Applied Cryptography Lab-06 Manual

Submitted by: Mahika Gupta
SRN: PES1UG20CS243
Date: 03/11/2022

Task 1: Becoming a certificate authority (CA)

Firstly, copy the /usr/lib/ssl/openssl.cnf file to your working directory

```
PES1UG20CS243:Mahika:~/.../pki_lab
$>cp /usr/lib/ssl/openssl.cnf .
PES1UG20CS243:Mahika:~/.../pki_lab
$>ls
Labsetup  openssl.cnf
PES1UG20CS243:Mahika:~/.../pki_lab
$>
```

Then create the following files and directories in the working directory:

```
pki_lab
  -
    demoCA
      -certs (dir)
      -crl (dir)
      -newcerts (dir)
      -index.txt (blank text file)
      -Serial (contains a 4 digit number, no line ending)
```

```
PES1UG20CS243:Mahika:~/.../pki_lab
$>cd demoCA
PES1UG20CS243:Mahika:~/.../demoCA
$>mkdir certs crl newcerts
PES1UG20CS243:Mahika:~/.../demoCA
$>ls
certs  crl  newcerts
PES1UG20CS243:Mahika:~/.../demoCA
$>touch index.txt
PES1UG20CS243:Mahika:~/.../demoCA
$>echo "1000" > serial
```

Creating certificate authority

Command

```
$ openssl req -x509 -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
```

Remember the passphrase, you'll have to use it in later tasks!

```
PES1UG20CS243:Mahika:~/.../pki_lab
$>openssl req -x509 -newkey rsa:4096 -sha256 -days 3650 -keyout ca.key -out ca.c
rt -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'
-----
PES1UG20CS243:Mahika:~/.../pki_lab
$>ls
ca.crt  ca.key  demoCA  Labsetup  openssl.cnf
PES1UG20CS243:Mahika:~/.../pki_lab
$>
```

Certificate Authority is created.

Viewing the contents of files generated

Commands

```
$ openssl x509 -in ca.crt -text -noout
```

```
PES1UG20CS243:Mahika:~/.../pki_lab
$>openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            51:7b:f0:1a:0e:17:7e:10:58:bd:3a:10:79:01:ca:29:3e:77:27:37
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: Nov  3 14:44:26 2022 GMT
            Not After : Oct 31 14:44:26 2032 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:c2:c5:a0:cb:97:9a:c5:89:9d:fc:1d:fe:90:30:
                    fd:08:bb:4f:d6:65:b9:31:30:74:fd:8e:73:ae:a0:
                    9f:e4:85:cf:f8:08:ce:55:90:cc:15:26:f2:f0:4f:
                    b4:e4:67:cd:36:ac:ef:dd:77:d6:ad:4c:db:4f:33:
                    fe:bb:95:da:f9:68:d2:f6:49:e8:90:12:4b:d8:03:
                    ed:8e:ed:14:61:73:98:2f:36:47:66:da:27:c4:ed:
                    87:0d:15:05:15:47:7b:3e:c2:4d:19:51:02:4e:62:
                    09:f4:4e:aa:1b:4d:fb:b5:db:12:36:3d:95:4d:21:
                    dd:f4:81:52:a1:3e:88:fb:c0:b3:d0:7c:17:df:24:
                    39:1d:11:fd:4a:d5:dd:ca:ff:f3:0a:78:9e:28:aa:
                    d4:f3:bc:eb:26:3d:7e:27:33:fe:56:5f:c3:bb:b6:
                    a9:d9:08:71:4e:2b:4c:e3:0f:0c:49:f2:c7:62:84:
                    7f:c8:07:62:bd:9b:1d:bc:1c:cc:19:04:73:00:39:
                    d5:62:67:5b:29:83:eb:88:02:cf:31:e7:27:80:b7:
                    30:17:22:61:b1:0b:45:3c:38:c0:f4:66:83:ae:b8:
                    86:39:b8:f4:ce:74:d7:e0:21:b0:e8:aa:a0:f3:74:
                    99:68:65:e4:19:80:7d:fb:0c:3a:cf:c8:77:6e:85:
                    ff:34:fb:2b:32:35:ef:ef:fd:7a:c8:d3:a1:2b:99:
                    9f:62:b8:85:f9:0a:aa:73:39:fd:9f:8f:34:7d:c5:
                    0a:5e:0f:f2:d5:0e:aa:75:21:4e:19:f3:d1:ec:2a:
                    29:0a:e9:82:a0:ca:b5:75:12:10:50:e4:89:3a:b8:
                    85:db:e0:2c:10:2a:c0:4a:8b:95:eb:64:ed:c0:de:
                    c7:54:d7:92:3b:59:07:fb:69:eb:fc:04:b2:d7:48:
                    a3:a0:ce:be:c7:6d:0d:5a:d4:eb:f4:09:22:41:91:
                    22:97:21:9d:d4:03:6c:a2:07:30:1e:17:3e:f6:2a:
                    8c:a5:79:f5:a2:82:4f:e7:fe:1c:41:c5:55:27:13:
```

```
                    b4:40:9a:54:e8:c4:38:26:0c:38:37:3d:b0:15:ff:
                    cc:d5:b7
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                28:BB:7A:EF:38:BE:45:57:2E:6E:E4:0F:75:39:A4:EB:5F:DA:D8:BD
            X509v3 Authority Key Identifier:
                keyid:28:BB:7A:EF:38:BE:45:57:2E:6E:E4:0F:75:39:A4:EB:5F:DA:D8:BD

            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         60:cc:eb:11:7c:cb:15:82:5a:a8:89:9f:e6:fb:78:ff:1b:c7:
         c9:28:e9:cd:af:07:81:cf:e7:a6:f2:24:ad:bf:e6:fe:2c:89:
         db:44:29:04:85:43:e5:d6:89:d0:0c:28:01:ed:9b:4f:6f:d2:
         d2:a3:d8:f2:63:39:63:7e:93:8c:b6:98:fa:6f:fb:dc:11:88:
         bf:9b:c2:f2:9f:66:0e:f1:69:7e:b5:9c:b7:23:51:de:a0:c4:
         39:8e:90:c7:66:b9:d1:5d:cf:43:b0:27:01:95:8d:59:35:63:
         b2:c6:5a:f8:68:f5:e5:c4:1e:b5:44:56:68:09:2b:a9:e4:b1:
         43:ea:f0:0f:04:e0:01:eb:36:46:b4:ac:3c:6a:ac:e2:c2:f7:
         ee:a2:c7:f9:a6:b9:a8:ea:f7:f8:57:08:d4:65:16:a0:46:03:
         ec:87:cf:9c:91:b4:a8:5a:15:06:d1:b8:84:66:99:c5:c5:d4:
         6b:d0:25:10:73:20:78:cd:5c:3c:bd:ca:f3:78:db:58:fe:c4:
         a2:84:ed:e3:b0:54:e8:3c:f5:50:71:a5:e6:e1:c0:75:cc:09:
         c8:f9:91:30:27:5d:44:73:c6:11:b7:ab:c6:b0:00:0c:f8:3f:
         26:49:2c:25:d2:bf:04:c6:7a:3c:a8:a2:55:78:85:fe:58:3a:
         0a:89:e7:58:65:46:39:6f:0f:93:2f:39:9f:20:23:b9:a0:da:
         e7:a2:a5:42:4c:20:a9:78:06:3a:8b:72:00:08:a3:2f:8e:c9:
         09:93:73:73:94:c6:5a:b2:6a:6a:ca:fe:b6:db:e3:4f:b3:d1:
         84:84:cb:bc:fc:39:d0:8f:f1:5d:a5:cb:8b:30:51:7e:18:0a:
         62:e0:2c:1b:92:93:1f:db:b0:9f:1c:19:2d:87:70:54:79:43:
         59:6a:d0:5a:dd:d9:de:df:66:3e:ce:1a:c1:30:ed:43:1a:42:
         06:4e:24:bb:27:7a:24:ad:94:90:2c:b6:cf:0f:cc:5e:6e:c5:
         80:8f:15:d5:e1:a7:94:fa:73:d6:e5:fd:00:99:f0:22:a2:ab:
         f9:e5:98:be:72:b1:a2:06:d8:66:a2:8c:e9:3a:ea:49:5d:73:
         24:2d:78:1c:a5:c6:f1:89:01:6e:b1:b0:1a:df:4c:52:46:d2:
         43:d8:58:6c:d1:d4:7c:97:aa:ef:8c:0c:14:80:f9:84:c7:0c:
         26:b1:77:86:55:e6:c4:a8:be:dd:e6:58:a2:6f:94:53:24:b6:
         43:28:e2:b1:75:55:05:a5:99:ca:8f:99:54:af:88:26:94:56:
         17:1c:ec:5e:c7:26:6c:84:53:6e:af:fc:e8:53:69:d1:53:91:
         7d:0d:a8:46:e8:b9:2d:13
PES1UG20CS243:Mahika:~/.../pki_lab
$>
```

