0.5        www.example32a.com
10.9.0.5        www.example32b.com
10.9.0.5        www.example32c.com
10.9.0.5        www.example60.com
10.9.0.5        www.example70.com

# For CSRF Lab
10.9.0.5        www.csrflabelgg.com
10.9.0.5        www.csrflab-defense.com
10.9.0.105      www.csrflab-attacker.com

# For Shellshock Lab
10.9.0.80       www.seedlab-shellshock.com
10.9.0.80       www.mehvish2024.com
```



```
  GNU nano 4.8                mehvish2024_apache_ssl.conf                Modified
    DocumentRoot /var/www/mehvish2024
    ServerName www.mehvish2024.com
    ServerAlias www.mehvish2024A.com
    ServerAlias www.mehvish2024B.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/server.crt
    SSLCertificateKeyFile /certs/server.key
</VirtualHost>
```

Dockerfile Configuration:

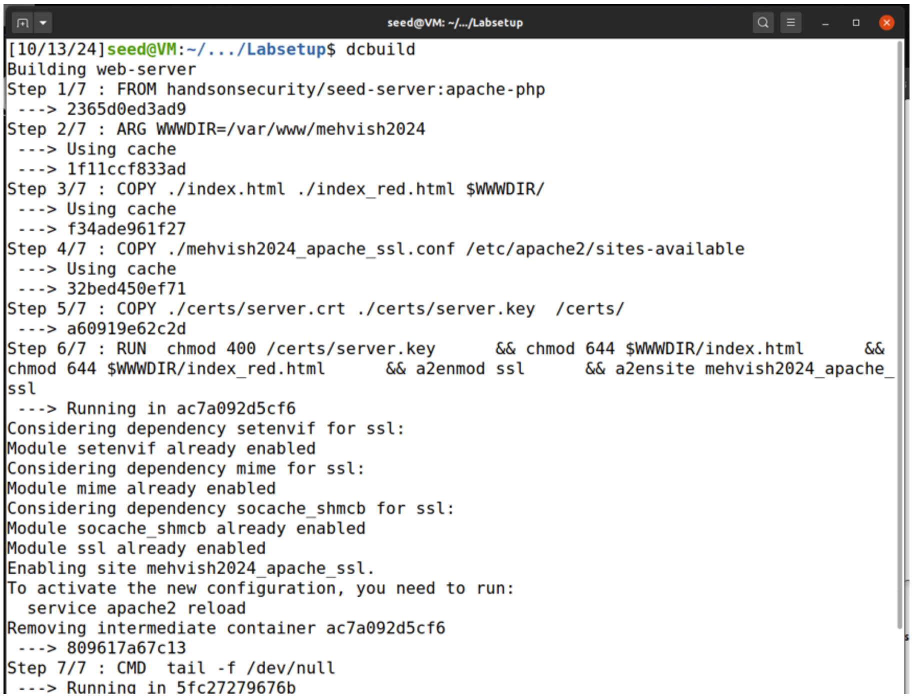
- Added commands to enable SSL module (a2enmod ssl)
- Added command to enable the custom Apache site (a2ensite [mehvish20204_apache_ssl])



```
  GNU nano 4.8                    Dockerfile                    Modified
FROM handsonsecurity/seed-server:apache-php

ARG WWWDIR=/var/www/mehvish2024

COPY ./index.html ./index_red.html $WWWDIR/
COPY ./mehvish2024_apache_ssl.conf /etc/apache2/sites-available
COPY ./certs/server.crt ./certs/server.key  /certs/

RUN  chmod 400 /certs/server.key \
     && chmod 644 $WWWDIR/index.html \
     && chmod 644 $WWWDIR/index_red.html \
     && a2enmod ssl \
     && a2ensite mehvish2024_apache_ssl

