Lab 2 Report

Task 1:

Generate CA

```
seed@VM: ~/.../Labsetup
[02/10/23]seed@VM:~/.../Labsetup$ openssl req -new -x509 -newkey rsa:4096 -sha256 -days 3650
-keyout ca.key -out ca.crt -config lab2_openssl.cnf
Generating a RSA private key
.....................................................................++++
.....................................................................................
.............................................++++
writing new private key to 'ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Pennsylvania
Locality Name (eg, city) []:State College
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PSU
Organizational Unit Name (eg, section) []:CMPSC 443
Common Name (e.g. server FQDN or YOUR name) []:Jerry Chen
Email Address []:ypc5269@psu.edu
[02/10/23]seed@VM:~/.../Labsetup$
```

ca.crt

```
seed@VM: ~/.../Lab_2
[02/10/23]seed@VM:~/.../Lab_2$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            7c:e6:48:8c:8a:52:89:ae:14:2b:a3:da:92:25:7c:ef:6a:34:82:5a
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = Some-State, O = PSU, OU = Jerry Chen, CN = Jerry Chen
        Validity
            Not Before: Feb 10 22:44:11 2023 GMT
            Not After : Feb  7 22:44:11 2033 GMT
        Subject: C = US, ST = Some-State, O = PSU, OU = Jerry Chen, CN = Jerry Chen
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:ee:4b:b3:b0:af:79:c6:4a:37:3b:00:6d:49:77:
                    be:3d:a1:df:7d:24:e2:a8:05:c7:9d:e4:be:20:a2:
                    3d:09:d4:2b:76:b0:e8:2f:5c:35:7a:7f:ad:38:70:
                    7b:ec:73:4f:52:fa:4e:66:69:40:51:52:3e:b3:59:
                    74:ca:da:94:a7:e3:f5:30:da:bf:e8:a9:d5:0a:ac:
                    df:01:68:0a:57:19:cd:fb:b5:aa:8e:53:52:51:51:
                    26:03:4b:58:ca:ae:d4:5a:a3:8f:bf:63:6a:97:86:
                    48:cf:5b:75:76:9d:cd:78:58:3a:63:0e:60:01:e5:
                    57:74:14:2d:4a:37:e5:ac:5c:5f:e8:c1:66:74:0a:
                    7a:e7:81:59:33:38:92:8b:7f:4e:72:d2:b1:b9:01:
                    c9:b1:71:f6:11:63:60:87:94:58:82:e1:99:82:84:
                    97:2d:94:33:80:09:f1:64:1a:a7:a2:44:8d:4d:da:
                    a1:92:2a:ea:ac:de:91:bc:c9:f3:07:36:ba:c3:7c:
                    9a:cd:78:b2:39:1e:79:7b:2c:d2:e4:8c:5b:51:e4:
                    88:a4:18:23:00:59:85:34:9f:95:68:2f:3f:23:01:
                    29:e7:96:68:da:75:c0:ee:53:42:91:51:ba:2e:c3:
```

```
seed@VM: ~/.../Lab_2
                    b7:14:b8:e0:52:7e:39:b8:5e:a4:dd:33:e6:42:46:
                    af:a4:f8:50:05:1a:9f:6c:ce:3f:97:a8:05:74:7e:
                    25:6f:5c:02:c7:89:ab:43:43:86:b3:62:a9:c0:50:
                    03:a2:e0:01:f2:d4:f5:c5:ac:6c:df:09:d9:a0:69:
                    c9:28:5a:af:ea:05:88:7a:e3:b3:7c:81:25:e1:86:
                    8c:16:db:e9:c3:a5:52:38:32:f7:0b:c3:0b:75:58:
                    69:3c:9b:0b:fd:f9:0f:af:c0:0f:d8:26:97:43:bc:
                    95:1c:35:ba:90:d0:86:73:dd:12:3e:88:44:b6:85:
                    38:e6:5b:a4:6f:61:ad:f9:bd:7b:0e:8d:95:92:ba:
                    0e:fa:2e:cb:2b:07:4c:23:ce:c4:d0:8a:fc:cf:70:
                    2e:39:0d:52:e7:8d:24:6d:c4:93:02:e8:a5:62:46:
                    a9:a8:59:83:a4:1a:7c:f2:b7:8c:c1:43:79:67:c1:
                    9f:2a:cc:d4:07:37:3a:f7:3f:b1:4b:cc:79:bc:ab:
                    9e:d8:53:ec:c6:18:6c:e0:2d:72:86:0a:b9:8e:9f:
                    08:d4:9a:47:93:cd:f8:b3:2e:3a:52:33:c9:bf:69:
                    00:58:0e:22:54:7e:18:35:5f:9c:48:e4:b4:8b:04:
                    2f:35:ec:2e:38:04:a0:89:e0:44:c2:ab:4e:65:36:
                    ca:38:f8:b9:39:56:e8:d0:0d:d6:00:53:b4:19:10:
                    38:d7:61
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                FC:B4:1C:C5:E9:91:80:94:98:48:63:73:B3:C9:6D:A8:6E:1A:97:0E
            X509v3 Authority Key Identifier:
                keyid:FC:B4:1C:C5:E9:91:80:94:98:48:63:73:B3:C9:6D:A8:6E:1A:97:0E

            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         e6:f9:6b:d8:2e:1b:cd:18:3a:3b:fc:b5:6e:a7:de:3c:be:f8:
         4d:bb:b5:45:b0:dd:74:0b:7d:77:53:17:e4:09:89:80:d9:f7:
         8a:52:6a:37:16:8b:1b:fe:fb:57:58:7f:1a:d8:8f:8a:7f:84:
```

```
seed@VM: ~/.../Lab_2
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         e6:f9:6b:d8:2e:1b:cd:18:3a:3b:fc:b5:6e:a7:de:3c:be:f8:
         4d:bb:b5:45:b0:dd:74:0b:7d:77:53:17:e4:09:89:80:d9:f7:
         8a:52:6a:37:16:8b:1b:fe:fb:57:58:7f:1a:d8:8f:8a:7f:84:
         17:73:42:a0:59:9e:aa:04:1c:63:af:c8:82:c1:2f:49:52:6a:
         bb:f4:33:a2:95:91:a9:02:19:83:44:ac:ea:0a:08:8e:61:eb:
         1c:1b:1f:12:92:fb:65:90:7a:cc:0a:d9:2e:41:56:f7:84:c1:
         83:af:44:d9:19:ac:d3:8f:3e:d8:b6:73:e0:4f:0c:cc:12:39:
         27:14:ce:91:1f:c0:ec:02:e0:bb:1b:1f:af:c0:9c:72:1b:e1:
         e3:e9:84:99:37:4b:ea:d2:79:53:36:1f:62:bb:41:ac:ac:36:
         da:99:b0:88:7c:c1:f3:d2:42:27:67:86:d8:6d:6f:de:73:b9:
         fd:2b:91:da:ad:29:66:01:69:15:27:20:81:db:00:ff:62:4d:
         50:77:85:31:5e:f9:90:ac:c6:aa:df:33:3b:b5:36:9d:be:08:
         79:86:ed:36:2f:c4:67:20:50:a8:40:a4:69:7e:8a:ed:3e:5a:
         b0:94:b7:34:26:a2:63:91:02:5b:02:b4:9d:82:1a:06:88:df:
         f5:7d:d2:78:a2:98:cd:db:44:e0:ef:65:2c:9a:af:59:f6:74:
         0b:0e:e5:09:16:14:3b:be:8c:30:31:50:71:36:b9:66:e9:26:
         5a:c6:d8:72:6f:a8:74:67:7d:30:04:86:5b:74:67:ad:5c:fe:
         e9:96:21:3f:43:e8:2f:36:55:d4:6f:3d:e1:ba:c9:b7:ec:71:
         3e:8f:f9:39:79:5e:5b:2b:33:bb:db:f3:8a:e0:49:91:bf:58:
         69:48:8d:7f:08:9f:aa:32:6e:b0:c8:f5:21:5f:c1:51:5a:e7:
         0e:06:5c:75:e6:5b:c4:5f:93:52:6c:38:4a:e6:e2:3e:db:ba:
         06:6b:86:7b:76:c3:05:a6:f4:b8:7b:a5:08:45:ae:7b:0a:0b:
         5c:9d:34:47:bc:c6:42:b0:5b:96:ea:5f:f2:36:f4:89:b4:fb:
         96:5d:8c:c7:69:74:e8:24:95:c0:ed:2d:57:1d:9b:b2:82:1f:
         2d:0f:36:a4:d7:72:e6:9b:30:aa:2c:b0:e4:dd:38:3b:08:bf:
         39:a8:82:f3:4a:67:3a:81:ac:a0:5a:36:6d:ae:34:1e:46:a3:
         eb:37:89:dd:6f:fe:41:18:a7:14:86:58:49:8f:46:45:3f:aa:
         9b:d3:49:97:7b:68:53:a9:1e:b6:fb:4b:46:b1:6e:cc:25:48:
         5c:c1:45:da:38:24:c4:c7
[02/10/23]seed@VM:~/.../Lab_2$
```

