Task 1: Becoming a Certificate Authority (CA)

You need to submit a detailed lab report, with screenshots, to describe what you have done and what you have observed. You also need to provide explanation to the observations that are interesting or surprising. Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will not receive credits. In addition, answer any questions if any.

- Copying the configuration file into our directory:
  - ```
    [03/10/24]seed@VM:/$ cp "/usr/lib/ssl/openssl.cnf" "/home/seed/labs/Assignment4"
    ```
    Then uncomment the 'unique_subject' line.
- Preparing the default settings (creating subdirectories and files) to match the configuration file
  - ```
    [03/10/24]seed@VM:~/.../Assignment4$ mkdir demoCA
    [03/10/24]seed@VM:~/.../Assignment4$ cd demoCA
    [03/10/24]seed@VM:~/.../demoCA$ mkdir certs
    [03/10/24]seed@VM:~/.../demoCA$ mkdir crl
    [03/10/24]seed@VM:~/.../demoCA$ mkdir newcerts
    [03/10/24]seed@VM:~/.../demoCA$ touch demoCA/index.txt
    touch: cannot touch 'demoCA/index.txt': No such file or directory
    [03/10/24]seed@VM:~/.../demoCA$ touch index.txt
    [03/10/24]seed@VM:~/.../demoCA$ echo '1001' > serial
    ```
- Generating a self-assigned certificate for the CA
  - ```
    [03/10/24]seed@VM:~/.../demoCA$ openssl req -x509 -newkey rsa:4096 -sha256 -days 3
    650 \
    > -keyout ca.key -out ca.crt
    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]:QA
    State or Province Name (full name) [Some-State]:Doha
    Locality Name (eg, city) []:AlHilal