CMD  tail -f /dev/null
```

Building and Running the Container:

- Ran docker-compose build (dcbuild)
- Ran docker-compose up (dcup)



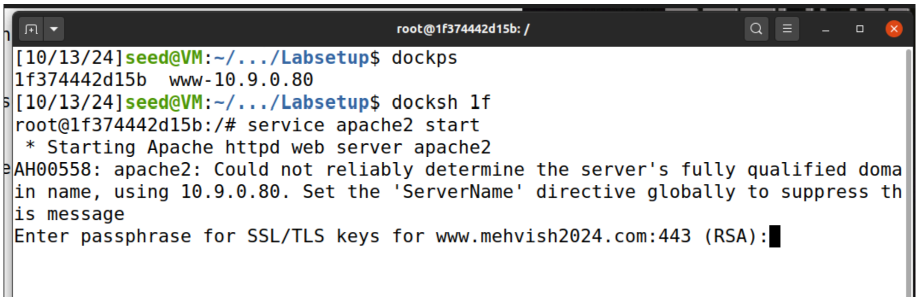
```
[10/13/24]seed@VM:~/.../Labsetup$ dcbuild
Building web-server
Step 1/7 : FROM handsonsecurity/seed-server:apache-php
 ---> 2365d0ed3ad9
Step 2/7 : ARG WWWDIR=/var/www/mehvish2024
 ---> Using cache
 ---> 1f11ccf833ad
Step 3/7 : COPY ./index.html ./index_red.html $WWWDIR/
 ---> Using cache
 ---> f34ade961f27
Step 4/7 : COPY ./mehvish2024_apache_ssl.conf /etc/apache2/sites-available
 ---> Using cache
 ---> 32bed450ef71
Step 5/7 : COPY ./certs/server.crt ./certs/server.key  /certs/
 ---> a60919e62c2d
Step 6/7 : RUN  chmod 400 /certs/server.key      && chmod 644 $WWWDIR/index.html      &&
chmod 644 $WWWDIR/index_red.html      && a2enmod ssl      && a2ensite mehvish2024_apache_
ssl
 ---> Running in ac7a092d5cf6
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
Enabling site mehvish2024_apache_ssl.
To activate the new configuration, you need to run:
  service apache2 reload
Removing intermediate container ac7a092d5cf6
 ---> 809617a67c13
Step 7/7 : CMD  tail -f /dev/null
 ---> Running in 5fc27279676b
```

Accessing the Container:

- Opened a new terminal
- Used dockps to list running containers
- Used docksh to access the container shell

Starting Apache Server:

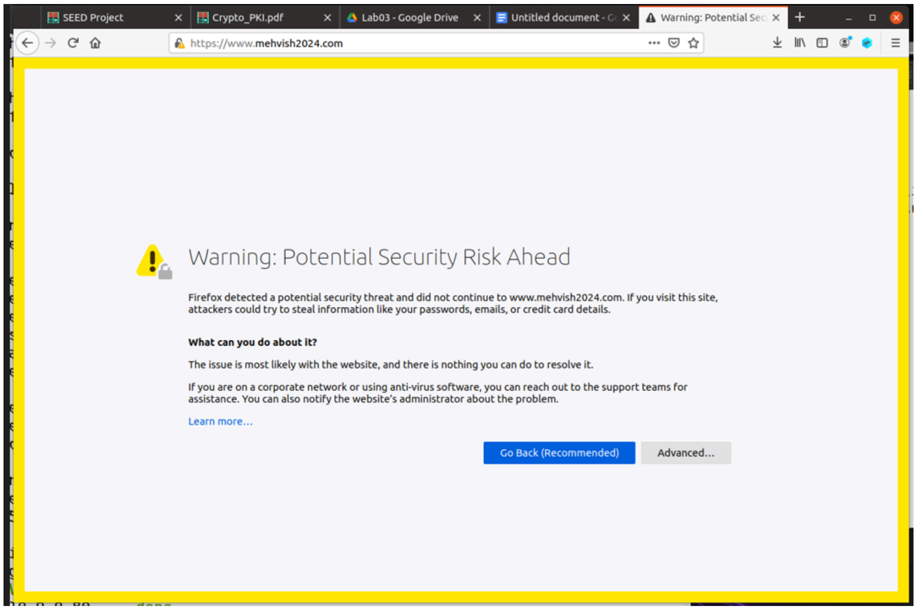
- Started the Apache server (using 'service apache2 start')
- Prompted to enter SSL/TLS key password for the website