The certificate

```
$ openssl rsa -in ca.key -text -noout
```

Take a screenshot and note your observations

```
PES1UG20CS243:Mahika:~/.../pki_lab
$>openssl rsa -in ca.key -text -noout
Enter pass phrase for ca.key:
RSA Private-Key: (4096 bit, 2 primes)
modulus:
    00:c2:c5:a0:cb:97:9a:c5:89:9d:fc:1d:fe:90:30:
    fd:08:bb:4f:d6:65:b9:31:30:74:fd:8e:73:ae:a0:
    9f:e4:85:cf:f8:08:ce:55:90:cc:15:26:f2:f0:4f:
    b4:e4:67:cd:36:ac:ef:dd:77:d6:ad:4c:db:4f:33:
    fe:bb:95:da:f9:68:d2:f6:49:e8:90:12:4b:d8:03:
    ed:8e:ed:14:61:73:98:2f:36:47:66:da:27:c4:ed:
    87:0d:15:05:15:47:7b:3e:c2:4d:19:51:02:4e:62:
    09:f4:4e:aa:1b:4d:fb:b5:db:12:36:3d:95:4d:21:
    dd:f4:81:52:a1:3e:88:fb:c0:b3:d0:7c:17:df:24:
    39:1d:11:fd:4a:d5:dd:ca:ff:f3:0a:78:9e:28:aa:
    d4:f3:bc:eb:26:3d:7e:27:33:fe:56:5f:c3:bb:b6:
    a9:d9:08:71:4e:2b:4c:e3:0f:0c:49:f2:c7:62:84:
    7f:c8:07:62:bd:9b:1d:bc:1c:cc:19:04:73:00:39:
    d5:62:67:5b:29:83:eb:88:02:cf:31:e7:27:80:b7:
    30:17:22:61:b1:0b:45:3c:38:c0:f4:66:83:ae:b8:
    86:39:b8:f4:ce:74:d7:e0:21:b0:e8:aa:a0:f3:74:
    99:68:65:e4:19:80:7d:fb:0c:3a:cf:c8:77:6e:85:
    ff:34:fb:2b:32:35:ef:ef:fd:7a:c8:d3:a1:2b:99:
    9f:62:b8:85:f9:0a:aa:73:39:fd:9f:8f:34:7d:c5:
    0a:5e:0f:f2:d5:0e:aa:75:21:4e:19:f3:d1:ec:2a:
    29:0a:e9:82:a0:ca:b5:75:12:10:50:e4:89:3a:b8:
    85:db:e0:2c:10:2a:c0:4a:8b:95:eb:64:ed:c0:de:
    c7:54:d7:92:3b:59:07:fb:69:eb:fc:04:b2:d7:48:
    a3:a0:ce:be:c7:6d:0d:5a:d4:eb:f4:09:22:41:91:
    22:97:21:9d:d4:03:6c:a2:07:30:1e:17:3e:f6:2a:
    8c:a5:79:f5:a2:82:4f:e7:fe:1c:41:c5:55:27:13:
    4e:c8:5e:ce:49:ac:a8:2e:d2:2d:e0:5e:12:dd:a8:
    1b:ef:f5:e7:23:52:bb:c4:97:3b:6d:e0:ac:21:98:
    a7:0c:ba:90:77:c5:f2:20:dc:96:bc:86:2b:26:21:
    a8:a6:15:7a:c5:6a:ce:d3:28:a7:8b:b3:e9:2f:ec:
    ea:32:4a:3d:ec:17:67:1b:98:5f:60:69:eb:68:0a:
    d5:86:5f:5a:99:06:57:1e:17:3f:35:b1:59:a9:38:
    f5:f4:71:8e:7c:61:26:0e:be:b6:aa:32:44:3c:c8:
    b4:40:9a:54:e8:c4:38:26:0c:38:37:3d:b0:15:ff:
    cc:d5:b7
publicExponent: 65537 (0x10001)
privateExponent:
    00:9f:ed:0e:1e:9d:99:23:e1:df:ab:08:25:e1:d7:
```

```
publicExponent: 65537 (0x10001)
privateExponent:
    00:9f:ed:0e:1e:9d:99:23:e1:df:ab:08:25:e1:d7:
    97:ac:f7:c0:92:56:6c:3d:8b:80:44:42:17:92:a7:
    a9:22:47:0d:80:a8:1a:63:ff:c4:d3:09:6c:29:0e:
    09:86:12:05:5a:83:9d:60:c7:e9:a9:da:95:a8:ef:
    14:96:8a:71:86:a1:1f:b7:c2:f0:06:7c:3f:72:5b:
    a7:4f:d8:33:07:e1:96:70:0d:ad:8b:32:4d:bd:51:
    1b:b7:0e:2f:62:4d:93:50:f0:d1:c5:9b:d2:bc:f1:
    9b:22:d3:04:b1:ee:d2:63:7c:41:f3:ef:95:0c:04:
    66:ef:40:d0:cc:3d:40:d5:16:61:8f:2a:95:9f:4f:
    6a:e6:07:c3:67:13:3c:4e:56:e3:05:12:0d:2b:6f:
    39:f3:f8:87:4c:9a:e9:5e:df:3e:53:45:c6:bd:f7:
    3a:77:4e:8b:5a:98:0b:45:d5:31:4d:f6:de:e8:71:
    cb:4a:3f:66:40:31:81:b4:d8:20:6d:da:4d:63:3e:
    19:8b:f7:39:cf:58:d6:a8:93:45:f5:bf:cb:9b:d0:
    ce:d7:f0:0f:2f:04:06:11:70:b8:5e:f5:5d:e2:b4:
    f8:e1:a4:90:be:85:0a:4c:aa:dd:4b:ed:ee:c2:78:
    57:0e:75:bb:59:85:3b:ec:4b:1a:6f:4a:37:66:b4:
    f7:da:e6:1b:50:8f:74:d7:6c:18:1e:11:64:f7:a2:
    ff:b8:3d:05:24:34:54:40:f4:6f:6f:eb:18:23:6c:
    49:bf:44:15:0e:90:5d:02:3f:08:b1:a1:d2:16:72:
    8e:ac:42:14:2c:41:94:7a:38:b2:21:4b:c8:cf:28:
    60:48:df:5b:fa:94:4e:58:be:15:75:6c:6f:90:e0:
    eb:74:1b:a8:8e:45:f4:39:cf:03:90:55:60:01:29:
    61:d5:86:3b:6b:2e:c2:93:05:50:cf:b0:56:8e:15:
    f9:82:a8:eb:fa:db:e6:d3:d3:b2:f3:42:9a:62:07:
    b1:d6:f6:a2:52:88:91:c1:fc:9b:36:0a:ae:f8:e9:
    4f:51:84:2b:a1:ea:80:98:15:cd:51:c6:a7:51:78:
    81:7e:41:ad:ab:ef:25:48:8c:3e:cb:81:7c:5e:a4:
    59:70:1a:56:e5:a4:3e:37:bf:fb:91:7e:51:46:a7:
    24:b3:d2:6e:ad:59:9b:7e:f6:dd:b6:2b:45:8c:62:
    fe:e0:de:86:34:79:f1:42:12:57:41:b5:dc:91:6f:
    ff:c0:2a:de:aa:ae:04:71:9d:f4:d2:6d:c1:fa:48:
    74:3b:ca:e3:c6:57:f8:2f:9e:f1:81:9c:43:0e:90:
    df:dd:58:ab:72:94:77:69:34:b1:de:1c:6c:4b:13:
    ff:eb:81
prime1:
    00:e5:73:e3:f6:61:ce:a8:a9:7a:90:9b:bb:0f:3d:
    0a:b1:de:91:e5:44:a5:43:0c:3b:e1:7c:e2:2e:44:
    cd:cd:d0:35:f8:8d:37:5d:b9:c0:3d:5b:f7:49:10:
    a7:3e:77:6d:06:a3:70:c3:1e:3f:00:b7:89:ac:85:
    b3:77:f6:29:35:ae:79:4f:f8:da:b7:d3:2b:db:21:
    8b:fa:1b:cd:14:0c:bb:b4:40:70:e4:10:03:89:31:
```

```
prime1:
    00:e5:73:e3:f6:61:ce:a8:a9:7a:90:9b:bb:0f:3d:
    0a:b1:de:91:e5:44:a5:43:0c:3b:e1:7c:e2:2e:44:
    cd:cd:d0:35:f8:8d:37:5d:b9:c0:3d:5b:f7:49:10:
    a7:3e:77:6d:06:a3:70:c3:1e:3f:00:b7:89:ac:85:
    b3:77:f6:29:35:ae:79:4f:f8:da:b7:d3:2b:db:21:
    8b:fa:1b:cd:14:0c:bb:b4:40:70:e4:19:03:89:31:
    7a:4d:b9:dc:2e:a8:99:37:01:cc:51:70:20:4f:4e:
    c3:61:ca:da:7c:d1:93:45:64:ae:84:28:07:77:94:
    05:63:18:8a:0f:10:bf:43:d8:4a:20:0b:2b:d3:b1:
    49:46:12:94:ae:ae:b8:0c:f9:62:5a:c9:e2:4c:7a:
    9a:2b:93:2d:09:df:f7:a1:11:2f:66:c1:bd:89:54:
    d7:14:46:15:57:6a:a5:78:3c:d0:9c:8b:89:1a:15:
    83:46:86:31:06:22:2d:fc:1c:bc:ec:c1:d6:5e:8e:
    83:0d:4e:c8:28:26:56:23:86:1c:07:e3:6a:6f:fa:
    29:eb:a5:e0:21:e9:aa:92:fd:3c:7e:fa:0e:7b:16:
    ea:60:e9:ef:d6:02:e0:5e:61:c8:39:9b:dc:16:76:
    a5:77:d8:d3:1d:e0:86:9e:87:8e:dc:74:ae:f3:40:
    4f:11
prime2:
    00:d9:4e:89:82:d5:f8:87:3a:69:ac:fb:01:b6:ef:
    42:40:c8:16:da:d6:cb:3d:7b:7b:91:36:10:5e:84:
    0c:4d:13:54:11:04:34:97:79:8d:dc:1e:f4:27:31:
    8d:34:90:da:2f:e2:eb:a4:14:a2:f0:c4:9a:c2:0e:
    45:86:01:99:c6:01:85:f8:64:52:86:fb:ce:3b:97:
    86:e0:41:ba:cb:02:e6:55:42:f6:46:c0:ba:d4:fd:
    e3:1a:29:6d:e3:4f:b8:76:de:15:fa:13:fc:51:a4:
    84:7b:27:77:28:40:36:a6:35:48:01:64:e4:60:19:
    7e:c4:53:ed:69:4f:e4:84:01:ec:63:f0:16:e0:a8:
    89:fb:d7:67:52:de:f1:a6:4b:80:24:ec:6c:55:cf:
    ec:ad:4a:2c:61:7a:02:ce:96:5e:85:24:b6:fc:59:
    3f:8b:bb:04:bc:6a:9d:5e:21:c7:40:db:f8:2d:72:
    29:cb:d7:7c:2a:ef:8c:98:96:3d:46:a1:ba:73:43:
    98:1c:61:2b:0d:01:a6:be:c5:57:e1:ef:4b:47:8a:
    94:d2:b4:90:08:87:b6:9a:2a:f2:3d:24:5d:c7:90:
    6d:af:e6:7a:b6:df:a1:20:68:36:b8:11:c4:5f:20:
    e6:3d:8f:3b:45:5c:24:cd:c1:02:6f:26:65:8b:58:
    68:47
exponent1:
    42:9f:6c:c0:7c:53:ba:0b:43:a8:3b:5f:8c:24:28:
    37:cf:2d:43:89:b4:06:8c:c5:d2:4a:25:8e:53:b2:
    02:21:83:9a:40:be:a3:bb:2c:83:64:71:9f:c8:73:
    17:23:2c:07:f2:6a:ea:6c:9c:d4:83:76:39:1e:b5:
```

```
exponent1:
    42:9f:6c:c0:7c:53:ba:0b:43:a8:3b:5f:8c:24:28:
    37:cf:2d:43:89:b4:06:8c:c5:d2:4a:25:8e:53:b2:
    02:21:83:9a:40:be:a3:bb:2c:83:64:71:9f:c8:73:
    17:23:2c:07:f2:6a:ea:6c:9c:d4:83:76:39:1e:b5:
    26:8e:d6:16:5d:2b:a2:39:da:9f:e7:73:e3:73:91:
    26:34:ee:4d:f5:08:87:64:f2:a2:78:54:db:7f:ff:
    48:14:40:47:57:f2:ec:d2:db:d5:85:9e:0c:09:0d:
    98:16:83:6c:1c:9a:0b:5b:19:85:0b:ee:67:1d:16:
    97:58:67:b5:ca:22:0e:fb:fd:41:e2:9c:7e:22:0a:
    e9:8a:b9:9b:22:e6:13:f6:51:45:95:3a:dd:03:f8:
    41:d0:c1:12:0d:f2:e3:d4:8e:93:e2:8b:3b:15:e4:
    41:61:bc:0e:9e:cb:9e:e6:e1:97:a2:b8:53:57:8d:
    bf:6b:75:4e:97:9c:0c:88:f7:9e:33:06:20:7c:76:
    b6:e5:7a:1e:96:4b:0a:93:85:0e:11:4d:35:68:48:
    c5:c0:6b:1c:cd:b1:16:6e:eb:22:df:4e:57:15:27:
    46:ae:86:51:f8:91:d7:35:c3:22:5f:0b:ff:85:c1:
    b3:d3:c4:30:f7:a1:7e:e4:53:69:d5:83:7a:e3:e0:
    51
exponent2:
    3d:10:44:b3:ef:4c:97:33:62:de:a8:ea:22:6d:b9:
    40:5a:f9:91:25:2a:97:6c:4b:9c:d2:84:67:0a:d4:
    2a:14:74:5b:13:c3:73:8d:44:bf:c6:32:f5:90:87:
    0d:6e:66:e1:6d:f2:a9:78:e3:10:a5:2e:97:b9:4a:
    f0:0d:23:18:f0:f4:a4:88:0c:68:c1:f9:81:e5:62:
    91:41:e7:2b:84:f5:14:a0:6c:74:15:54:6a:e5:ad:
    1b:7c:e8:d4:27:62:be:84:49:c8:ac:35:0a:fc:1f:
    fe:3b:68:d0:76:ba:e4:99:b4:52:2f:f7:bc:c9:6d:
    45:de:0f:a8:b8:3a:8e:9d:bb:bf:99:87:d4:39:88:
    0c:ac:ca:ec:0e:99:f9:10:de:41:81:ee:2f:6e:ee:
    23:03:e4:d4:bf:64:6a:88:f6:a6:93:5a:98:2e:bc:
    1c:97:c1:0c:f1:28:a7:7a:f6:72:d3:5d:39:e8:0a:
    b6:ad:26:c7:29:e9:68:37:4f:a0:b9:71:9b:52:33:
    3c:46:51:c2:a5:e4:25:57:6f:0a:9e:23:99:46:e7:
    eb:0d:b2:2b:b3:77:2c:7b:44:f6:c9:71:50:d2:d4:
    ff:c8:d4:52:ef:24:67:e6:e0:f9:78:84:a5:f6:a8:
    bc:43:b3:74:1a:20:7d:70:ef:2e:2c:ab:fc:2c:2b:
    a1
coefficient:
    65:a5:66:c7:40:a7:65:09:38:39:98:7e:69:96:c4:
    cf:2b:58:a6:a6:55:44:74:27:8b:48:d7:3c:04:67:
    12:95:8d:3e:ea:56:4e:f3:8b:35:8e:d3:bc:79:6d:
    45:5b:f7:c9:0e:b0:dd:21:36:63:63:ff:2c:9d:b9:
```

```
coefficient:
    65:a5:66:c7:40:a7:65:09:38:39:98:7e:69:96:c4:
    cf:2b:58:a6:a6:55:44:74:27:8b:48:d7:3c:04:67:
    12:95:8d:3e:ea:56:4e:f3:8b:35:8e:d3:bc:79:6d:
    45:5b:f7:c9:0e:b0:dd:21:36:63:63:ff:2c:9d:b9:
    dd:58:a4:84:de:09:2e:61:1e:2e:17:fb:61:f3:34:
    e0:e3:cb:07:46:9d:4f:72:1b:1e:e2:e1:28:87:d2:
    7f:6e:7b:8a:eb:59:ee:95:d7:94:fc:a8:11:9b:2b:
    73:b7:cb:06:62:de:88:20:13:26:5e:a2:31:c5:b0:
    d7:42:9c:ae:af:4b:c5:66:94:9f:53:22:38:b8:ca:
    b9:6d:93:eb:46:0e:ac:80:e4:60:34:95:45:f9:ce:
    9c:c7:38:5a:4c:10:5c:71:35:4a:46:3f:a8:7d:96:
    50:ef:88:4a:62:67:ac:29:0a:72:10:79:33:91:70:
    cc:24:7a:f4:bd:82:e9:a7:0c:a1:4e:45:bf:16:3f:
    3e:ec:d3:ff:b6:f0:2b:b5:b0:65:a4:7c:4d:93:a9:
    b1:3f:42:89:65:82:61:63:48:5d:ca:02:c5:e2:f6:
    e3:63:1a:42:ae:ae:9f:03:34:cc:ec:e3:61:c3:51:
    18:85:89:76:74:d6:fd:ec:fd:01:60:92:64:eb:cf:
    15
PES1UG20CS243:Mahika:~/.../pki_lab
$>
```