Ca key

```
seed@VM: ~/.../Lab_2
02/10/23]seed@VM:~/.../Lab_2$ openssl rsa -in ca.key -text -noout
nter pass phrase for ca.key:
SA Private-Key: (4096 bit, 2 primes)
odulus:
    00:ee:4b:b3:b0:af:79:c6:4a:37:3b:00:6d:49:77:
    be:3d:a1:df:7d:24:e2:a8:05:c7:9d:e4:be:20:a2:
    3d:09:d4:2b:76:b0:e8:2f:5c:35:7a:7f:ad:38:70:
    7b:ec:73:4f:52:fa:4e:66:69:40:51:52:3e:b3:59:
    74:ca:da:94:a7:e3:f5:30:da:bf:e8:a9:d5:0a:ac:
    df:01:68:0a:57:19:cd:fb:b5:aa:8e:53:52:51:51:
    26:03:4b:58:ca:ae:d4:5a:a3:8f:bf:63:6a:97:86:
    48:cf:5b:75:76:9d:cd:78:58:3a:63:0e:60:01:e5:
    57:74:14:2d:4a:37:e5:ac:5c:5f:e8:c1:66:74:0a:
    7a:e7:81:59:33:38:92:8b:7f:4e:72:d2:b1:b9:01:
    c9:b1:71:f6:11:63:60:87:94:58:82:e1:99:82:84:
    97:2d:94:33:80:09:f1:64:1a:a7:a2:44:8d:4d:da:
    a1:92:2a:ea:ac:de:91:bc:c9:f3:07:36:ba:c3:7c:
    9a:cd:78:b2:39:1e:79:7b:2c:d2:e4:8c:5b:51:e4:
    88:a4:18:23:00:59:85:34:9f:95:68:2f:3f:23:01:
    29:e7:96:68:da:75:c0:ee:53:42:91:51:ba:2e:c3:
    b7:14:b8:e0:52:7e:39:b8:5e:a4:dd:33:e6:42:46:
    af:a4:f8:50:05:1a:9f:6c:ce:3f:97:a8:05:74:7e:
    25:6f:5c:02:c7:89:ab:43:43:86:b3:62:a9:c0:50:
    03:a2:e0:01:f2:d4:f5:c5:ac:6c:df:09:d9:a0:69:
    c9:28:5a:af:ea:05:88:7a:e3:b3:7c:81:25:e1:86:
    8c:16:db:e9:c3:a5:52:38:32:f7:0b:c3:0b:75:58:
    69:3c:9b:0b:fd:f9:0f:af:c0:0f:d8:26:97:43:bc:
    95:1c:35:ba:90:d0:86:73:dd:12:3e:88:44:b6:85:
    38:e6:5b:a4:6f:61:ad:f9:bd:7b:0e:8d:95:92:ba:
    0e:fa:2e:cb:2b:07:4c:23:ce:c4:d0:8a:fc:cf:70:
    2e:39:0d:52:e7:8d:24:6d:c4:93:02:e8:a5:62:46:
    a9:a8:59:83:a4:1a:7c:f2:b7:8c:c1:43:79:67:c1:
```

```
seed@VM: ~/.../Lab_2
    9f:2a:cc:d4:07:37:3a:f7:3f:b1:4b:cc:79:bc:ab:
    9e:d8:53:ec:c6:18:6c:e0:2d:72:86:0a:b9:8e:9f:
    08:d4:9a:47:93:cd:f8:b3:2e:3a:52:33:c9:bf:69:
    00:58:0e:22:54:7e:18:35:5f:9c:48:e4:b4:8b:04:
    2f:35:ec:2e:38:04:a0:89:e0:44:c2:ab:4e:65:36:
    ca:38:f8:b9:39:56:e8:d0:0d:d6:00:53:b4:19:10:
    38:d7:61
publicExponent: 65537 (0x10001)
privateExponent:
    78:5d:36:8b:45:67:3e:18:58:a3:6d:c8:c5:f6:3c:
    da:86:bc:0b:4b:29:4d:73:75:eb:b4:11:b1:0c:21:
    c6:a8:2b:b8:0d:0d:8a:76:89:f0:b1:32:fe:b2:1a:
    76:49:9c:44:ae:78:11:54:92:8f:40:fa:b8:be:b3:
    b6:8f:07:cd:71:e0:74:67:d9:cd:9c:93:26:8c:41:
    2c:45:b0:0b:64:d6:5d:90:da:70:7f:77:b1:e9:4a:
    49:19:b2:e4:d5:c0:1f:74:44:74:88:b3:db:8b:91:
    95:63:7e:06:87:18:b4:f3:e3:b2:0b:1d:c5:77:61:
    60:19:9c:f2:c3:1f:38:9b:84:3a:5e:0d:f1:09:26:
    21:6f:7d:6d:d8:e2:74:a1:be:2f:53:6b:3f:a6:be:
    88:e9:a6:40:0c:31:42:ea:54:76:ef:9b:09:89:0d:
    8f:91:2f:1e:3a:67:7a:87:d8:2a:a7:73:b4:62:7d:
    80:06:3b:79:4c:06:d3:14:32:b4:6f:19:91:0a:8c:
    6a:c2:cf:4a:f8:b0:a5:dd:f3:3c:4c:05:08:6d:65:
    f3:74:d9:a1:20:96:9f:09:08:7f:92:75:d2:a9:90:
    d0:10:72:2f:fe:90:90:10:f0:2b:d4:db:35:29:d8:
    7d:18:10:fe:ba:11:4f:a6:46:a2:10:c7:fa:ac:17:
    a5:43:d5:c1:fa:27:db:44:8e:c5:99:77:1f:37:f5:
    a3:55:75:b7:cf:92:a6:dc:67:0d:48:e4:0f:1f:67:
    e9:e7:fb:ad:f6:32:03:48:86:d6:17:ad:29:e7:ea:
    da:a7:10:6d:94:68:68:62:5f:ce:6f:f8:81:3f:15:
    6c:3d:9a:7d:3c:c6:08:b4:81:ad:1d:89:b8:bd:dd:
    aa:d0:2d:eb:3e:87:c7:9a:94:67:6a:a7:3f:a6:ee:
```

```
seed@VM: ~/.../Lab_2
    a6:bb:6f:3c:ff:0c:2c:6f:d5:c0:50:36:b8:68:b9:
    0e:29:1e:ec:1c:b9:2d:8b:f5:d3:c1:ef:64:45:2a:
    4e:cc:76:8a:0b:19:46:45:c2:38:d7:dc:80:71:58:
    1f:3b:21:e9:1a:03:a1:ef:b3:66:0b:37:80:66:ce:
    56:76:02:61:52:db:a7:cb:29:d1:d5:11:8d:32:ca:
    17:7e:f4:74:bd:8c:3f:f7:81:10:a7:14:97:10:09:
    4a:82:78:8e:58:03:47:a5:e5:05:8b:00:94:ab:9b:
    6f:58:e1:4a:03:2a:f3:9b:8b:40:5b:08:71:9d:ff:
    40:7d:d4:89:63:85:80:8b:31:3c:a8:dd:53:63:da:
    26:27:f5:ca:3f:fe:d6:6e:2d:ee:a9:8d:27:4c:9c:
    83:7a:ca:1d:02:55:81:4c:c4:09:d2:bd:35:b1:e5:
    68:01
prime1:
    00:fb:74:83:1b:87:93:10:01:78:34:86:30:89:f7:
    6a:f0:66:a8:1b:b7:45:be:51:84:07:dd:37:a2:cb:
    c2:fb:79:7f:92:2b:20:3e:5b:ce:ff:f1:3d:72:d4:
    45:b3:6e:02:a3:9a:4f:f3:f2:92:84:0c:1f:0a:1e:
    bd:bc:55:a4:4e:43:af:28:d4:c7:54:33:ed:6d:33:
    b7:9c:ce:24:54:b9:07:49:38:27:88:29:d6:2e:d8:
    a8:10:92:ea:da:94:40:63:87:94:0f:44:94:41:47:
    7d:97:d9:ca:1f:4e:f6:cb:ae:28:0c:93:67:eb:11:
    c3:a1:4b:22:a9:ea:c6:63:39:ec:98:0d:bb:36:35:
    c7:90:47:f1:3a:0e:b4:06:98:90:d5:5d:ad:1e:62:
    c7:be:86:c2:15:68:23:21:34:75:43:7f:93:4a:08:
    69:62:51:64:c4:8f:90:47:3b:74:f0:2f:88:70:22:
    09:32:8c:81:35:06:4a:48:91:a5:58:b0:16:a7:ae:
    63:1b:31:1f:e3:ec:4d:95:e8:83:fa:c0:62:1a:89:
    04:28:de:25:e1:49:ff:d2:a1:09:ae:f0:e9:8e:99:
    da:42:91:12:0a:4f:a0:cd:af:37:6b:7b:37:34:4b:
    c1:7d:98:31:39:1c:92:65:8e:f6:8c:c6:02:22:de:
    37:c1
prime2:
```

```
seed@VM: ~/.../Lab_2
prime2:
    00:f2:9a:4d:07:e3:2a:c7:54:43:31:7a:9a:c8:c3:
    ed:7d:6d:63:33:fe:c0:7c:d5:46:fd:0f:2e:39:05:
    e8:0b:67:8b:7d:a0:b6:39:09:9c:4d:c8:3b:f2:e7:
    f7:53:51:6d:77:56:2b:29:99:24:74:87:4f:56:9c:
    f9:d2:f1:3b:f7:9b:cc:5e:d5:d3:40:a0:ce:95:18:
    14:ae:7d:1d:38:92:a7:2d:7d:a6:47:5f:ee:44:81:
    81:19:15:4d:1d:e5:4e:41:6f:22:3b:a2:ab:a1:8b:
    81:b2:30:8c:18:ee:e1:de:17:bb:38:c2:f3:d7:bb:
    2d:73:c6:ae:73:6d:08:24:a9:68:de:e2:db:9a:78:
    c0:87:aa:df:57:62:ff:9a:78:b4:25:21:e4:e2:bf:
    5e:b8:3a:ab:a4:ea:88:ed:a2:9d:80:e3:ab:ed:02:
    db:eb:0e:4d:84:ef:9d:6a:75:6b:a4:9b:73:4f:26:
    a3:8f:e0:ee:86:4b:04:b8:79:bf:ba:45:ab:11:3c:
    7d:f9:cc:06:ea:67:89:83:53:09:34:1a:ac:b3:ca:
    67:7d:d0:df:f4:8c:c8:a6:9a:a0:61:3f:d9:d7:a9:
    96:b2:e2:fc:c6:94:24:43:a2:71:cd:74:df:21:67:
    f0:42:6c:41:a4:59:11:d0:7b:24:3c:21:4a:0f:51:
    87:a1
exponent1:
    07:ae:6d:7a:df:cf:5c:43:cf:3a:3b:87:2c:0f:c4:
    d2:87:30:47:78:77:c6:f2:92:87:f2:f8:0a:1f:13:
    5b:bf:40:68:64:ac:dd:7a:cc:7e:01:0e:91:7d:6e:
    8b:a6:a6:a9:fc:c2:c8:7e:f6:7e:d6:27:f4:95:2f:
    d2:9b:03:23:e8:e9:66:e3:e9:1a:e7:63:2f:5c:cf:
    15:19:2e:fe:ef:90:0b:6a:8d:ba:99:1c:93:dd:c6:
    74:8b:28:65:78:f5:e6:94:73:af:6b:b6:e3:af:9d:
    64:90:20:9e:88:38:fd:cb:da:29:58:2f:6a:7c:e6:
    6e:fc:ee:98:26:35:dd:3e:1d:be:1f:5d:42:b0:ad:
    e1:f8:70:a4:07:62:f4:78:a0:a4:03:f2:8f:e5:10:
    98:ff:60:da:6a:8d:f8:2b:b4:11:55:ca:58:0e:9d:
    b9:85:27:00:e2:29:d4:23:3a:d5:43:7e:75:7e:74:
```

```
seed@VM: ~/.../Lab_2
    ad:78:a1:51:cf:59:61:92:21:6c:ee:24:23:07:2e:
    bb:db:ea:4f:7a:1e:7c:9f:d7:b8:47:3c:37:f7:4b:
    8b:3c:0e:08:2d:cc:84:d0:aa:8d:0f:8a:f2:f2:3c:
    3a:a0:57:de:bc:c3:fa:c4:89:7a:dd:0e:b8:a8:3f:
    c6:e8:69:48:87:58:e9:85:4e:7e:ca:65:b2:4e:fb:
    81
exponent2:
    00:ce:10:f8:8b:51:8e:fd:9e:fa:30:25:f7:21:bf:
    22:93:de:7d:5c:25:f0:74:58:68:a2:fc:e9:03:30:
    9c:28:4b:bc:75:6a:34:3e:00:86:ce:9e:dd:24:f7:
    99:e2:20:91:3d:c3:68:88:3d:f7:74:2f:96:d9:78:
    1e:cf:e9:6e:49:65:01:d4:30:05:ef:a8:67:b0:c6:
    b2:92:7f:dd:79:37:40:5f:68:91:fb:a0:65:6f:b5:
    1c:e6:24:6c:cb:8f:01:c8:9c:d0:54:1d:59:71:af:
    60:eb:ed:46:a2:cb:0d:f9:aa:e8:b1:4f:0e:f6:58:
    9c:43:f2:28:2e:0d:17:d4:a4:3d:5a:cd:11:41:85:
    7d:eb:fe:dd:14:8a:17:98:ab:1c:41:4a:27:f3:de:
    1f:63:97:1a:42:cb:a0:a1:50:f6:3e:0b:a4:f6:7d:
    ee:35:1b:82:06:ff:cd:13:27:47:d6:9a:df:f8:04:
    56:fc:18:50:22:ab:c8:07:b6:0a:7f:fb:3b:52:39:
    b2:bb:a2:6c:e1:60:2e:b2:e8:ae:31:9e:d2:c1:28:
    94:7d:8f:15:1b:d1:15:82:46:67:22:13:ad:42:fd:
    5e:ee:f5:d5:46:0b:81:3e:1d:d6:52:71:0a:32:82:
    e9:d6:51:c3:f4:08:60:14:58:f4:af:4a:8b:70:b5:
    8c:e1
coefficient:
    2b:d0:1e:cf:09:92:81:f4:4a:20:a8:f9:e6:d3:cf:
    04:a2:a4:de:ea:fb:0a:fb:97:16:44:59:9f:4f:65:
    32:e6:cc:72:1f:42:a0:76:b5:e3:e4:de:94:e2:d2:
    e1:30:1c:77:c2:29:92:20:e2:f7:54:37:52:68:52:
    46:57:2a:78:52:f9:7c:65:30:6f:7b:4c:c0:3c:a3:
    a5:09:47:f9:80:e0:03:78:44:b8:4a:c0:21:f5:6f:
```

```
coefficient:
    2b:d0:1e:cf:09:92:81:f4:4a:20:a8:f9:e6:d3:cf:
    04:a2:a4:de:ea:fb:0a:fb:97:16:44:59:9f:4f:65:
    32:e6:cc:72:1f:42:a0:76:b5:e3:e4:de:94:e2:d2:
    e1:30:1c:77:c2:29:92:20:e2:f7:54:37:52:68:52:
    46:57:2a:78:52:f9:7c:65:30:6f:7b:4c:c0:3c:a3:
    a5:09:47:f9:80:e0:03:78:44:b8:4a:c0:21:f5:6f:
    7f:e2:fc:92:cb:03:e0:75:dd:90:83:00:a5:50:2d:
    2c:7a:fd:c3:df:a9:5e:8f:25:41:2f:00:4d:4d:40:
    f7:f5:a1:75:6e:3a:f4:6c:fb:b0:97:6a:75:40:a7:
    ef:67:f6:bc:fc:b8:dc:37:96:08:b8:d3:a7:49:dc:
    dd:a8:5e:99:2c:ab:a5:41:76:05:73:66:8d:7c:3b:
    1e:c0:10:24:61:14:ba:fe:40:20:0e:e9:7f:cf:63:
    a3:ff:1a:cb:9a:f8:e4:cb:d2:42:1a:77:dc:7b:66:
    6d:26:b2:fc:11:ff:87:0a:54:c3:36:e6:55:7e:4d:
    ba:01:23:45:83:0b:f6:03:41:6d:d8:81:1f:70:d5:
    b2:d4:31:21:ce:4f:2a:68:bd:95:2d:1f:54:7b:a3:
    32:72:94:d7:0c:72:53:bd:5a:bd:8f:b0:cb:6b:a9:
    a6
[02/10/23]seed@VM:~/.../Lab_2$
```