```
[10/13/24]seed@VM:~/.../Labsetup$ dockps
1f374442d15b  www-10.9.0.80
[10/13/24]seed@VM:~/.../Labsetup$ docksh 1f
root@1f374442d15b:/# service apache2 start
 * Starting Apache httpd web server apache2
AH00558: apache2: Could not reliably determine the server's fully qualified doma
in name, using 10.9.0.80. Set the 'ServerName' directive globally to suppress th
is message
Enter passphrase for SSL/TLS keys for www.mehvish2024.com:443 (RSA):
```

Initial Browser Test:

- Opened Firefox and typed the custom website name
- Encountered a security warning due to an untrusted certificate



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to www.mehvish2024.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

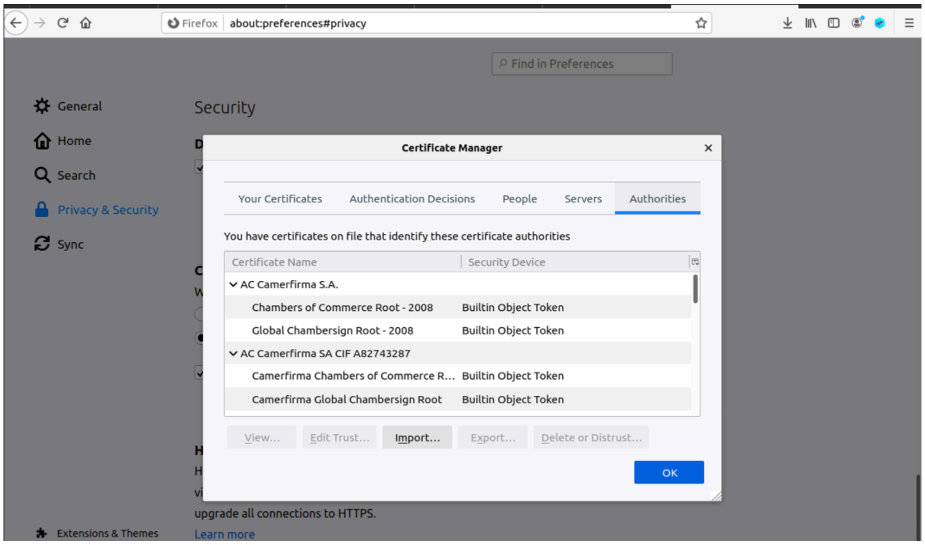
If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Browsing the website. Now, point the browser to your web server (note: you should put https at the beginning of your URL, instead of using http). Please describe and explain your observations. Most likely, you will not be able to succeed, this is because ... (the reasons are omitted here; students should provide the explanation in their lab reports). Please fix the problem and demonstrate that you can successfully visit the HTTPS website

This occurs because the browser does not trust the self-signed certificate used by your web server. Self-signed certificates are not issued by a recognized Certificate Authority (CA), which browsers rely on to verify the authenticity of websites. To protect against potential man-in-the-middle attacks, browsers are designed to warn users about connections using untrusted certificates. To resolve this issue and successfully visit the HTTPS website, we must manually add the self-signed certificate to our browser's trust store. After completing this process and refreshing the page, we can access the HTTPS website without warnings, demonstrating a successful secure connection.

Certificate Trust Setup:

- Navigated to Firefox settings (about:preferences#privacy)
- Located and clicked "View Certificates"
- In the Authorities tab, imported the custom certificate
- Selected "Trust this CA to identify websites"

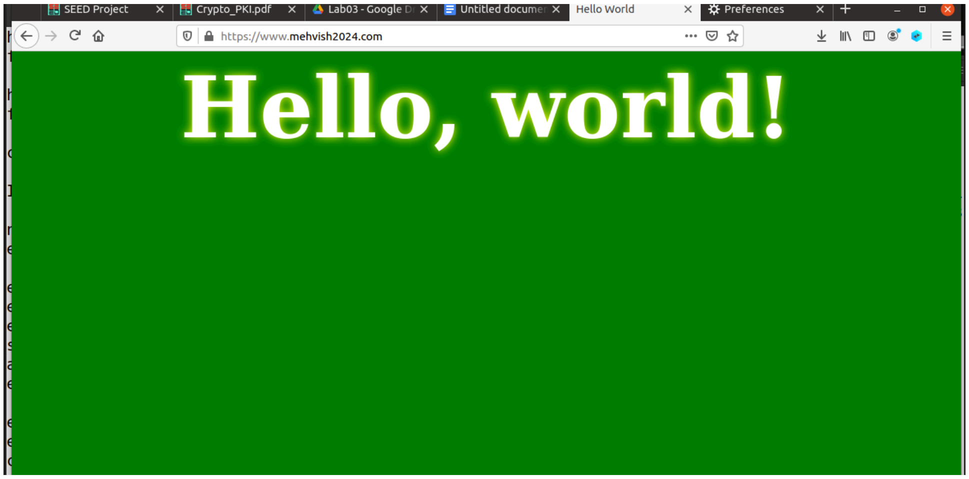


You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce R…	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token

Successful HTTPS Connection:

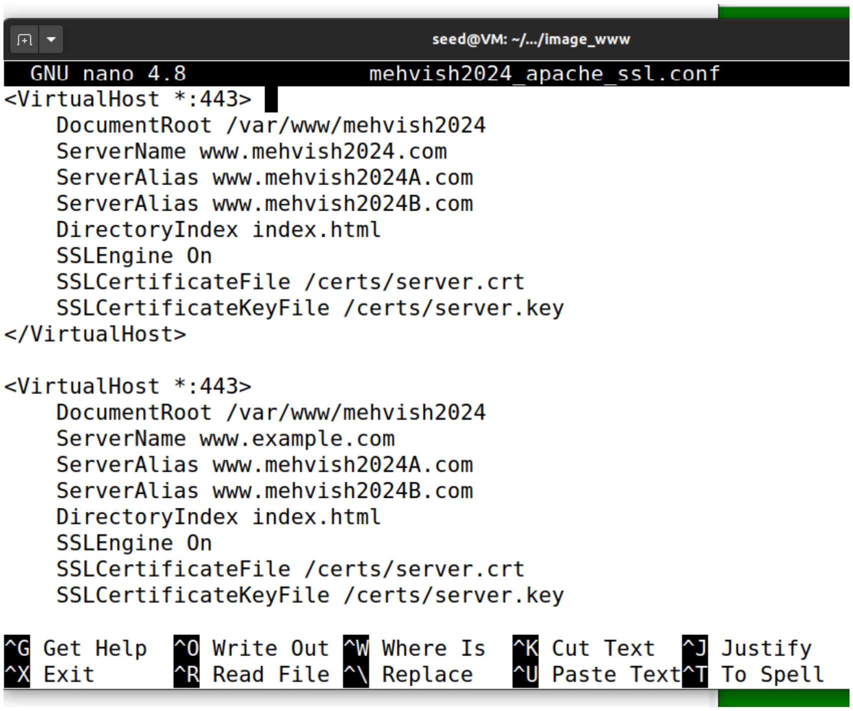
- Refreshed the browser
- Successfully loaded the website, displaying "Hello World"



Task 5: Launching a Man-In-The-Middle Attack

Setting up the malicious website:

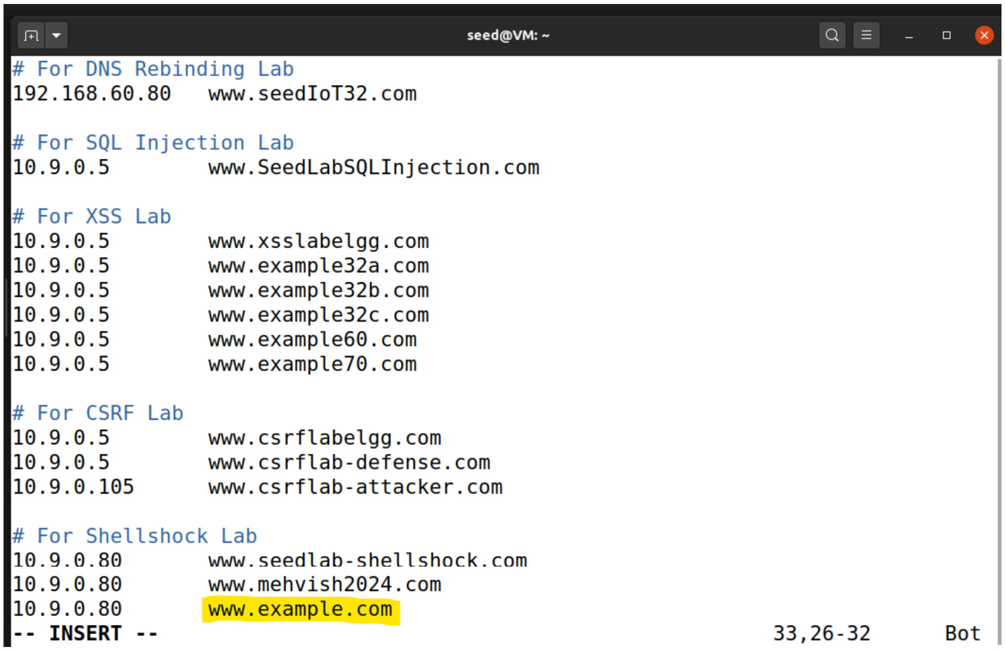
- Reused the VirtualHost configuration from the previous Apache SSL setup
- Modified the ServerName in apache_ssl.conf to redirect to www.example.com
- Kept the same SSL certificate used from the previous task