The parameters for the CA are described above:

Task 2: Generating a Certificate Request for the web server

Step 1 - Generate a public/private key pair

Command

```
$ openssl req -newkey rsa:2048 -sha256 \
```



```
$ 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"
```

```
PES1UG20CS243:Mahika:~/.../pki_lab
$>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'
-----
PES1UG20CS243:Mahika:~/.../pki_lab
$>ls
ca.crt  ca.key  demoCA  Labsetup  openssl.cnf  server.csr  server.key
PES1UG20CS243:Mahika:~/.../pki_lab
$>
```

Generating a certificate request is done

The keys will be stored in server.key
Again, keep track of the passphrase used.
View the created file using the command:

```
$ openssl req -in server.csr-text -noout
```

```
PES1UG20CS243:Mahika:~/.../pki_lab
$>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:ae:78:85:bf:aa:ba:48:e6:7c:c7:14:ac:9c:07:
                    a0:f8:56:43:44:fd:e6:46:36:1b:85:f5:5a:e5:7d:
                    f8:d4:d8:6c:d1:f9:98:5d:f0:2c:43:82:80:9c:fa:
                    39:97:ea:85:b9:dd:ce:9d:2b:b3:e0:87:4f:ed:21:
                    eb:f2:9f:b7:d0:12:94:75:e7:22:30:2f:f7:6c:f1:
                    3b:0b:c1:6f:e8:cb:c4:0a:80:0f:df:ea:bd:49:3b:
                    f8:b2:54:b0:a8:46:86:f9:60:1e:7e:8d:b3:75:2d:
                    67:f4:5d:31:5c:06:53:72:5e:af:5a:a8:8c:5b:e2:
                    ee:da:62:6f:fd:4b:fb:23:82:38:e9:1e:d7:e0:54:
                    db:ff:ba:77:76:1c:37:02:5a:1f:a2:a8:75:6a:2b:
                    4e:21:3f:f3:d8:18:a6:65:41:d3:04:e2:0b:9f:c9:
                    87:ea:6a:a7:24:6e:2c:5e:13:25:6c:58:f0:20:3f:
                    37:fd:48:5b:f7:0a:4f:15:e0:32:28:35:54:b5:95:
                    8b:83:da:c3:25:5e:06:fe:aa:c6:5c:f5:da:7b:cf:
                    1c:48:f4:8e:a5:dc:7d:11:27:fd:62:6e:3d:62:51:
                    e1:f9:9e:a7:58:2e:90:d2:74:21:35:06:76:47:77:
                    b2:16:4a:72:25:2b:ea:cc:34:74:d3:b9:91:4b:d0:
                    f7:43
                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
         0f:1b:72:74:e9:01:0f:69:d1:25:1b:22:88:bf:2b:f3:9a:5e:
         0c:bd:0d:be:6e:72:a7:1d:4d:3c:00:71:b1:f4:50:3b:9e:e7:
         27:ab:2f:5f:79:3b:3f:41:9e:c3:92:1e:6f:59:25:6c:03:7d:
         b4:d3:e6:9d:b6:62:57:73:9a:67:d1:41:27:69:72:29:f9:41:
         13:1f:e2:83:b9:54:17:ca:d9:76:b9:fc:f0:ee:0e:41:75:2c:
         57:61:99:a4:a2:40:c7:61:2a:6e:2b:94:8c:86:35:39:0e:e0:
         c5:ad:d5:37:6b:65:a3:34:38:64:91:cf:96:4e:8e:42:89:9e:
         48:3a:9e:b9:70:e8:d5:e2:b7:cf:16:fe:18:d0:dc:e9:99:c5:
         91:05:9d:07:46:bf:94:0d:7a:10:cb:95:d1:07:32:f3:f2:40:
         6f:20:c1:31:e1:7f:a4:de:ba:3f:4b:48:b2:09:3a:30:0b:8d:
```

```
    Signature Algorithm: sha256WithRSAEncryption
         0f:1b:72:74:e9:01:0f:69:d1:25:1b:22:88:bf:2b:f3:9a:5e:
         0c:bd:0d:be:6e:72:a7:1d:4d:3c:00:71:b1:f4:50:3b:9e:e7:
         27:ab:2f:5f:79:3b:3f:41:9e:c3:92:1e:6f:59:25:6c:03:7d:
         b4:d3:e6:9d:b6:62:57:73:9a:67:d1:41:27:69:72:29:f9:41:
         13:1f:e2:83:b9:54:17:ca:d9:76:b9:fc:f0:ee:0e:41:75:2c:
         57:61:99:a4:a2:40:c7:61:2a:6e:2b:94:8c:86:35:39:0e:e0:
         c5:ad:d5:37:6b:65:a3:34:38:64:91:cf:96:4e:8e:42:89:9e:
         48:3a:9e:b9:70:e8:d5:e2:b7:cf:16:fe:18:d0:dc:e9:99:c5:
         91:05:9d:07:46:bf:94:0d:7a:10:cb:95:d1:07:32:f3:f2:40:
         6f:20:c1:31:e1:7f:a4:de:ba:3f:4b:48:b2:09:3a:30:0b:8d:
         9e:ed:37:4d:b5:1f:05:0e:d5:0d:5f:8b:68:fe:23:f4:8c:97:
         b7:56:57:c7:7e:c6:f0:5c:42:84:48:cf:1a:42:8c:3c:fc:88:
         b8:46:bb:19:dd:c2:51:4e:ab:34:72:37:c0:d2:d0:43:7c:31:
         26:dc:ee:62:23:13:aa:39:25:39:db:b5:e6:60:1d:37:4c:b9:
         15:83:c2:3b
PES1UG20CS243:Mahika:~/.../pki_lab
$>
```