The CA is generated by rsa 4096 sha256 using my own config.

The Issuer and Subject are identical, indicating that is a self-signed certificate.

When the certificate contains digital signatures, then it is CA certificate. In this case, my own certificate is self-signed.

Task 2:

Creating own server key and csr. My own DNS: www.problemsolver68.com

Alternative names command are in the bottom part of the $openssl req command

```
seed@VM: ~/.../Labsetup
State or Province Name (full name) [Some-State]:Pennsylvania
Locality Name (eg, city) []:State College
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PSU
Organizational Unit Name (eg, section) []:CMPSC 443
Common Name (e.g. server FQDN or YOUR name) []:Jerry Chen
Email Address []:ypc5269@psu.edu
[02/10/23]seed@VM:~/.../Labsetup$ openssl req -newkey rsa:2048 -sha256 -keyout server.key -ou
t server.csr -subj "/CN=www.problemsolver68.com/O=Problemsolver 68 /C=JP" -passout pass:sense
i -config lab2_openssl.cnf -addext "subjectAltName = DNS:www.problemsolver68.com, DNS:www.pro
blemsolver68A.com, DNS:www.problemsolver68B.com" -config lab2_openssl.cfg
Can't open lab2_openssl.cfg for reading, No such file or directory
140414012495168:error:02001002:system library:fopen:No such file or directory:crypto/bio/bss_
file.c:69:fopen('lab2_openssl.cfg','r')
140414012495168:error:2006D080:BIO routines:BIO_new_file:no such file:crypto/bio/bss_file.c:7
6:
[02/10/23]seed@VM:~/.../Labsetup$ openssl req -newkey rsa:2048 -sha256 -keyout server.key -ou
t server.csr -subj "/CN=www.problemsolver68.com/O=Problemsolver 68 /C=JP" -passout pass:sense
i -config lab2_openssl.cnf -addext "subjectAltName = DNS:www.problemsolver68.com, DNS:www.pro
blemsolver68A.com, DNS:www.problemsolver68B.com" -config lab2_openssl.cnf
Generating a RSA private key
...............................+++++
.......................................................+++++
writing new private key to 'server.key'
-----
[02/10/23]seed@VM:~/.../Labsetup$
```

Server csr

```
seed@VM: ~/.../Labsetup
[02/10/23]seed@VM:~/.../Labsetup$ openssl req -in server.csr -text -noout
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = www.problemsolver68.com, O = "Problemsolver 68 ", C = JP
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:df:ec:30:cb:7b:b5:ce:40:e9:c5:5c:fb:9c:24:
                    8b:36:50:c8:33:48:ea:1b:c2:c2:e4:5c:ba:a5:a3:
                    a7:5a:2b:2d:92:98:85:f3:ca:46:bc:50:4a:9d:58:
                    af:d5:81:df:7f:2d:4f:f6:fc:23:3f:1f:f1:c7:64:
                    f8:fc:27:dd:2b:04:8b:44:00:bc:e1:57:10:02:5a:
                    b4:52:0b:3f:27:a4:01:27:73:49:21:d1:6e:5f:47:
                    a7:2f:00:1e:82:a5:51:2b:cb:16:45:04:86:e2:ad:
                    08:de:8e:f4:1d:8b:b5:24:46:9d:b2:1f:21:ad:fb:
                    9f:1f:a4:d1:69:a9:b2:ac:62:35:f3:7e:ef:a9:3d:
                    be:87:3a:1f:c5:2c:d1:24:1e:02:d0:45:54:c3:94:
                    c5:bf:72:83:1b:11:bd:2f:32:2c:79:d6:2c:52:e9:
                    67:66:5c:1f:82:8a:e1:bd:28:ea:10:c2:39:4f:54:
                    90:11:8d:a0:60:15:e0:34:8c:d5:f7:3d:42:9c:66:
                    6e:04:20:d7:7a:7f:2f:03:37:07:ad:a3:7b:b1:aa:
                    df:ed:01:54:1f:25:50:ad:84:76:a0:72:20:46:f3:
                    87:e6:50:9c:0b:c5:91:b1:7f:7d:77:b1:49:b1:1a:
                    c1:0d:66:e8:46:dc:03:78:9a:7a:5a:5c:18:cd:fe:
                    1f:db
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Subject Alternative Name:
```

```
seed@VM: ~/.../Labsetup
                    be:87:3a:1f:c5:2c:d1:24:1e:02:d0:45:54:c3:94:
                    c5:bf:72:83:1b:11:bd:2f:32:2c:79:d6:2c:52:e9:
                    67:66:5c:1f:82:8a:e1:bd:28:ea:10:c2:39:4f:54:
                    90:11:8d:a0:60:15:e0:34:8c:d5:f7:3d:42:9c:66:
                    6e:04:20:d7:7a:7f:2f:03:37:07:ad:a3:7b:b1:aa:
                    df:ed:01:54:1f:25:50:ad:84:76:a0:72:20:46:f3:
                    87:e6:50:9c:0b:c5:91:b1:7f:7d:77:b1:49:b1:1a:
                    c1:0d:66:e8:46:dc:03:78:9a:7a:5a:5c:18:cd:fe:
                    1f:db
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Subject Alternative Name:
                DNS:www.problemsolver68.com, DNS:www.problemsolver68A.com, DNS:www.problemsolver68B.com
    Signature Algorithm: sha256WithRSAEncryption
         67:72:d8:c4:e4:73:50:a6:9c:68:4d:61:ca:7e:4f:ec:99:b4:
         8d:af:cb:66:e5:33:0b:94:93:72:29:2a:a0:3e:06:93:87:6e:
         ea:bc:02:03:9d:ea:af:7f:be:3b:3b:10:4f:30:80:e0:a1:21:
         3f:07:92:f8:9a:6b:10:a3:2c:16:50:b8:5c:6e:94:1b:1d:ab:
         28:90:c7:e8:c4:43:d6:8f:72:96:d7:77:33:7c:51:25:1e:35:
         32:42:da:a9:91:17:53:33:a8:71:3b:37:d6:12:9f:87:84:67:
         2b:01:ca:70:ba:8e:c1:75:09:c4:f8:85:aa:62:f8:35:88:c5:
         bd:7d:d4:6d:9b:e0:25:fd:71:a8:46:2f:92:9e:bb:62:a1:b6:
         82:9f:e7:8b:78:4f:9e:26:0c:4d:a0:d1:ef:3e:8e:3b:48:ab:
         e0:86:f9:cc:1c:bd:94:c2:06:23:be:21:12:ea:20:48:a6:0a:
         51:f4:a5:44:b8:00:66:ad:b0:d6:df:e3:87:5a:db:e6:ed:19:
         c1:b1:fd:55:08:77:c7:ca:a5:17:ec:1b:c0:d8:21:bc:cf:df:
         fe:95:be:8d:43:35:30:1d:1a:15:e0:34:9d:a6:02:38:c4:89:
         50:fd:1d:11:fe:d8:c3:c8:99:cc:7e:df:e2:80:8f:f8:68:0d:
         0c:0a:50:4d
[02/10/23]seed@VM:~/.../Labsetup$
```