```
  GNU nano 4.8                  mehvish2024_apache_ssl.conf
<VirtualHost *:443>
    DocumentRoot /var/www/mehvish2024
    ServerName www.mehvish2024.com
    ServerAlias www.mehvish2024A.com
    ServerAlias www.mehvish2024B.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/server.crt
    SSLCertificateKeyFile /certs/server.key
</VirtualHost>

<VirtualHost *:443>
    DocumentRoot /var/www/mehvish2024
    ServerName www.example.com
    ServerAlias www.mehvish2024A.com
    ServerAlias www.mehvish2024B.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/server.crt
    SSLCertificateKeyFile /certs/server.key

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify
^X Exit      ^R Read File ^\ Replace   ^U Paste Text^T To Spell
```

Implementing the "man in the middle" part:

- Modified the /etc/hosts file to map example.com to the IP address of the malicious server
- This step simulates a DNS cache poisoning attack



```
# For DNS Rebinding Lab
192.168.60.80   www.seedIoT32.com

# For SQL Injection Lab
10.9.0.5        www.SeedLabSQLInjection.com

# For XSS Lab
10.9.0.5        www.xsslabelgg.com
10.9.0.5        www.example32a.com
10.9.0.5        www.example32b.com
10.9.0.5        www.example32c.com
10.9.0.5        www.example60.com
10.9.0.5        www.example70.com

# For CSRF Lab
10.9.0.5        www.csrflabelgg.com
10.9.0.5        www.csrflab-defense.com
10.9.0.105      www.csrflab-attacker.com