    Organization Name (eg, company) [Internet Widgits Pty Ltd]:QU
    Organizational Unit Name (eg, section) []:Engineering
    Common Name (e.g. server FQDN or YOUR name) []:Rouaa
    Email Address []:rn2106763@qu.edu.qa
    ```
- Looking at the decoded content of the X509 certificate and the RSA key
  - What part of the certificate indicates this is a CA's certificate?
    i) After running the command responsible for decoding the X509 certificate:

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

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

i) After running the command responsible for decoding the X509 certificate:

(1) Issuer = Subject

(2) Subject Key identifier = Authority Key Identifier

```
        Issuer: C = QA, ST = Doha, L = AlHilal, O = QU, OU = Engineering, CN = R
ouaa, emailAddress = rn2106763@qu.edu.qa
        Validity
            Not Before: Mar 10 07:51:25 2024 GMT
            Not After : Mar  8 07:51:25 2034 GMT
        Subject: C = QA, ST = Doha, L = AlHilal, O = QU, OU = Engineering, CN =
Rouaa, emailAddress = rn2106763@qu.edu.qa
```

```
  X509v3 extensions:
      X509v3 Subject Key Identifier:
          1E:20:F7:B4:15:C8:AE:11:6F:E5:67:07:42:86:04:4A:A0:CD:2B:81
      X509v3 Authority Key Identifier:
          keyid:1E:20:F7:B4:15:C8:AE:11:6F:E5:67:07:42:86:04:4A:A0:CD:2B:8
```

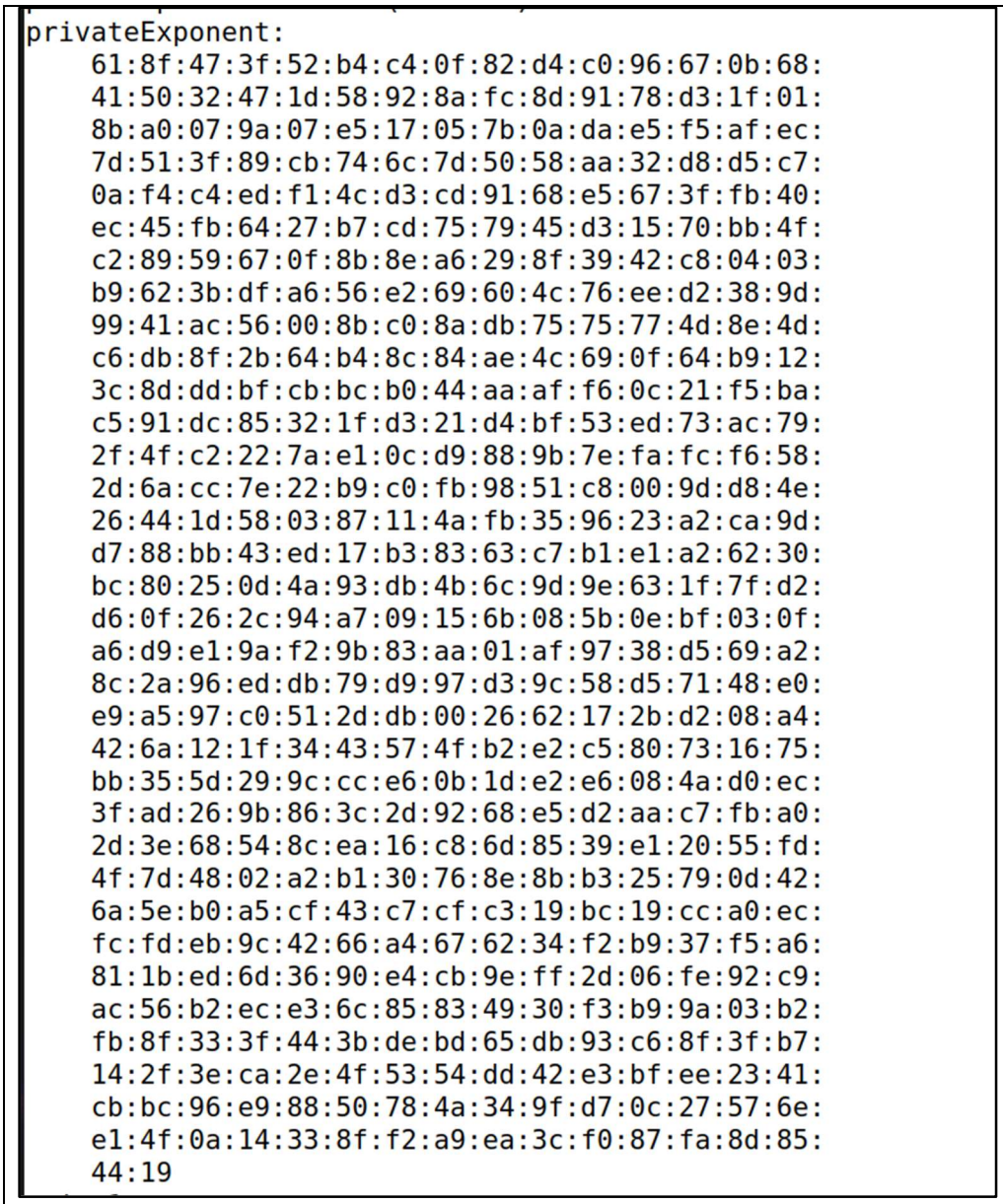
- In the RSA algorithm, we have a public exponent e, a private exponent d, a modulus n, and two secret numbers p and q, such that n = pq. Please identify the values for these elements in your certificate and key files.