Server key

```
seed@VM: ~/.../Labsetup
[02/10/23]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:df:ec:30:cb:7b:b5:ce:40:e9:c5:5c:fb:9c:24:
    8b:36:50:c8:33:48:ea:1b:c2:c2:e4:5c:ba:a5:a3:
    a7:5a:2b:2d:92:98:85:f3:ca:46:bc:50:4a:9d:58:
    af:d5:81:df:7f:2d:4f:f6:fc:23:3f:1f:f1:c7:64:
    f8:fc:27:dd:2b:04:8b:44:00:bc:e1:57:10:02:5a:
    b4:52:0b:3f:27:a4:01:27:73:49:21:d1:6e:5f:47:
    a7:2f:00:1e:82:a5:51:2b:cb:16:45:04:86:e2:ad:
    08:de:8e:f4:1d:8b:b5:24:46:9d:b2:1f:21:ad:fb:
    9f:1f:a4:d1:69:a9:b2:ac:62:35:f3:7e:ef:a9:3d:
    be:87:3a:1f:c5:2c:d1:24:1e:02:d0:45:54:c3:94:
    c5:bf:72:83:1b:11:bd:2f:32:2c:79:d6:2c:52:e9:
    67:66:5c:1f:82:8a:e1:bd:28:ea:10:c2:39:4f:54:
    90:11:8d:a0:60:15:e0:34:8c:d5:f7:3d:42:9c:66:
    6e:04:20:d7:7a:7f:2f:03:37:07:ad:a3:7b:b1:aa:
    df:ed:01:54:1f:25:50:ad:84:76:a0:72:20:46:f3:
    87:e6:50:9c:0b:c5:91:b1:7f:7d:77:b1:49:b1:1a:
    c1:0d:66:e8:46:dc:03:78:9a:7a:5a:5c:18:cd:fe:
    1f:db
publicExponent: 65537 (0x10001)
privateExponent:
    00:95:9f:4d:cf:79:bf:36:ad:3b:47:4c:65:37:a5:
    57:7c:18:a8:5d:54:58:51:ea:66:ad:8e:a4:8c:ef:
    78:70:90:af:67:e8:10:81:a0:e4:79:0a:31:81:47:
    f4:5d:f6:e4:ef:26:c8:ea:e0:f9:70:41:99:1d:c2:
    03:79:01:ee:0f:c3:7e:87:16:f3:1e:a3:3d:28:45:
    91:7d:cc:d4:0b:59:d4:07:97:4a:03:95:dc:69:40:
    08:9f:28:36:3a:d7:da:10:28:28:9e:3f:73:1d:dd:
```

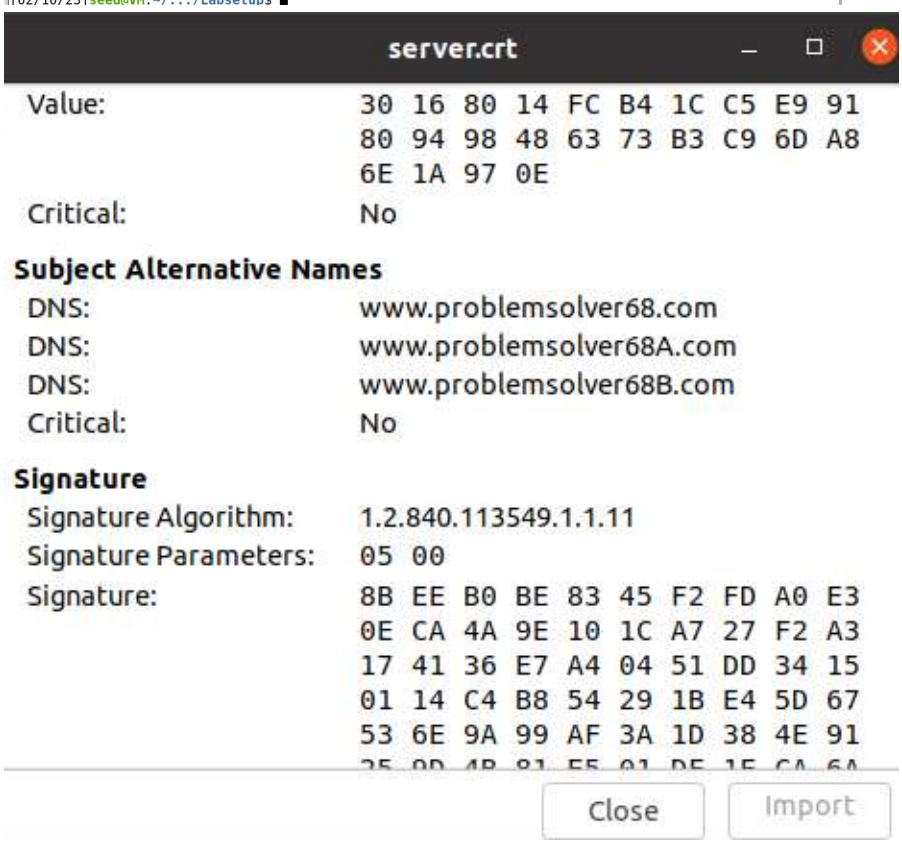
```
seed@VM: ~/.../Labsetup
    bf:32:6f:55:00:b5:0c:79:cb:d1:ad:66:8d:eb:a2:
    59:66:1c:8c:6d:4d:1d:fd:7e:76:02:db:7b:bd:9f:
    b3:1c:ac:4a:df:8e:ad:30:35:36:e3:ae:9e:95:2d:
    7a:f5:89:c7:94:ac:fd:ee:5b:07:fb:79:83:11:87:
    09:c5:15:af:ac:9d:4d:84:29:b0:58:ab:09:f8:39:
    e3:aa:9b:38:e3:79:39:00:df:dc:7f:ed:24:c4:f4:
    09:29:42:61:21:77:ef:ed:85:75:bf:38:1c:03:cb:
    19:fb:1a:fd:77:d6:21:7b:0a:51:3b:8c:55:40:58:
    90:7b:a1:5c:49:6e:97:1b:f3:9a:22:3d:49:d3:f0:
    14:05:de:c2:cf:e2:dd:6b:af:98:ea:93:53:c9:b3:
    10:49
prime1:
    00:fa:64:8b:51:85:7c:5e:0b:00:32:d7:d5:8a:29:
    96:7c:82:a1:98:ab:ec:ff:14:e1:61:12:7f:19:ef:
    39:7d:bd:67:94:cd:10:37:fe:8d:0c:25:01:c9:09:
    10:3b:8f:15:94:bf:82:b9:71:00:59:1e:a9:f0:65:
    6b:cc:11:46:59:fa:bd:dc:46:b9:af:65:3b:21:52:
    96:df:53:ab:27:c2:09:1e:4b:e2:55:2f:6c:8f:3c:
    25:3f:d5:b3:f0:4c:95:8e:6f:53:48:15:98:ff:46:
    cf:7b:59:d9:0e:a0:16:0e:0b:a3:9f:4a:f6:af:69:
    0e:08:3c:44:29:e7:4c:cc:bf
prime2:
    00:e4:ef:e5:e1:d1:4e:af:ce:88:ee:29:57:2d:ea:
    ef:96:7a:c8:ee:53:ed:3f:9e:6e:a8:9f:44:2f:f5:
    ba:62:da:48:cc:ec:e4:f2:0b:b2:8b:00:40:78:b3:
    f5:f4:28:b0:e0:9d:9d:f0:4c:b7:3b:59:60:af:b5:
    2b:00:fa:86:da:f6:8c:74:98:97:fc:4a:bd:03:fb:
    a4:f9:1e:38:2b:8d:84:c3:03:7f:34:83:fb:b2:1d:
    20:8b:39:ce:8b:a9:72:d2:77:1f:fb:b6:5d:c4:ae:
    d2:e2:7c:2d:a3:c1:22:4d:a9:6b:8b:8a:cb:cd:9b:
    44:47:a3:ce:75:8c:fe:47:e5
```

```
seed@VM: ~/.../Labsetup
exponent1:
    00:c6:1a:84:6b:74:2c:28:8f:95:91:a4:58:0b:9e:
    c9:b4:2a:fa:45:3b:49:1f:ab:da:81:1d:cc:37:ad:
    a0:93:ce:25:c4:81:d5:a2:27:a0:5a:8a:70:f6:28:
    58:92:76:ab:41:6b:9f:b6:ae:23:f3:5e:a2:5f:53:
    2e:cd:5e:a1:85:91:2f:63:b7:05:34:32:e8:6c:7d:
    d6:66:4c:e1:2e:6c:83:20:58:33:72:e8:39:80:bd:
    ba:4e:dd:fa:26:55:c1:41:d6:ec:52:2c:dc:46:a4:
    34:85:c8:59:46:0b:fc:47:12:88:5b:00:49:5a:10:
    c9:0c:54:fa:2d:19:16:17:2b
exponent2:
    2a:eb:06:4f:85:2b:99:2d:c0:e1:d5:02:30:eb:80:
    2a:d7:ad:df:70:00:64:12:d1:6f:ef:1b:9b:5a:17:
    ac:fc:7a:f5:5f:db:b3:bc:99:a6:11:50:04:d0:c7:
    e5:13:d3:c4:e8:07:79:cb:07:f6:aa:54:c3:db:d4:
    ca:04:2d:4f:d3:34:95:8f:1d:bf:00:4b:da:f9:4b:
    fe:1f:ba:2c:00:05:c9:81:58:51:82:04:a7:69:6a:
    76:6f:49:d7:48:d6:eb:b9:c5:57:2c:e2:fb:42:42:
    ea:8e:99:07:bf:e7:2c:63:fc:73:56:7b:ca:79:b7:
    1d:2f:0a:3f:63:45:30:39
coefficient:
    00:b2:ab:db:3c:1f:52:75:68:36:b0:4a:ed:fd:02:
    66:5c:25:3b:ba:39:51:b2:9d:a3:3c:bf:7f:a4:29:
    c3:6a:da:58:43:73:06:04:b8:d2:8a:50:e6:0e:6d:
    ef:94:71:38:f1:46:cf:67:47:77:60:ac:a7:b7:fb:
    7c:13:29:2e:e4:30:13:c0:2b:6d:4f:93:ff:04:fc:
    33:f8:e5:20:04:09:4f:b0:e3:a0:e1:8b:5f:53:41:
    3c:2c:ce:cb:7c:25:68:53:72:36:74:5f:75:87:c5:
    f7:ea:a0:cf:cb:ee:1b:90:56:bb:00:88:78:7d:e3:
    98:26:da:4c:b8:7e:33:f0:0c
[02/10/23]seed@VM:~/.../Labsetup$
```