# For Shellshock Lab
10.9.0.80       www.seedlab-shellshock.com
10.9.0.80       www.mehvish2024.com
10.9.0.80       www.example.com
-- INSERT --                                                33,26-32      Bot
```

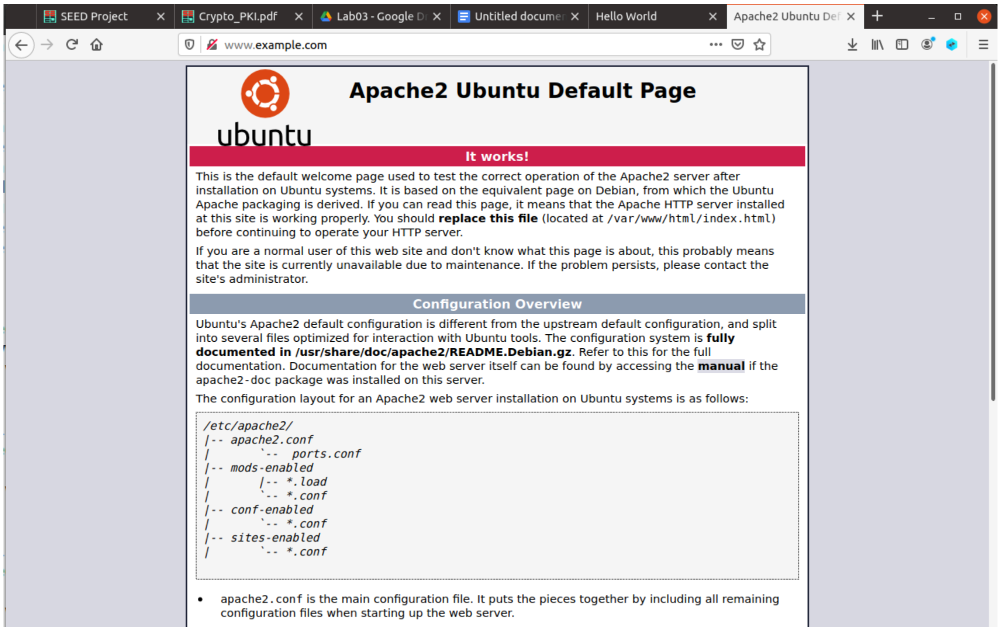
Configuring and starting the Apache server:

- Enabled the new VirtualHost configuration
- Started/restarted the Apache server

Browsing the target website:

- Attempted to access example.com and www.example.com

- Observed that the connection was not secure



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

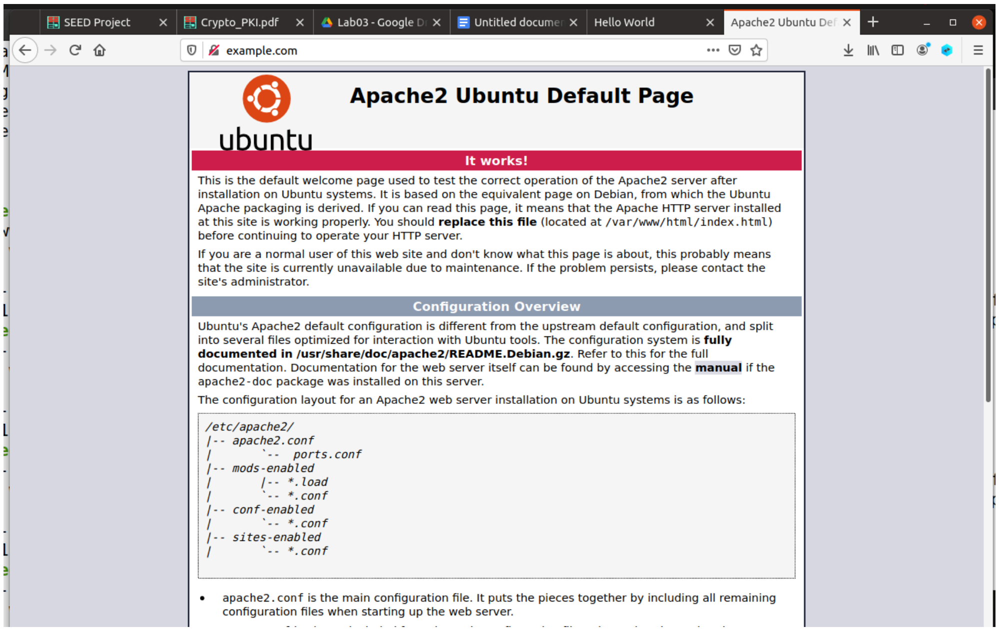
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

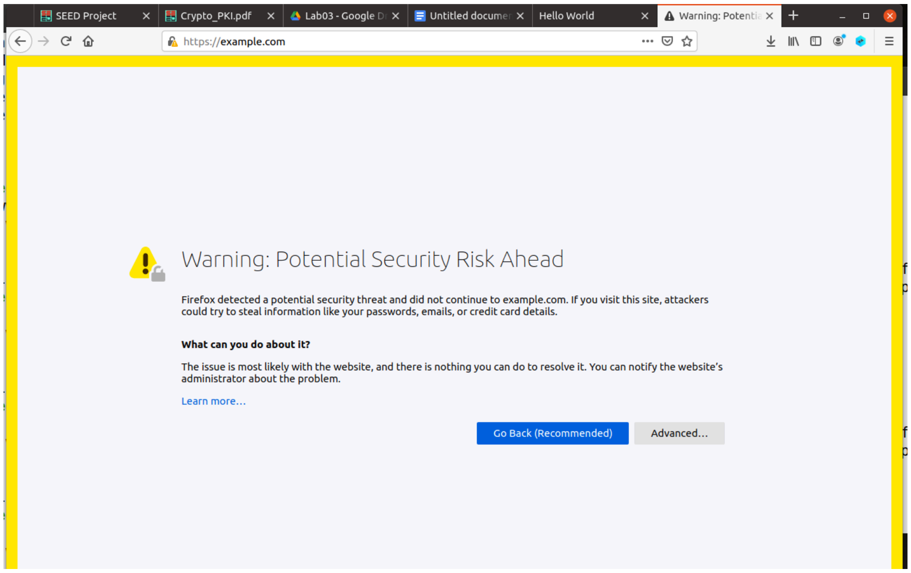
```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

Attempting a secure connection:

- Tried accessing https://example.com

- Observed that the connection was still not secure



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to example.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it. You can notify the website's administrator about the problem.