$ openssl rsa -in server.key -text -noout

```
PES1UG20CS243:Mahika:~/.../pki_lab
$>openssl rsa -in server.key -text -noout
Enter pass phrase for server.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
    00:ae:78:85:bf:aa:ba:48:e6:7c:c7:14:ac:9c:07:
    a0:f8:56:43:44:fd:e6:46:36:1b:85:f5:5a:e5:7d:
    f8:d4:d8:6c:d1:f9:98:5d:f0:2c:43:82:80:9c:fa:
    39:97:ea:85:b9:dd:ce:9d:2b:b3:e0:87:4f:ed:21:
    eb:f2:9f:b7:d0:12:94:75:e7:22:30:2f:f7:6c:f1:
    3b:0b:c1:6f:e8:cb:c4:0a:80:0f:df:ea:bd:49:3b:
    f8:b2:54:b0:a8:46:86:f9:60:1e:7e:8d:b3:75:2d:
    67:f4:5d:31:5c:06:53:72:5e:af:5a:a8:8c:5b:e2:
    ee:da:62:6f:fd:4b:fb:23:82:38:e9:1e:d7:e0:54:
    db:ff:ba:77:76:1c:37:02:5a:1f:a2:a8:75:6a:2b:
    4e:21:3f:f3:d8:18:a6:65:41:d3:04:e2:0b:9f:c9:
    87:ea:6a:a7:24:6e:2c:5e:13:25:6c:58:f0:20:3f:
    37:fd:48:5b:f7:0a:4f:15:e0:32:28:35:54:b5:95:
    8b:83:da:c3:25:5e:06:fe:aa:c6:5c:f5:da:7b:cf:
    1c:48:f4:8e:a5:dc:7d:11:27:fd:62:6e:3d:62:51:
    e1:f9:9e:a7:58:2e:90:d2:74:21:35:06:76:47:77:
    b2:16:4a:72:25:2b:ea:cc:34:74:d3:b9:91:4b:d0:
    f7:43
publicExponent: 65537 (0x10001)
privateExponent:
    00:93:4a:3e:27:ac:1b:2d:f6:1f:3a:f6:52:2e:3b:
    26:82:e0:58:54:03:41:06:df:20:e7:3b:56:2c:4d:
    e7:e6:d0:7b:35:dc:cf:eb:e6:19:88:38:c1:19:45:
    09:a0:1d:a6:1d:5e:8a:d2:17:15:f9:24:62:ae:5f:
    a7:d0:a1:53:cd:7e:12:05:63:46:72:85:dc:0d:05:
    ae:02:63:a0:75:58:a8:bc:f0:95:f6:44:36:de:7f:
    99:99:fb:73:53:ec:8e:80:32:cc:2b:ac:b6:e6:e2:
    99:53:2b:e5:c2:b9:b8:72:e2:4a:89:6f:a7:66:df:
    33:23:fc:5c:6c:eb:5b:2e:02:99:88:b1:e2:80:c8:
    c8:3a:4e:fc:fa:c1:82:0f:ef:55:10:4b:58:02:ec:
    51:fd:a4:5a:8f:41:39:e7:fe:07:9b:77:17:90:a7:
    b1:41:6f:b3:e5:22:35:b3:6c:98:be:4c:b1:ac:6f:
    79:6f:5a:60:65:07:7d:03:a8:2e:27:c4:2a:72:76:
    34:c8:be:2f:37:b3:67:32:5a:8a:50:12:31:0b:50:
    86:53:25:7c:b6:c9:90:34:2b:25:79:f7:eb:7b:c7:
    4a:c2:3c:af:bb:e9:41:de:b6:b5:a2:d6:71:70:a6:
    4a:ad:42:92:40:0e:45:ab:05:ae:be:7a:d5:40:85:
    f8:21
prime1:
```

```
    4a:ad:42:92:40:0e:45:ab:05:ae:be:7a:d5:40:85:
    f8:21
prime1:
    00:dd:ae:ed:58:06:ae:1a:e4:de:86:fe:74:77:45:
    5d:d2:b5:72:e1:0f:64:43:75:77:d5:8c:6f:97:23:
    54:ab:ac:f3:26:93:a4:f0:95:37:ba:24:a4:ac:e4:
    50:d7:c1:78:e8:3c:a8:eb:c5:b4:da:55:e2:a4:b0:
    93:58:66:a6:eb:0d:b6:c2:6a:ff:2b:ea:c8:ce:3b:
    f7:ce:bc:79:e1:6f:6b:ee:61:42:df:b0:f6:42:f7:
    15:89:3e:f3:37:62:4e:65:79:f5:28:2a:72:f3:4c:
    e0:6f:4c:60:45:a6:d3:8f:6b:cf:62:e7:a2:ed:d4:
    34:0f:7e:22:98:22:46:5d:71
prime2:
    00:c9:7a:9d:17:49:0c:f2:6c:8f:f5:1a:d9:3b:38:
    f5:e4:5d:d7:e4:fe:4b:a0:0a:89:84:ab:a7:63:74:
    65:fc:66:fd:ae:bd:b7:d6:74:48:96:88:d5:b4:70:
    38:a7:26:73:b3:e9:8f:56:d9:cf:68:bd:22:9a:7a:
    60:1d:23:cc:f8:20:e6:b7:13:35:53:e0:d4:54:90:
    c6:4b:c4:46:d4:af:d2:29:12:42:50:e2:13:44:3d:
    ac:ed:cb:f5:56:47:cf:f7:67:78:4b:03:eb:1b:b4:
    af:cd:75:d3:05:1f:a9:ed:4c:be:bc:a0:5a:2f:dd:
    62:9d:70:e6:84:95:1c:15:f3
exponent1:
    47:87:f9:67:ed:07:e2:ff:b4:da:44:63:1a:55:54:
    b7:f7:fa:b0:aa:81:c4:ce:b3:b3:41:94:84:65:4f:
    1d:f2:39:a7:59:fe:df:ee:96:43:c7:2d:27:e8:a8:
    39:66:61:78:36:92:9f:39:75:68:fa:4b:9e:ae:a7:
    6c:df:fa:be:5f:f7:77:f6:84:8e:0c:3d:6d:66:a6:
    48:9c:42:8b:be:a3:4a:11:32:3d:f1:e1:14:ac:9b:
    d3:64:6f:a0:90:65:11:93:6f:ca:dd:1f:a8:68:47:
    07:42:d2:d1:c6:c9:ff:3e:5f:75:df:9e:90:35:67:
    f3:13:d5:5f:d7:b7:72:d1
exponent2:
    00:83:43:2f:df:40:c7:7f:95:3d:00:b9:da:37:1c:
    38:0e:ed:18:bf:e6:f0:cc:36:b1:3b:4f:3e:01:ac:
    8e:d9:2f:1c:2d:61:0a:c9:5b:ff:02:9b:e9:66:e2:
    09:f6:d4:35:63:4c:52:07:8a:65:f7:5d:e9:92:6d:
    11:fb:4a:1c:ba:b7:6c:b8:6f:7a:39:c8:6b:6d:20:
    d9:1f:f9:a3:0f:e3:f0:6e:b3:a7:a2:dc:77:22:e9:
    6f:a5:89:50:b0:42:9e:fa:17:5e:26:b9:49:ce:46:
    1c:97:26:21:31:e0:5c:2b:ee:e9:01:29:13:38:c5:
    e9:fe:9a:d4:84:22:45:27:03
coefficient:
```

```
coefficient:
    40:95:ac:3e:43:ec:63:fa:bf:13:4e:7c:b9:09:ec:
    ea:91:8d:00:11:20:53:96:b1:b3:03:8a:11:92:64:
    d3:46:ea:3c:75:80:fc:9a:57:e9:45:67:bc:26:34:
    ac:af:bc:eb:76:67:8f:6c:37:a6:46:ae:b6:7d:70:
    b9:59:6c:ea:06:ab:ef:8e:76:9f:b2:ed:a8:bb:3c:
    35:75:4b:f9:8f:60:97:b5:57:dc:e0:56:f1:58:77:
    d4:bd:e5:93:31:d5:9e:bd:72:30:4e:b4:d7:e3:b0:
    d8:26:c3:91:dd:20:56:be:8e:2e:be:a1:f4:75:3a:
    07:23:84:fa:c6:a8:b2:72
PES1UG20CS243:Mahika:~/.../pki_lab
$>
```

Task 3: Generating a Certificate for your server

Command

```
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
```

In this MD5 sha256 algorithm is used, it will be valid for 3650 days and server certificate is created:

```
$>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: Nov  3 14:54:39 2022 GMT
            Not After : Oct 31 14:54:39 2032 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:
                AC:7D:63:CA:E6:4E:F7:09:02:1E:2F:4E:60:49:D1:DB:76:32:9B:86
            X509v3 Authority Key Identifier:
                keyid:28:BB:7A:EF:38:BE:45:57:2E:6E:E4:0F:75:39:A4:EB:5F:DA:D8:BD

Certificate is to be certified until Oct 31 14:54:39 2032 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
PES1UG20CS243:Mahika:~/.../pki_lab
$>
```