Task 3:

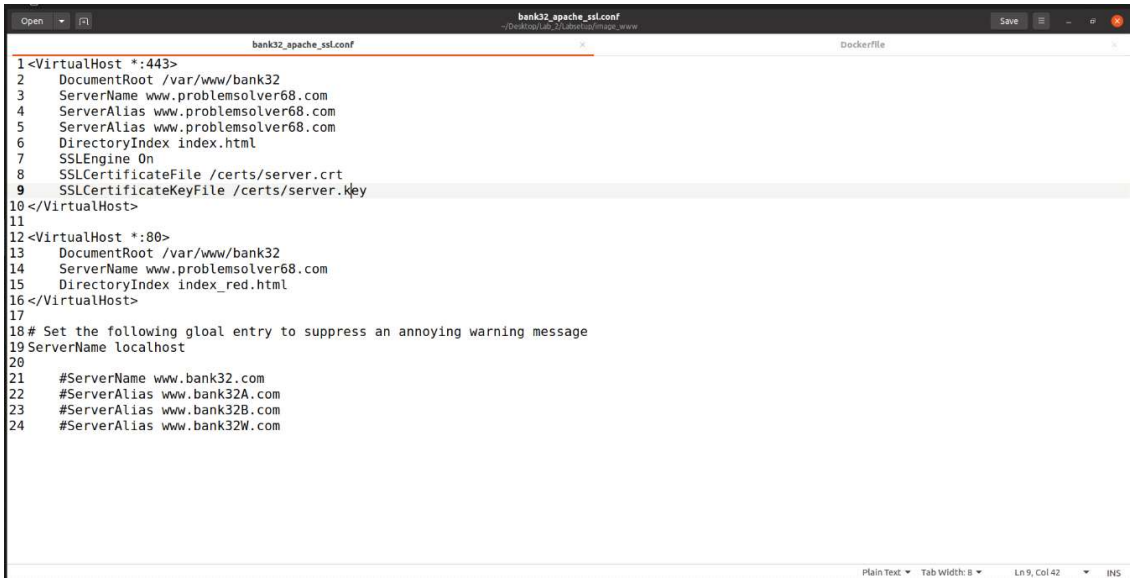
Sign ca to own server, then server.crt will appear along side server.key and server.csr

```
seed@VM: ~/.../Labsetup
-----
[02/10/23]seed@VM:~/.../Labsetup$ openssl ca -config lab2_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 lab2_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: Feb 10 06:00:30 2023 GMT
            Not After : Feb  7 06:00:30 2033 GMT
        Subject:
            countryName               = JP
            organizationName          = Problemsolver 68
            commonName                = www.problemsolver68.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                BB:76:E5:9D:E1:77:8B:A4:E3:90:1E:C5:AC:A2:3E:88:45:F8:A2:25
            X509v3 Authority Key Identifier:
                keyid:3D:A7:35:0B:C9:BA:55:18:81:D4:79:BE:03:EB:32:B7:55:51:56:3E

Certificate is to be certified until Feb  7 06:00:30 2033 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
[02/10/23]seed@VM:~/.../Labsetup$
```