Learn more…

Observations:

Based on our observations from this task, we can conclude that while we successfully redirected traffic intended for example.com to our malicious server, we were unable to fully execute a seamless Man-in-the-Middle (MITM) attack. This is due to the robust security measures implemented by modern web browsers and the HTTPS protocol.

When users attempted to access the non-secure version (http://example.com), they were indeed directed to our malicious page. However, the browser indicated that the connection was not secure, alerting users to potential risks. This is because HTTP does not provide any encryption or authentication.

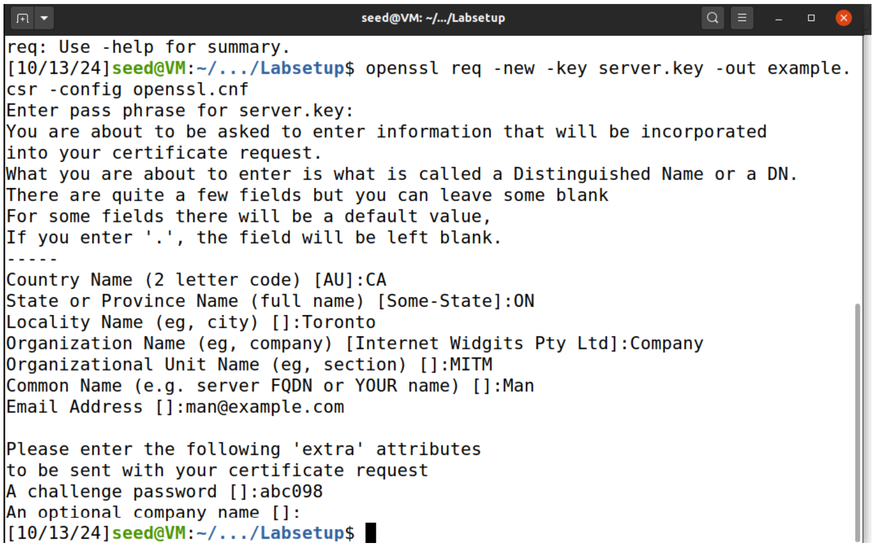
More importantly, when users tried to access the secure version (https://example.com), the browser displayed a prominent security warning. This occurred because our malicious server could not present a valid SSL/TLS certificate for example.com. The certificate we used, being self-signed and not issued by a trusted Certificate Authority, did not match the domain name the user was trying to access.

This demonstration highlights the effectiveness of the Public Key Infrastructure (PKI) and HTTPS in preventing MITM attacks. While we could intercept and redirect the traffic, we could not convincingly impersonate a legitimate website without triggering security warnings. In conclusion, our attempt at a MITM attack was unsuccessful in bypassing modern browser security measures.

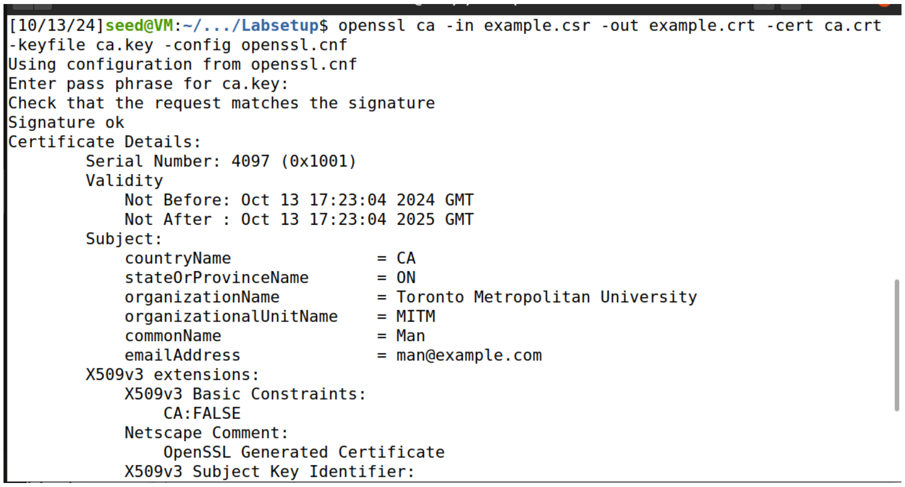
Task 6: Launching a Man-In-The-Middle Attack with a Compromised CA

Initial Steps:

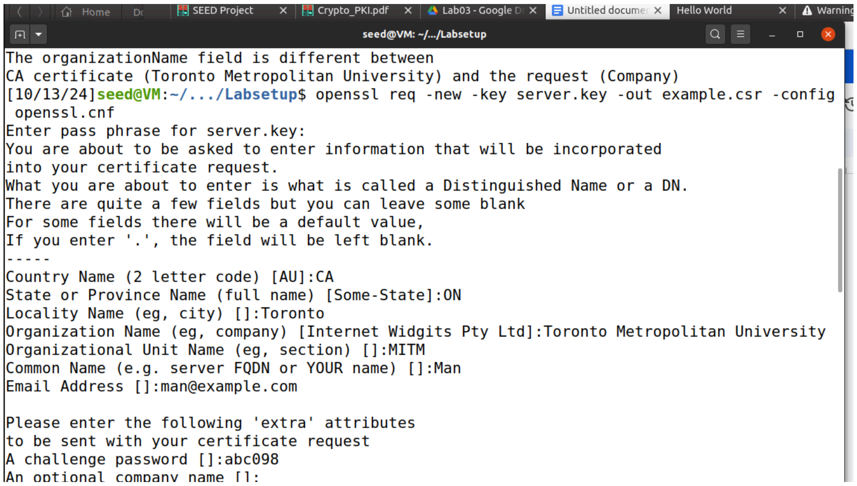
- Created a new example.csr (Certificate Signing Request) using the existing server.key
- Generated a new example.crt (certificate) signed by the compromised CA