Viewing the contents of files generated

Command

```
$ openssl x509 -in server.crt -text -noout
```

```
PES1UG20CS243:Mahika:~/.../pki_lab
$>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: Nov  3 14:54:39 2022 GMT
            Not After : Oct 31 14:54:39 2032 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:ae:78:85:bf:aa:ba:48:e6:7c:c7:14:ac:9c:07:
                    a0:f8:56:43:44:fd:e6:46:36:1b:85:f5:5a:e5:7d:
                    f8:d4:d8:6c:d1:f9:98:5d:f0:2c:43:82:80:9c:fa:
                    39:97:ea:85:b9:dd:ce:9d:2b:b3:e0:87:4f:ed:21:
                    eb:f2:9f:b7:d0:12:94:75:e7:22:30:2f:f7:6c:f1:
                    3b:0b:c1:6f:e8:cb:c4:0a:80:0f:df:ea:bd:49:3b:
                    f8:b2:54:b0:a8:46:86:f9:60:1e:7e:8d:b3:75:2d:
                    67:f4:5d:31:5c:06:53:72:5e:af:5a:a8:8c:5b:e2:
                    ee:da:62:6f:fd:4b:fb:23:82:38:e9:1e:d7:e0:54:
                    db:ff:ba:77:76:1c:37:02:5a:1f:a2:a8:75:6a:2b:
                    4e:21:3f:f3:d8:18:a6:65:41:d3:04:e2:0b:9f:c9:
                    87:ea:6a:a7:24:6e:2c:5e:13:25:6c:58:f0:20:3f:
                    37:fd:48:5b:f7:0a:4f:15:e0:32:28:35:54:b5:95:
                    8b:83:da:c3:25:5e:06:fe:aa:c6:5c:f5:da:7b:cf:
                    1c:48:f4:8e:a5:dc:7d:11:27:fd:62:6e:3d:62:51:
                    e1:f9:9e:a7:58:2e:90:d2:74:21:35:06:76:47:77:
                    b2:16:4a:72:25:2b:ea:cc:34:74:d3:b9:91:4b:d0:
                    f7:43
                Exponent: 65537 (0x10001)
```

```
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                AC:7D:63:CA:E6:4E:F7:09:02:1E:2F:4E:60:49:D1:DB:76:32:9B:86
            X509v3 Authority Key Identifier:
                keyid:28:BB:7A:EF:38:BE:45:57:2E:6E:E4:0F:75:39:A4:EB:5F:DA:D8:BD

    Signature Algorithm: sha256WithRSAEncryption
         12:bc:e1:a5:e5:90:f8:68:dd:98:4d:ec:ff:6c:eb:ac:0c:b3:
         88:3c:ad:52:4d:c0:89:9f:9b:0f:94:dd:d2:d4:a0:ac:ea:91:
         44:29:89:f6:61:7c:f4:3b:61:67:0a:65:5e:59:91:96:8c:59:
         4e:ba:e5:2b:dc:36:55:e6:7a:34:f4:9c:f9:fc:a2:92:8f:a1:
         44:e6:12:be:ce:98:8a:e2:ae:ae:f2:bd:fe:73:5a:6c:54:69:
         7e:31:53:5c:11:43:96:ce:5c:3a:de:28:81:d9:20:47:21:8f:
         bb:cb:54:42:42:c8:b9:fd:b8:fc:cc:a5:11:14:40:28:8b:3a:
         98:65:a4:d0:20:dd:6c:15:cf:a0:aa:c1:2a:a4:92:76:f4:ef:
         c4:36:c0:df:92:a3:cb:5b:2e:fe:43:40:ae:11:70:d1:7a:6f:
         1d:97:c3:d8:b6:45:f5:6e:ac:51:b0:89:12:58:10:63:e5:94:
         85:56:3f:f5:64:8b:56:a8:78:5c:4e:5b:05:84:2d:c5:eb:e3:
         f1:f1:e5:f7:37:eb:8c:d6:7b:27:21:f6:2b:e8:21:aa:39:bd:
         2a:f7:59:b6:10:dc:ed:54:54:a5:cc:53:a6:f6:f4:92:3e:7c:
         f9:86:08:b0:7d:c6:6d:6b:f9:41:91:4d:6a:2f:bf:44:9f:77:
         83:b9:c0:1d:5a:93:d6:91:03:ef:62:f9:6a:5b:26:21:af:89:
         fc:8a:35:f6:81:0f:16:55:f7:4e:ef:6e:70:7a:78:15:9c:22:
         b1:a2:be:01:e5:dc:bf:ae:45:ad:63:c1:c3:8d:b5:e2:4b:1c:
         6b:10:6a:af:d3:54:b9:5f:b4:b8:1b:84:a3:3a:5a:45:12:45:
         bc:58:59:1b:fa:41:a1:6b:b0:86:cb:6e:b5:b8:a8:1f:80:99:
         e7:93:1a:6a:e6:82:57:65:dc:c7:10:c1:89:f9:4e:29:41:47:
         1c:2d:07:9d:e5:c0:35:9f:45:76:f9:22:38:3b:9c:14:33:98:
         a5:89:94:69:5b:fb:1e:ae:7b:b0:ec:f6:c6:59:b4:2c:4c:11:
         f9:3b:72:51:ac:70:99:8c:f5:8b:e9:05:a8:2b:c1:45:13:5e:
         b5:15:90:07:e7:2e:e3:81:5e:b9:28:b9:06:7f:5a:b1:fb:a3:
         db:ff:36:09:d9:c2:7b:22:76:75:4a:95:75:ec:87:00:06:43:
         a6:c6:bc:ea:71:ce:46:67:63:35:8b:17:24:4a:d8:ce:81:a4:
         24:1e:79:a9:82:98:37:09:05:23:9a:69:3a:d6:fb:9f:14:24:
         58:52:81:02:68:22:66:00:a5:a2:1f:f3:7b:59:56:f9:b5:8f:
         b6:f8:6a:b4:c6:c1:ae:d6
PES1UG20CS243:Mahika:~/.../pki_lab
$>
```

Task 4: Deploying Certificate in an Apache Based HTTPS Website

Step 1 - Setting up the required files

Copy the files `server.crt`, `server.key` and `ca.crt` to `Labsetup/image_www/certs` and rename them to `bank32.crt`, `bank32.key` and `modelCA.crt` respectively.

Step 2 - Building docker

Step 2 - Building docker

Navigate to Labsetup and run the following commands

Commands

```
$ docker-compose build
$ docker-compose up
```

```
PES1UG20CS243:Mahika:~/.../Labsetup
$>dcbuild
Building web-server
Step 1/7 : FROM handsonsecurity/seed-server:apache-php
apache-php: Pulling from handsonsecurity/seed-server
da7391352a9b: Already exists
14428a6d4bcd: Already exists
2c2d948710f2: Already exists
d801bb9d0b6c: Pull complete
Digest: sha256:fb3b6a03575af14b6a59ada1d7a272a61bc0f2d975d0776dba98eff0948de275
Status: Downloaded newer image for handsonsecurity/seed-server:apache-php
 ---> 2365d0ed3ad9
Step 2/7 : ARG WWWDIR=/var/www/bank32
 ---> Running in 01db3315e64a
Removing intermediate container 01db3315e64a
 ---> ee59e318602a
Step 3/7 : COPY ./index.html ./index_red.html $WWWDIR/
 ---> af5fee9c50b8
Step 4/7 : COPY ./bank32_apache_ssl.conf /etc/apache2/sites-available
 ---> 5b8029607e88
Step 5/7 : COPY ./certs/bank32.crt ./certs/bank32.key  /certs/
 ---> 16d021f1df20
Step 6/7 : RUN  chmod 400 /certs/bank32.key      && chmod 644 $WWWDIR/index.html      && chmod 644 $WWWDIR/index_red.html      && a2ensite
bank32_apache_ssl
 ---> Running in 8d9d27a01780
Enabling site bank32_apache_ssl.
To activate the new configuration, you need to run:
  service apache2 reload
Removing intermediate container 8d9d27a01780
 ---> 78076e3cb435
Step 7/7 : CMD  tail -f /dev/null
 ---> Running in bba7ab1c4749
Removing intermediate container bba7ab1c4749
 ---> b9ec285de95a

Successfully built b9ec285de95a
Successfully tagged seed-image-www-pki:latest
PES1UG20CS243:Mahika:~/.../Labsetup
$>dcup
Creating network "net-10.9.0.0" with the default driver
Creating www-10.9.0.80 ... done
Attaching to www-10.9.0.80
```

```
# in a different terminal
$ dockps
# Note the id of the container
$ docksh <id of container>
# Inside the docker shell
% service apache2 start
```

```
PES1UG20CS243:Mahika:~/.../Labsetup
$>dockps
3c33ccb88d88  www-10.9.0.80
PES1UG20CS243:Mahika:~/.../Labsetup
$>docksh 3c
root@3c33ccb88d88:/# service apache2 start
 * Starting Apache httpd web server apache2
Enter passphrase for SSL/TLS keys for www.bank32.com:443 (RSA):
 *
root@3c33ccb88d88:/#
```