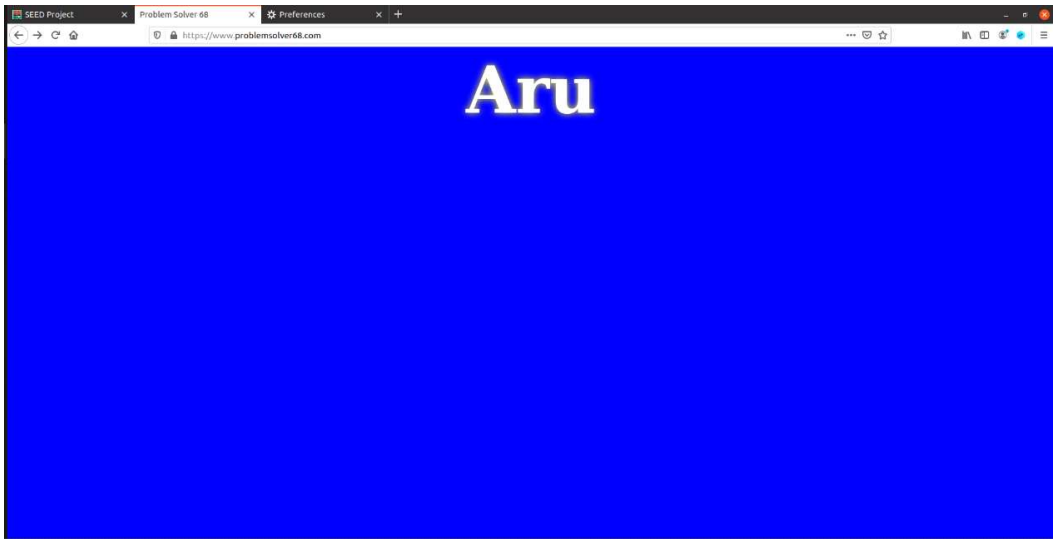
Task 4

Custom bank32 config file with new certificate directory and YouTube DNS

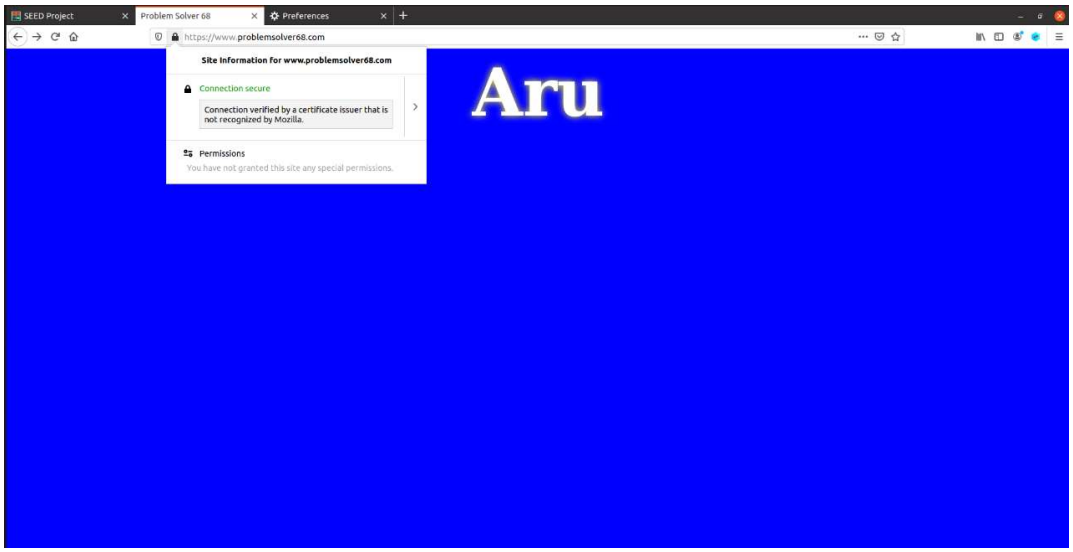


```
<VirtualHost *:443>
    DocumentRoot /var/www/bank32
    ServerName www.problemsolver68.com
    ServerAlias www.problemsolver68.com
    ServerAlias www.problemsolver68.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/server.crt
    SSLCertificateKeyFile /certs/server.key
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot /var/www/bank32
    ServerName www.problemsolver68.com
    DirectoryIndex index_red.html
</VirtualHost>

# Set the following gloal entry to suppress an annoying warning message
ServerName localhost

    #ServerName www.bank32.com
    #ServerAlias www.bank32A.com
    #ServerAlias www.bank32B.com
    #ServerAlias www.bank32W.com
```

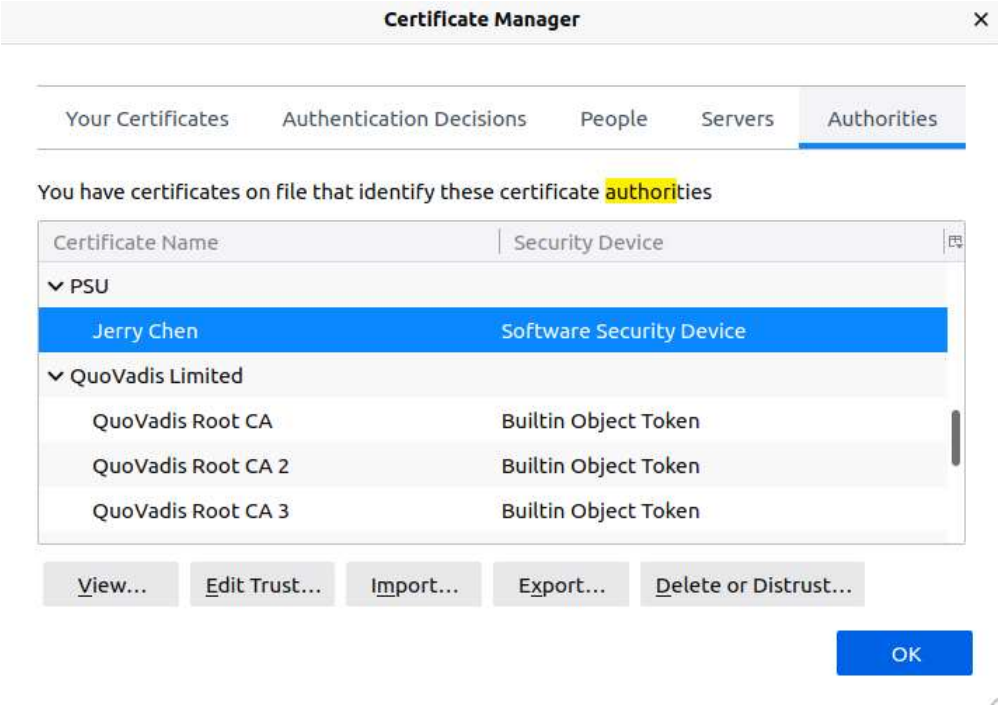
Accessed own certificated website



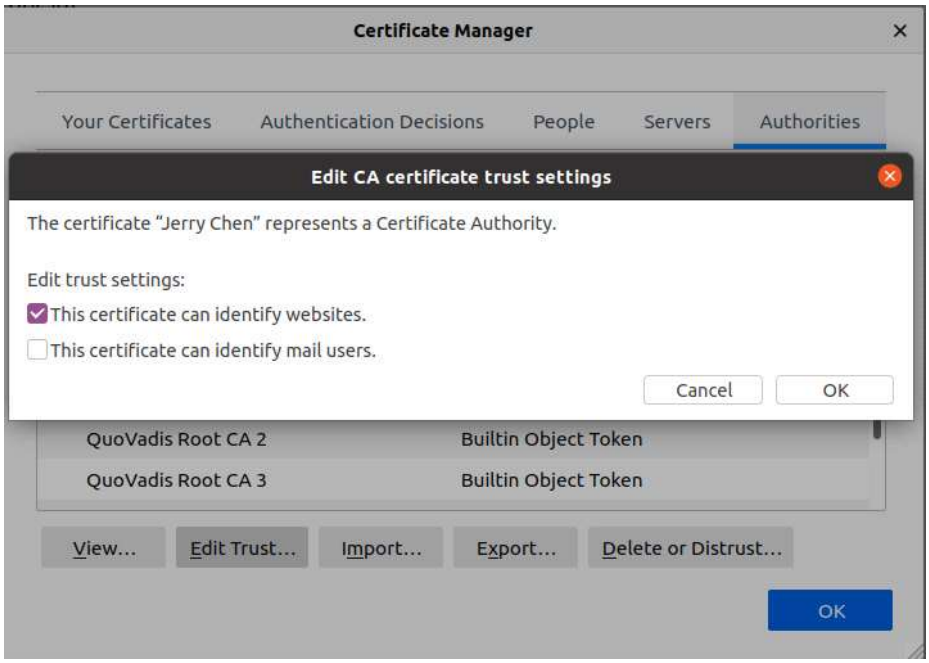
Browser shows certificate on, therefore secure connection



Imported CA



Check identify websites to let browser trust it.