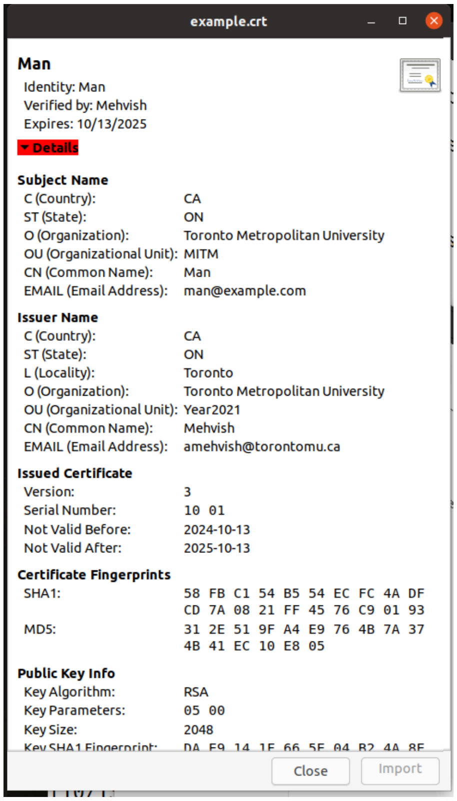
```
req: Use -help for summary.
[10/13/24]seed@VM:~/.../Labsetup$ openssl req -new -key server.key -out example.
csr -config openssl.cnf
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter 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]:CA
State or Province Name (full name) [Some-State]:ON
Locality Name (eg, city) []:Toronto
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Company
Organizational Unit Name (eg, section) []:MITM
Common Name (e.g. server FQDN or YOUR name) []:Man
Email Address []:man@example.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:abc098
An optional company name []:
[10/13/24]seed@VM:~/.../Labsetup$ 
```



```
[10/13/24]seed@VM:~/.../Labsetup$ openssl ca -in example.csr -out example.crt -cert ca.crt
-keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4097 (0x1001)
        Validity
            Not Before: Oct 13 17:23:04 2024 GMT
            Not After : Oct 13 17:23:04 2025 GMT
        Subject:
            countryName               = CA
            stateOrProvinceName       = ON
            organizationName          = Toronto Metropolitan University
            organizationalUnitName    = MITM
            commonName                = Man
            emailAddress              = man@example.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
```



```
The organizationName field is different between
CA certificate (Toronto Metropolitan University) and the request (Company)
[10/13/24]seed@VM:~/.../Labsetup$ openssl req -new -key server.key -out example.csr -config
 openssl.cnf
Enter pass phrase for server.key:
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]:CA
State or Province Name (full name) [Some-State]:ON
Locality Name (eg, city) []:Toronto
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Toronto Metropolitan University
Organizational Unit Name (eg, section) []:MITM
Common Name (e.g. server FQDN or YOUR name) []:Man
Email Address []:man@example.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:abc098
An optional company name []:
```



Man

Identity: Man
Verified by: Mehvish
Expires: 10/13/2025

Subject Name

```
C (Country):                  CA
ST (State):                   ON
O (Organization):             Toronto Metropolitan University
OU (Organizational Unit):     MITM
CN (Common Name):             Man
EMAIL (Email Address):        man@example.com
```

Issuer Name

```
C (Country):                  CA
ST (State):                   ON
L (Locality):                 Toronto
O (Organization):             Toronto Metropolitan University
OU (Organizational Unit):     Year2021
CN (Common Name):             Mehvish
EMAIL (Email Address):        amehvish@torontomu.ca
```

Issued Certificate

```
Version:                      3
Serial Number:                10 01
Not Valid Before:             2024-10-13
Not Valid After:              2025-10-13
```

Certificate Fingerprints

```
SHA1:                         58 FB C1 54 B5 54 EC FC 4A DF
                              CD 7A 08 21 FF 45 76 C9 01 93
MD5:                          31 2E 51 9F A4 E9 76 4B 7A 37
                              4B 41 EC 10 E8 05
```

Public Key Info

```
Key Algorithm:                RSA
Key Parameters:               05 00
Key Size:                     2048
Key SHA1 Fingerprint:         DA E9 14 1F 66 5F 04 B2 4A 8F
```

Setting up the malicious server:

- Updated Apache configuration to use the new fake certificate for example.com
- Configured the server to impersonate example.com