Step 3 - Setting up DNS

Open /etc/hosts in a text editor as root (in the seed vm)
Add the following entry at the end

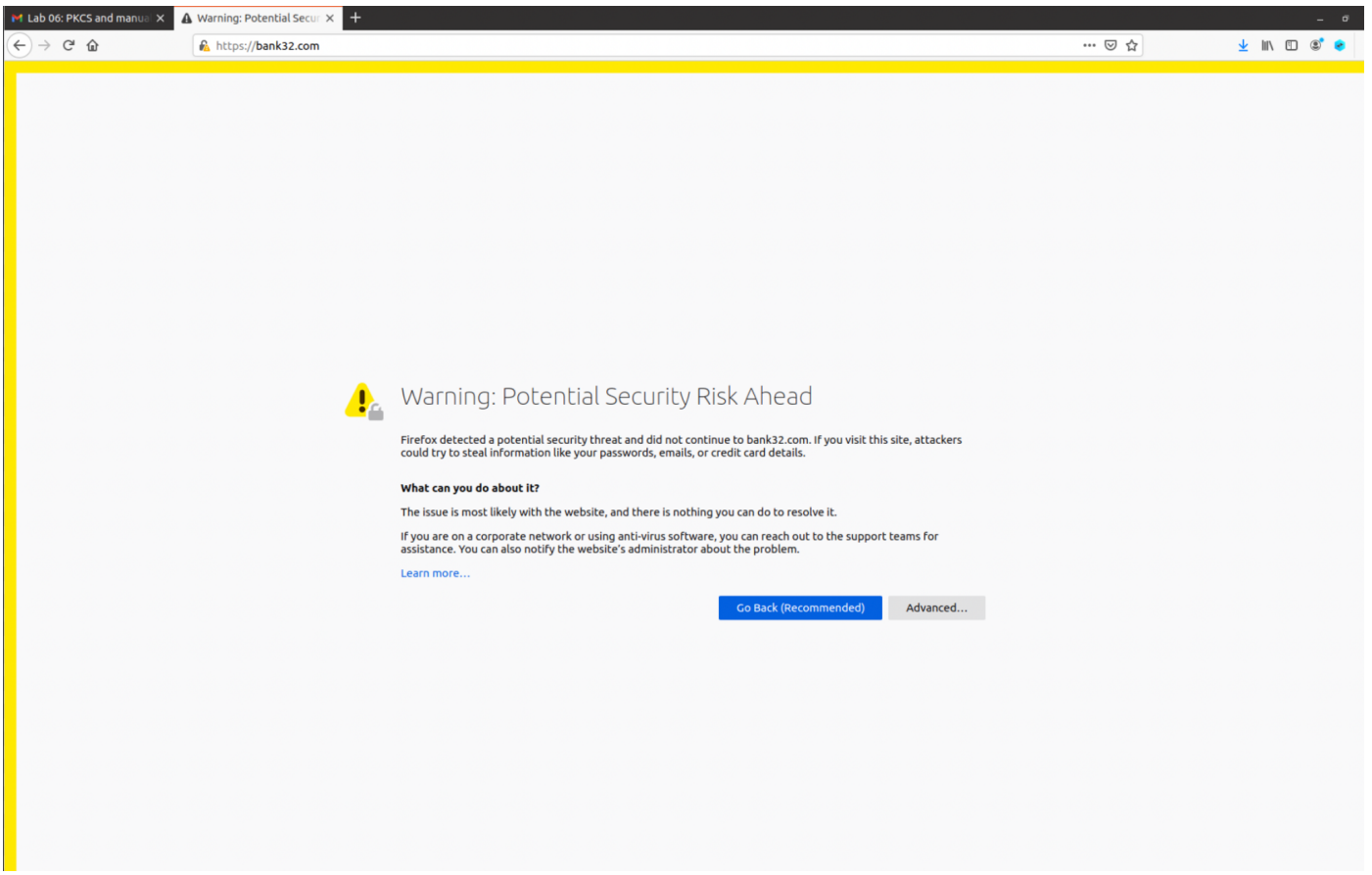
```
10.9.0.80 www.bank32.com
```

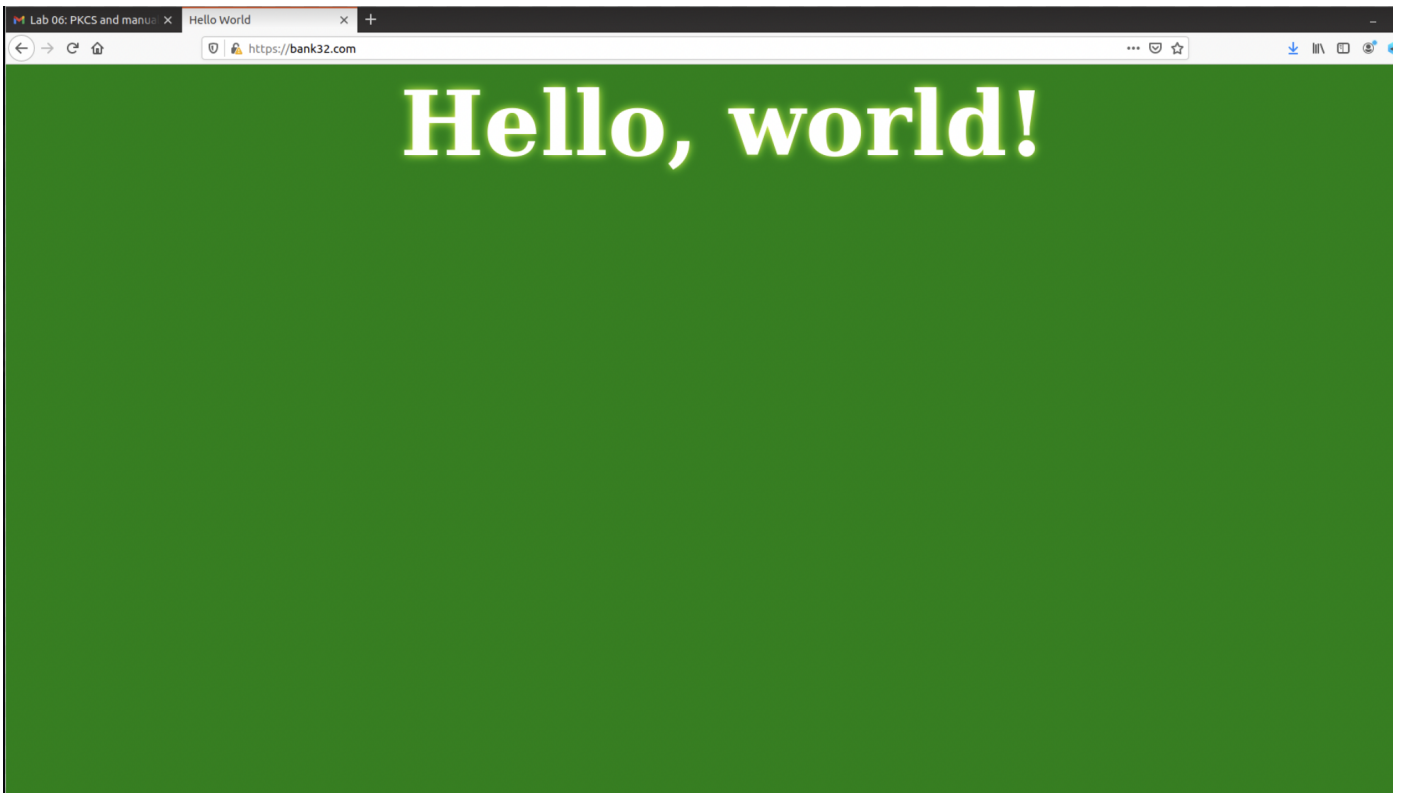
```
  GNU nano 4.8                                                  /etc/hosts
127.0.0.1       localhost
127.0.1.1       VM

# 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

# 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

# For pki lab
10.9.0.80       bank32.com
```

Bank32 is added to the hosts file so it can be accessed.