Task 5

The site I chose to fake is www.youtube.com .

Fake DNS ssl configuration

```
<VirtualHost *:443>
    DocumentRoot /var/www/bank32
    ServerName www.youtube.com
    ServerAlias www.problemsolver68A.com
    ServerAlias www.problemsolver68B.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/server.crt
    SSLCertificateKeyFile /certs/server.key
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot /var/www/bank32
    ServerName www.problemsolver68.com
    DirectoryIndex index_red.html
</VirtualHost>

# Set the following gloal entry to suppress an annoying warning message
ServerName localhost

    #ServerName www.bank32.com
    #ServerAlias www.bank32A.com
    #ServerAlias www.bank32B.com
    #ServerAlias www.bank32W.com
```

Also add youtube.com to host for DNS polluting

```
127.0.0.1       localhost
127.0.1.1       VM

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

# Lab 2
10.9.0.80 www.problemsolver68.com
10.9.0.80 www.bank32.com
10.9.0.80 www.youtube.com

# 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
```

Youtube.com now redirects to my own website. However, the browser always shows unsecured connection as the certificate is absent or mismatching.

Task 6:

To launch man-in-middle attack:

First, create a dummy server.csr as youtube-server.csr, youtube-server.key to impersonate

Youtube's certificate.

```
seed@VM: ~/.../Lab_2
[02/10/23]seed@VM:~/.../Lab_2$ openssl req -newkey rsa:2048 -sha256 -keyout yout
ube-server.key -out youtube-server.csr -subj "/CN=www.youtube.com/O=Google inc./
C=US" -passout -pass:bilibili -config lab2_openssl.cnf -addext "subjectAltName =
 DNS:www.youtube.com, DNS:www.yt.com, DNS:www.ytb.com"
Invalid password argument "-pass:bilibili"
Error getting passwords
[02/10/23]seed@VM:~/.../Lab_2$ openssl req -newkey rsa:2048 -sha256 -keyout yout
ube-server.key -out youtube-server.csr -subj "/CN=www.youtube.com/O=Google inc./
C=US" -passout pass:bilibili -config lab2_openssl.cnf -addext "subjectAltName =
DNS:www.youtube.com, DNS:www.yt.com, DNS:www.ytb.com"
Generating a RSA private key
......+++++
.......................+++++
writing new private key to 'youtube-server.key'
-----
[02/10/23]seed@VM:~/.../Lab_2$
```

Then, sign the dummy csr using my own CA.

```
seed@VM: ~/.../Lab_2
[02/10/23]seed@VM:~/.../Lab_2$ openssl ca -config lab2_openssl.cnf -policy policy_anything -md sh
a256 -days 3650 -in youtube-server.csr -out youtube-server.crt -batch -cert ca.crt -keyfile ca.ke
y
Using configuration from lab2_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: Feb 11 02:14:10 2023 GMT
            Not After : Feb  8 02:14:10 2033 GMT
        Subject:
            countryName               = US
            organizationName          = Google inc.
            commonName                = www.youtube.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                49:9C:23:89:37:6A:D7:25:71:22:DA:32:F0:BF:7B:2D:D8:F0:4D:70
            X509v3 Authority Key Identifier:
                keyid:FC:B4:1C:C5:E9:91:80:94:98:48:63:73:B3:C9:6D:A8:6E:1A:97:0E

            X509v3 Subject Alternative Name:
                DNS:www.youtube.com, DNS:www.yt.com, DNS:www.ytb.com
Certificate is to be certified until Feb  8 02:14:10 2033 GMT (3650 days)

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

Next, modify Dockerfile and ssl configuration with its CA & key path to the dummy CA & key.

*Maybe alter the /etc/apache2/sites-available/000-default.conf. In 000-default.conf, add entry virtual host 443 just like the given configuration from the lab shown in task4. But this time, the server name will be www.youtube.com. I did it yet not sure about if this is

the crucial part.

```
FROM handsonsecurity/seed-server:apache-php

ARG WWWDIR=/var/www/bank32

COPY ./index.html ./index_red.html $WWWDIR/
COPY ./bank32_apache_ssl.conf /etc/apache2/sites-available
COPY ./certs/youtube-server.crt ./certs/youtube-server.key  /certs/

RUN  chmod 400 /certs/youtube-server.key \
     && chmod 644 $WWWDIR/index.html \
     && chmod 644 $WWWDIR/index_red.html \
     && a2ensite bank32_apache_ssl

CMD  tail -f /dev/null
```

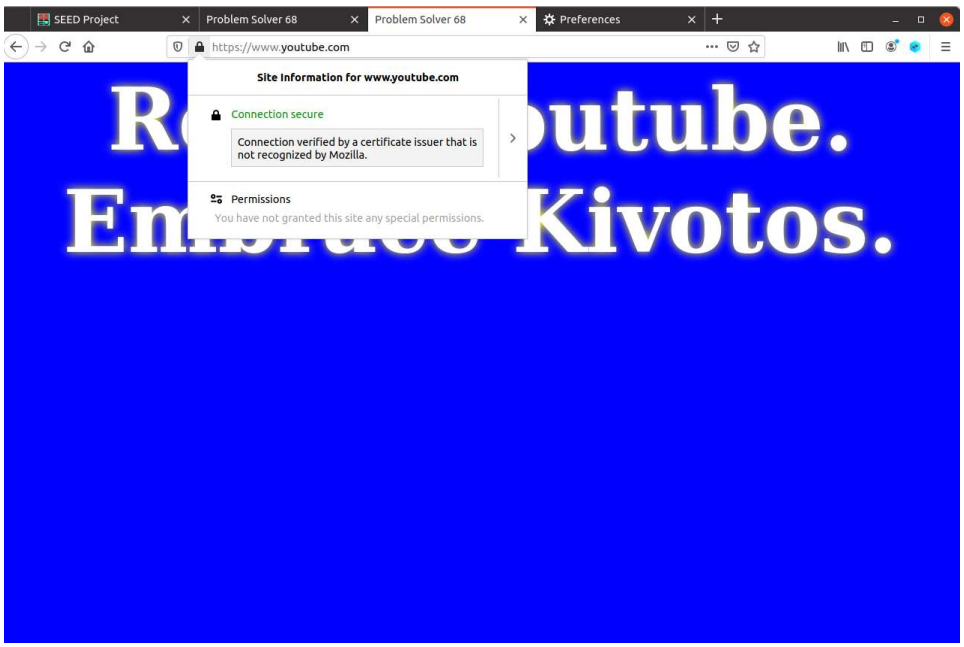
Open bank32_apache_ssl.conf
~/Desktop/Lab_2/image_www

```
<VirtualHost *:443>
    DocumentRoot /var/www/bank32
    ServerName www.youtube.com
    ServerAlias www.yt.com
    ServerAlias www.ytb.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/youtube-server.crt
    SSLCertificateKeyFile /certs/youtube-server.key
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot /var/www/bank32
    ServerName www.youtube.com
    DirectoryIndex index_red.html
</VirtualHost>

# Set the following gloal entry to suppress an annoying warning message
ServerName localhost
```

Finally, do $docker-compose build and ‘up’ the docker so that new configuration will be utilized. Enable apache2 service. This time the website will be your own but impersonating www.youtube.com, and the browser will not raise awareness.

Definitely Youtube


SEED Project
Problem Solver 68
Problem Solver 68
Preferences
https://www.youtube.com
Reject Youtube.
Embrace Kivotos.


SEED Project
Problem Solver 68
Problem Solver 68
Preferences
https://www.youtube.com
Site Information for www.youtube.com
Connection secure
Connection verified by a certificate issuer that is not recognized by Mozilla.
Permissions
You have not granted this site any special permissions.