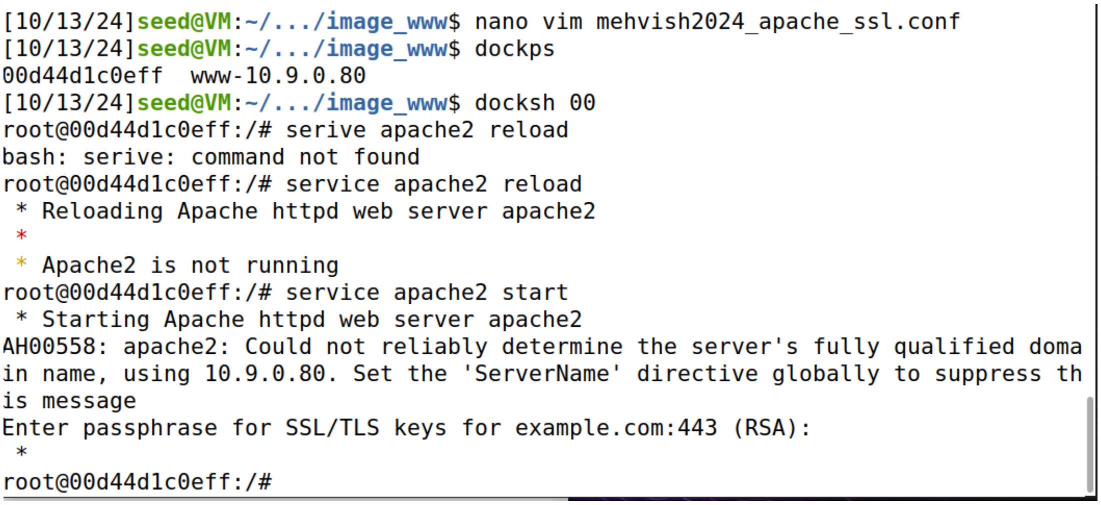
Launching the attack:

- Used dockps to list running containers
- Accessed the container shell using docksh
- Reloaded Apache configuration

- Started the Apache server

SSL/TLS Configuration:

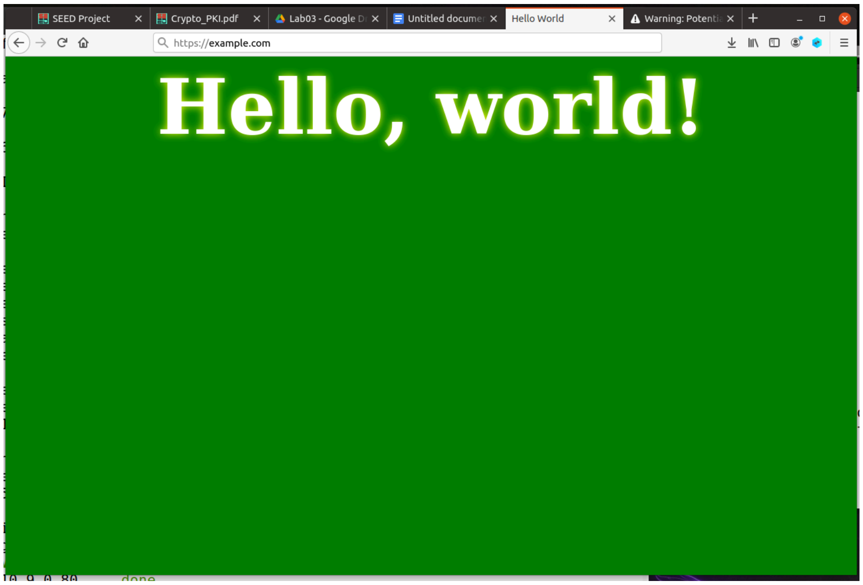
- Entered the passphrase for the SSL/TLS private key when prompted



```
[10/13/24]seed@VM:~/.../image_www$ nano vim mehvish2024_apache_ssl.conf
[10/13/24]seed@VM:~/.../image_www$ dockps
00d44d1c0eff  www-10.9.0.80
[10/13/24]seed@VM:~/.../image_www$ docksh 00
root@00d44d1c0eff:/# serive apache2 reload
bash: serive: command not found
root@00d44d1c0eff:/# service apache2 reload
 * Reloading Apache httpd web server apache2
 *
 * Apache2 is not running
root@00d44d1c0eff:/# service apache2 start
 * Starting Apache httpd web server apache2
AH00558: apache2: Could not reliably determine the server's fully qualified doma
in name, using 10.9.0.80. Set the 'ServerName' directive globally to suppress th
is message
Enter passphrase for SSL/TLS keys for example.com:443 (RSA):
 *
root@00d44d1c0eff:/#
```

Verifying the attack:

- Accessed example.com from Firefox
- Observed that browser recognizes the CA and hence believes that this is the actual certificate for example.com
- Confirmed that the connection appeared secure



Hello, world!

Observations:

When accessing example.com through the browser, the connection appeared secure without any warning flags. This seamless impersonation was possible due to the fake certificate generated using the compromised CA's private key. The browser accepted this certificate as valid, displaying the padlock icon typically associated with secure connections. Upon examining the certificate details, it was evident that the browser recognized it as issued by a trusted authority, further solidifying the attack's effectiveness. The content displayed on the fake website mirrored that of the legitimate website, making the deception virtually undetectable to an average user. This successful MITM attack demonstrates the severe security implications of a compromised root CA, as it allows attackers to generate seemingly legitimate certificates for any domain. The experiment underscores the critical importance of protecting CA private keys.