Step 4

Open firefox and navigate to https://www.bank32.com
Take a screenshot and note your observations



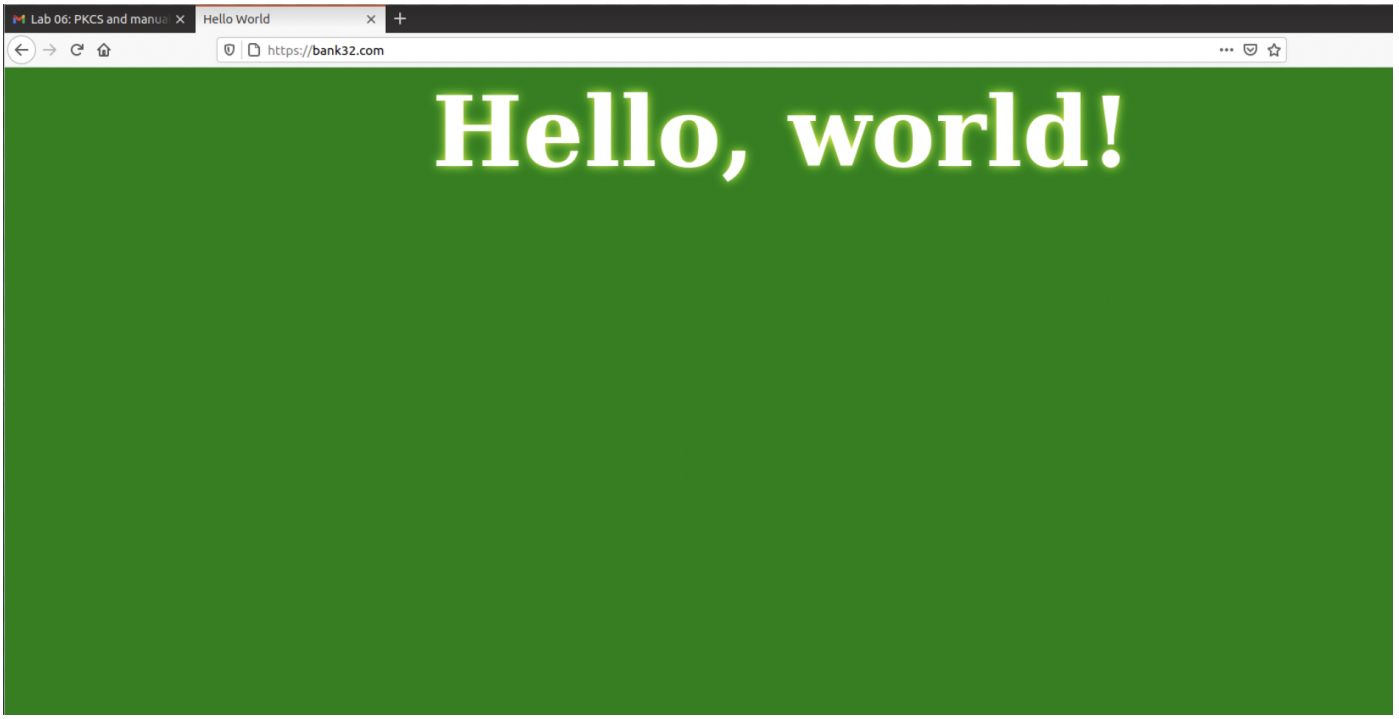


We can see that it is not secure and there is no certificate, so the certificate will have to be imported:

Step 5

1. Go to
2. At the bottom, under certificates, click on "View Certificates", then "import"
3. Select the ca.crt that you generated and import it 4. Ensure to check the "trust this CA to identify websites" 5. Open again

Take a screenshot and note your observations



Once the certificate is imported, we can see the secure lock and the certificate.

Question

Since bank32.com points to 10.9.0.80, if we use https://10.9.0.80 instead, we will be connecting to the same web server. Please do so, describe and explain your observations

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

Step 1: Setting up the malicious website.

In Task 4, we have already set up an HTTPS website. We will use the same Apache server to impersonate . To achievethat, we will follow the instruction in Task 4 to add a VirtualHost entry to Apache's SSL configuration file: the ServerName should be www.example.com, but the rest of the configuration can be the same as that used in Task 4.

Step 2: Becoming the man in the middle

Add the following entry to the victim's /etc/hosts file:

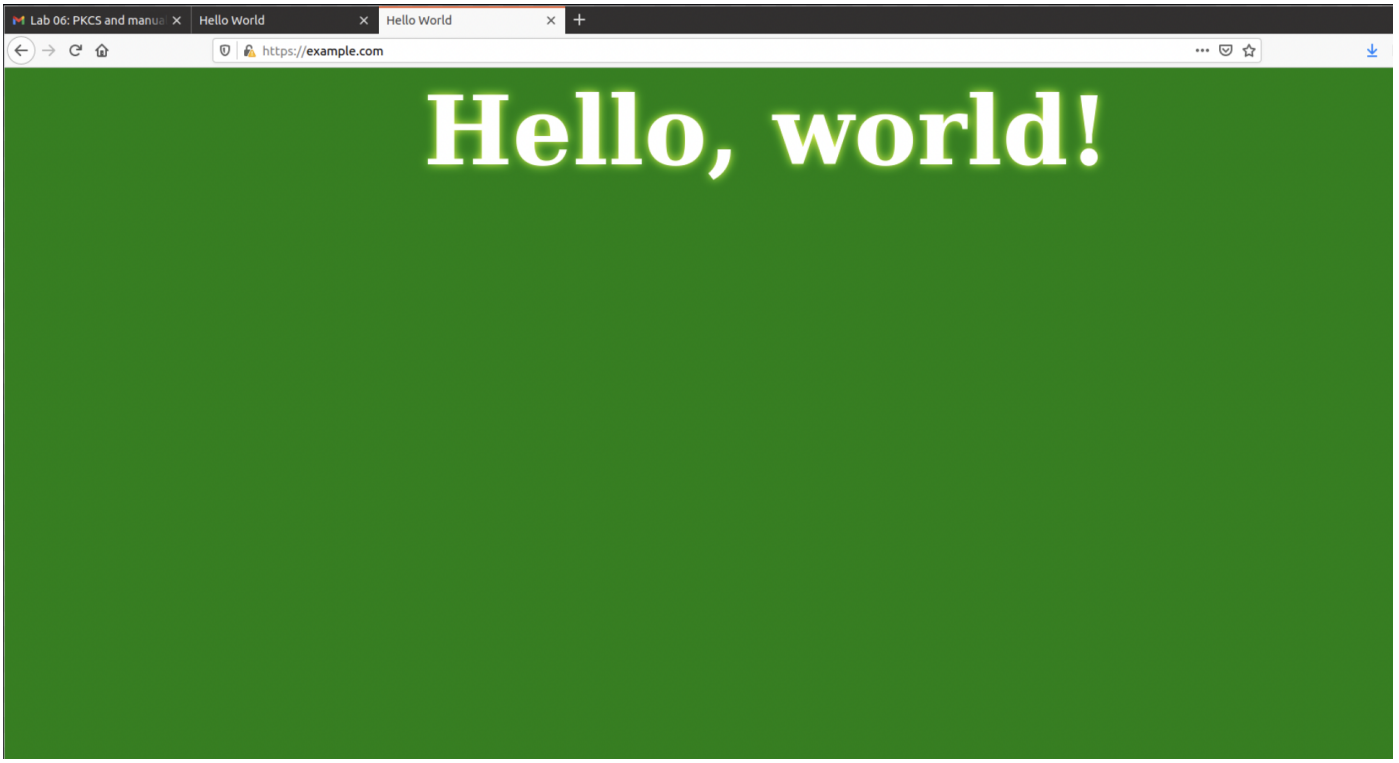
```
10.9.0.80
```

```
  GNU nano 4.8                                                  /etc/hosts
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

# 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

# For pki lab
10.9.0.80       example.com
```

The hostname is changed to example.com

Step 3 -

Open in firefox and note your observations.



It is not secure