  i) After running the command responsible for decoding the RSA key:

  (1) Public Exponent (e)

```
publicExponent: 65537 (0x10001)
```

  (2) Private Exponent (d)


privateExponent:
61:8f:47:3f:52:b4:c4:0f:82:d4:c0:96:67:0b:68:
41:50:32:47:1d:58:92:8a:fc:8d:91:78:d3:1f:01:
8b:a0:07:9a:07:e5:17:05:7b:0a:da:e5:f5:af:ec:
7d:51:3f:89:cb:74:6c:7d:50:58:aa:32:d8:d5:c7:
0a:f4:c4:ed:f1:4c:d3:cd:91:68:e5:67:3f:fb:40:
ec:45:fb:64:27:b7:cd:75:79:45:d3:15:70:bb:4f:
c2:89:59:67:0f:8b:8e:a6:29:8f:39:42:c8:04:03:
b9:62:3b:df:a6:56:e2:69:60:4c:76:ee:d2:38:9d:
99:41:ac:56:00:8b:c0:8a:db:75:75:77:4d:8e:4d:
c6:db:8f:2b:64:b4:8c:84:ae:4c:69:0f:64:b9:12:
3c:8d:dd:bf:cb:bc:b0:44:aa:af:f6:0c:21:f5:ba:
c5:91:dc:85:32:1f:d3:21:d4:bf:53:ed:73:ac:79:
2f:4f:c2:22:7a:e1:0c:d9:88:9b:7e:fa:fc:f6:58:
2d:6a:cc:7e:22:b9:c0:fb:98:51:c8:00:9d:d8:4e:
26:44:1d:58:03:87:11:4a:fb:35:96:23:a2:ca:9d:
d7:88:bb:43:ed:17:b3:83:63:c7:b1:e1:a2:62:30:
bc:80:25:0d:4a:93:db:4b:6c:9d:9e:63:1f:7f:d2:
d6:0f:26:2c:94:a7:09:15:6b:08:5b:0e:bf:03:0f:
a6:d9:e1:9a:f2:9b:83:aa:01:af:97:38:d5:69:a2:
8c:2a:96:ed:db:79:d9:97:d3:9c:58:d5:71:48:e0:
e9:a5:97:c0:51:2d:db:00:26:62:17:2b:d2:08:a4:
42:6a:12:1f:34:43:57:4f:b2:e2:c5:80:73:16:75:
bb:35:5d:29:9c:cc:e6:0b:1d:e2:e6:08:4a:d0:ec:
3f:ad:26:9b:86:3c:2d:92:68:e5:d2:aa:c7:fb:a0:
2d:3e:68:54:8c:ea:16:c8:6d:85:39:e1:20:55:fd:
4f:7d:48:02:a2:b1:30:76:8e:8b:b3:25:79:0d:42:
6a:5e:b0:a5:cf:43:c7:cf:c3:19:bc:19:cc:a0:ec:
fc:fd:eb:9c:42:66:a4:67:62:34:f2:b9:37:f5:a6:
81:1b:ed:6d:36:90:e4:cb:9e:ff:2d:06:fe:92:c9:
ac:56:b2:ec:e3:6c:85:83:49:30:f3:b9:9a:03:b2:
fb:8f:33:3f:44:3b:de:bd:65:db:93:c6:8f:3f:b7:
14:2f:3e:ca:2e:4f:53:54:dd:42:e3:bf:ee:23:41:
cb:bc:96:e9:88:50:78:4a:34:9f:d7:0c:27:57:6e:
e1:4f:0a:14:33:8f:f2:a9:ea:3c:f0:87:fa:8d:85:
44:19

(3) A modulus n

```
modulus:
    00:cf:1e:81:fc:aa:77:e7:7d:18:bb:3f:5d:eb:f2:
    42:e1:23:46:3c:11:f9:ed:c0:89:22:90:94:a5:53:
    1d:cb:09:d4:32:9d:86:05:18:b6:93:f5:db:37:c2:
    95:ad:f2:ce:0d:75:8f:a5:eb:c5:bb:fc:94:4d:18:
    6e:00:98:74:63:3b:e9:f3:3f:b7:35:94:18:42:7f:
    05:49:72:eb:5e:59:3b:09:c7:90:a3:4e:3a:83:43:
    ec:25:4b:37:2f:18:38:60:58:09:dd:07:10:c7:59:
    93:bd:81:f5:91:0f:65:5c:80:21:5a:3c:7f:a7:29:
    94:2c:e8:71:e8:63:a9:4c:90:87:13:8f:eb:97:6c:
    8c:39:98:b8:9f:85:21:fe:84:7a:03:69:4d:05:a8:
    d9:a6:9a:a1:7d:f2:89:54:59:74:5a:90:5c:d0:43:
    e8:68:cb:28:a4:c8:ba:77:76:bc:63:c8:f9:a4:f5:
    e8:0c:69:f6:19:ae:db:e4:06:59:0a:5c:d5:86:0a:
    39:ea:4c:24:e4:f1:38:a3:3f:59:fd:1d:e4:04:c8:
    c9:45:a0:fe:75:66:93:27:ac:61:10:6a:17:97:b1:
    da:80:43:07:84:cd:f5:39:6d:bd:d9:45:06:27:cd:
    de:ea:d3:cf:e1:58:b9:f0:e6:ac:44:7d:97:ca:8d:
    5c:d1:cd:3b:36:f0:07:08:cb:24:8e:6a:77:61:10:
    67:ea:7f:b2:2f:62:c5:2c:27:33:62:da:3f:a4:1f:
    8e:67:90:4a:50:8c:92:4b:4e:d4:e2:8f:23:6e:4d:
    5c:89:bc:41:67:a3:60:39:f1:2d:91:78:67:68:9e:
    66:38:b0:fd:d0:b1:6b:cb:05:b9:ee:59:05:2b:c9:
    90:ae:1f:7e:a2:4f:2d:7e:82:f8:be:90:6c:22:f8:
    23:d7:6e:fe:09:da:c6:a8:c3:6d:f4:9d:44:a4:f1:
    79:7d:ab:be:de:bb:7a:7b:c9:f8:9d:cf:18:a0:35:
    6b:05:47:cf:65:80:0d:21:c4:44:a9:bc:f2:f4:06:
    4a:43:59:66:fa:ec:02:7e:d2:8d:83:f6:0a:6a:67:
    44:08:73:c4:c9:21:c5:17:a2:76:3b:bc:da:06:5a:
    3e:23:53:72:b6:18:27:51:d5:95:92:fe:e5:9a:10:
    fb:2b:e9:f7:28:1e:65:50:cf:aa:60:7d:64:29:03:
    c0:1a:ec:1e:00:70:8e:40:a8:0c:f4:3d:59:4f:82:
    a2:a4:ca:14:7d:54:83:09:30:c0:13:74:2a:94:23:
    0e:0c:5f:6c:66:97:d4:37:a4:38:38:a4:e5:3a:3f:
    5c:b1:cf:61:f4:b3:27:5a:b3:cf:ea:b8:37:45:d3:
    d8:70:d9
```

(4) Secret numbers p and q

```
prime1:
    00:f0:d8:d7:b6:94:ed:6c:ff:12:80:99:d4:1f:b8:
    23:87:75:5a:54:72:3b:17:c0:99:2a:4c:08:d9:4b:
    1a:5e:7e:2c:4e:6a:41:36:56:0b:4b:a2:6f:a3:9d:
    16:ab:87:5c:da:2d:a7:78:89:35:fa:61:3b:ec:2f:
    08:cf:17:e0:da:62:d5:2d:63:f9:4f:33:bc:5a:e0:
    79:a8:de:a0:3a:cd:c6:7c:6f:be:e7:fe:41:5e:6c:
    17:73:48:d6:5f:d3:6c:1e:37:dd:6b:d4:e4:24:e1:
    cd:83:72:29:cc:83:63:36:96:e4:a5:82:9e:dd:7a:
    c5:bf:80:ea:78:73:ce:bb:95:9e:5f:cf:a3:eb:49:
    ee:c5:30:33:9a:5d:f1:08:f6:d5:6a:b1:d7:88:75:
    1d:4c:7e:f9:39:5e:0b:c6:cb:2e:2d:03:3c:87:8a:
    6d:a7:06:13:da:8d:66:e4:a4:62:29:98:9e:57:6d:
    01:a1:83:df:db:97:0e:64:96:b9:75:4f:47:aa:f4:
    f6:5e:86:ef:f8:59:6e:25:b8:3c:b5:52:96:e9:01:
    82:dd:58:32:07:fa:6a:cc:99:b9:2e:d0:dc:7e:0b:
    59:84:e2:9d:3a:aa:25:c0:fa:0e:a1:f1:d3:c2:ba:
    c0:f7:bf:47:c0:83:cc:e0:fe:51:76:5d:9a:c4:01:
    36:1b
prime2:
    00:dc:26:6e:fd:93:19:17:7d:8e:4e:6a:50:0a:06:
    27:fb:b3:43:83:cb:ea:54:9d:b7:05:59:05:d1:26:
    d7:97:b5:15:71:ec:38:fc:70:68:ee:9a:80:a8:b3:
    89:5e:6f:85:fe:45:32:46:35:c7:56:09:6a:57:5f:
    94:bc:b9:a8:bb:e5:74:33:e7:57:e7:02:df:4f:d5:
    07:24:68:1f:74:00:b1:46:68:3d:e7:98:1e:31:c8:
    76:9c:f7:d1:f7:4f:e2:d8:79:46:fa:e5:d6:79:2a:
    4c:5f:84:53:c3:a3:5b:7e:a1:6a:49:32:02:25:9e:
    d5:58:93:be:3a:a2:6f:d8:69:3b:ae:32:f3:99:de:
    9d:61:85:0a:d2:c8:45:3e:d7:80:b9:86:3e:a0:2a:
    d6:4c:34:3a:d5:eb:29:43:a7:c4:29:9a:7e:66:97:
    b9:2b:66:5f:1a:12:e6:24:c6:2d:6e:d5:3c:ec:c9:
    55:62:d8:20:6b:54:54:90:89:b9:55:a5:f0:d7:fb:
    19:1f:c0:c6:01:0f:dc:7f:f0:08:a3:6c:b6:ec:34:
    f1:e8:11:1e:39:fe:b6:34:e8:ac:29:a1:05:27:fc:
    fc:24:81:46:f0:c6:e1:ea:90:ed:20:d2:57:83:6e:
    4d:ac:4d:59:39:ec:43:85:52:ad:8d:3d:bc:ba:d2:
    f4:1b
```

Task 2: Generating a Certificate Request for Your Web Server

You need to submit a detailed lab report, with screenshots, to describe what you have done and what you have observed. You also need to provide explanation to the observations that are interesting or surprising. Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will not receive credits. In addition, answer any questions if any.

- Generating a Certificate Signing Request, with two alternative names:

```
[03/10/24]seed@VM:~/.../demoCA$ -addext "subjectAltName = DNS:www.naim2024.com, \
> DNS:www.rouaanaim.com, \
> DNS:www.rouaa.com"
-addext: command not found
[03/10/24]seed@VM:~/.../demoCA$
[03/10/24]seed@VM:~/.../demoCA$ openssl req -newkey rsa:2048 -sha256 \
> -keyout server.key -out server.csr \
> -subj "/CN=www.yourserver.com/O=YourCompany Inc./C=US" \
> -addext "subjectAltName = DNS:www.naim2024.com, DNS:www.rouaanaim.com, DNS:www.r
ouaa.com" \
> -passout pass:dees
Generating a RSA private key
.....................................+++++
.....................................+++++
writing new private key to 'server.key'
-----
```

- Viewing the decoded content of CSR

```
[03/10/24]seed@VM:~/.../demoCA$ openssl req -in server.csr -text -noout
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = www.yourserver.com, O = YourCompany Inc., C = US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:d3:b3:34:05:71:93:35:8a:e5:75:cb:d4:2d:bb:
                    4d:b0:0e:ca:34:aa:74:de:4f:00:d1:b8:6c:fb:21:
                    43:6f:92:c2:c2:c5:5e:1e:61:82:0e:c8:c6:bc:d5:
                    12:3c:52:37:56:ea:bd:86:20:93:10:fc:11:66:7f:
                    fe:87:60:5c:89:78:a4:3a:67:c4:1d:a8:51:2f:02:
                    fe:3b:f3:9b:02:08:db:48:d0:57:b6:fb:14:16:fd:
                    86:63:62:72:09:65:1f:94:01:9d:a5:24:d9:f3:4c:
                    c2:5e:69:46:0a:88:3b:2d:8e:1a:3e:f8:6a:a7:78:
                    92:23:11:f3:88:df:b3:3e:48:72:2f:7d:b9:c2:3c:
                    c5:ef:c6:13:7e:b9:f4:53:c2:e7:06:b3:77:69:fc:
                    4a:6c:fa:3e:00:8e:61:e8:75:f0:c8:55:87:23:4f:
                    47:4f:ac:0b:98:48:22:94:f1:c4:8d:7d:ae:93:64:
                    74:88:13:43:2c:1c:15:9d:25:dc:9d:98:e1:52:5e:
                    8d:73:89:f1:7d:13:4f:37:93:80:5d:11:63:ad:f6:
                    6b:0a:8a:24:c6:de:b0:3f:a9:0f:99:14:3a:66:d9:
                    6b:20:be:a2:68:32:49:41:72:1c:9a:ce:95:36:8d:
                    a8:95:52:cb:fd:0f:b8:7b:05:c7:d7:d1:b7:11:17:
                    cd:af
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Subject Alternative Name:
                DNS:www.naim2024.com, DNS:www.rouaanaim.com, DNS:www.rouaa.com
    Signature Algorithm: sha256WithRSAEncryption
         a1:4b:7a:bd:d0:39:04:d3:fb:0a:dc:5a:83:40:95:a3:f0:72:
         d2:7b:4b:3f:db:6e:02:2e:e6:33:6b:2a:0f:8b:44:f3:3e:96:
         18:0a:e5:bd:b2:44:55:10:b4:2e:0d:cf:55:28:56:5b:e8:2d:
         13:86:6a:60:fb:b7:df:00:d9:83:83:23:0a:62:28:12:23:89:
         23:d0:85:96:c0:f9:8c:d7:f4:20:c5:4f:af:ac:9f:db:a3:06:
         da:3e:5c:22:23:b9:24:81:3a:50:5d:b2:db:de:a1:8a:d6:b9:
         8a:32:6e:50:ad:eb:04:5e:f7:24:0f:49:70:a0:85:ed:92:73:
         41:9b:cf:89:f1:82:b7:50:48:c1:1b:9e:dc:d6:7e:c8:59:4b:
         50:8d:aa:82:f5:21:1f:86:2e:a3:4c:fd:ef:11:9f:4b:7c:85:
         55:78:62:fd:8e:4c:17:11:31:42:44:90:4d:2b:b5:27:42:a7:
         56:8f:b8:45:ad:65:14:ec:19:7e:c4:2f:cb:95:d9:93:b1:c9:
         3d:ce:9c:1b:39:79:6a:95:0f:ec:22:2c:de:e0:4c:d2:33:8f:
         bb:e7:ba:8c:27:56:fc:10:bb:4b:29:99:ad:c0:0e:3c:bf:d0:
         73:d3:a6:df:a1:05:d9:90:1e:8b:c9:9f:bb:69:24:5a:08:7b:
         fb:13:6d:94
```

- Viewing the decoded content of the private key files

```
[03/10/24]seed@VM:~/.../demoCA$ openssl rsa -in server.key -text -noout
Enter pass phrase for server.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
    00:d3:b3:34:05:71:93:35:8a:e5:75:cb:d4:2d:bb:
    4d:b0:0e:ca:34:aa:74:de:4f:00:d1:b8:6c:fb:21:
    43:6f:92:c2:c2:c5:5e:1e:61:82:0e:c8:c6:bc:d5:
    12:3c:52:37:56:ea:bd:86:20:93:10:fc:11:66:7f:
    fe:87:60:5c:89:78:a4:3a:67:c4:1d:a8:51:2f:02:
    fe:3b:f3:9b:02:08:db:48:d0:57:b6:fb:14:16:fd:
    86:63:62:72:09:65:1f:94:01:9d:a5:24:d9:f3:4c:
    c2:5e:69:46:0a:88:3b:2d:8e:1a:3e:f8:6a:a7:78:
    92:23:11:f3:88:df:b3:3e:48:72:2f:7d:b9:c2:3c:
    c5:ef:c6:13:7e:b9:f4:53:c2:e7:06:b3:77:69:fc:
    4a:6c:fa:3e:00:8e:61:e8:75:f0:c8:55:87:23:4f:
    47:4f:ac:0b:98:48:22:94:f1:c4:8d:7d:ae:93:64:
    74:88:13:43:2c:1c:15:9d:25:dc:9d:98:e1:52:5e:
    8d:73:89:f1:7d:13:4f:37:93:80:5d:11:63:ad:f6:
    6b:0a:8a:24:c6:de:b0:3f:a9:0f:99:14:3a:66:d9:
    6b:20:be:a2:68:32:49:41:72:1c:9a:ce:95:36:8d:
    a8:95:52:cb:fd:0f:b8:7b:05:c7:d7:d1:b7:11:17:
    cd:af
publicExponent: 65537 (0x10001)
privateExponent:
    00:8f:da:24:ce:52:27:da:e9:40:14:f4:65:80:91:
    d7:2f:7c:4d:50:ce:47:4d:cc:d7:5c:aa:fa:7b:07:
    56:60:99:94:78:6f:4f:0e:4b:e9:e9:8b:ea:e7:e3:
    cd:59:69:f0:aa:c2:25:f8:df:67:af:d1:e9:2d:02:
    6a:7d:a9:30:18:45:ff:2a:a4:da:31:e0:ef:11:87:
    f2:23:e0:dc:02:dc:eb:cd:25:ad:84:ec:45:f1:7d:
    62:f5:63:ae:e3:cd:70:50:cd:6c:47:0c:ac:81:54:
    36:7b:9b:03:7a:22:aa:3b:c1:64:fa:47:29:8a:15:
    37:10:57:a1:69:ef:c0:47:e0:0c:2d:62:55:8c:80:
    92:1f:84:06:45:97:15:be:65:b4:dd:e0:14:5d:17:
    88:3d:f1:82:47:d0:4a:b9:ab:07:a3:c0:2a:ce:ed:
    9a:cd:8a:ee:2c:d3:dd:f6:dd:64:39:35:ab:14:56:
    6f:d8:93:90:27:da:d1:8e:39:1d:c5:80:bd:b3:5c:
    b4:e0:fc:3b:27:5a:a3:59:e8:f8:df:c9:98:44:1f:
    6a:c2:8c:d5:f2:9a:c3:b4:08:87:11:7b:3f:0b:51:
    5e:46:41:a6:fe:2e:ce:f4:79:37:38:6d:6c:ce:69:
    ec:72:3f:eb:94:20:99:3d:22:f7:ba:6c:fb:69:55:
    5d:11
prime1:
    00:ed:79:bf:2b:bb:c9:6a:7d:07:cb:b2:00:a4:cc:
    ec:f9:25:e2:b7:77:c1:0e:58:7a:6d:fc:42:a1:7b:
    38:07:ee:2d:69:95:34:6c:f2:e4:0e:ee:f0:13:50:
    bc:1c:0f:b2:37:ae:33:d0:7c:92:8a:2f:c4:ba:28:
    d4:40:21:7d:44:c9:fa:9d:51:4c:4b:bc:09:46:ac:
    88:8f:a7:44:12:de:d1:0a:75:77:bb:8c:29:40:20:
```

```
prime1:
    00:ed:79:bf:2b:bb:c9:6a:7d:07:cb:b2:00:a4:cc:
    ec:f9:25:e2:b7:77:c1:0e:58:7a:6d:fc:42:a1:7b:
    38:07:ee:2d:69:95:34:6c:f2:e4:0e:ee:f0:13:50:
    bc:1c:0f:b2:37:ae:33:d0:7c:92:8a:2f:c4:ba:28:
    d4:40:21:7d:44:c9:fa:9d:51:4c:4b:bc:09:46:ac:
    88:8f:a7:44:12:de:d1:0a:75:77:bb:8c:29:40:20:
    f3:e7:df:16:3f:f7:16:0a:53:39:32:c5:f0:ee:97:
    99:b8:a1:51:b3:53:16:ce:a1:b6:fa:86:f9:c5:4a:
    f3:84:e3:0a:11:42:aa:c4:f9
prime2:
    00:e4:36:bb:a8:6c:67:f8:b4:77:2f:05:1a:82:ca:
    1a:41:41:eb:90:bc:f8:c1:af:5f:4d:a1:d4:de:5f:
    02:85:03:3f:98:54:fd:9f:87:ec:f2:2b:fa:bd:2a:
    d0:f4:62:cf:cd:8c:7f:9b:86:87:e5:f8:af:70:9a:
    60:45:24:c1:79:1c:11:74:dd:1b:b0:a4:e9:aa:3d:
    a7:69:43:a9:74:b7:59:4d:f7:fd:4e:26:b1:a7:55:
    fd:75:b6:14:ce:f7:f4:93:97:e7:ab:e9:fc:9e:35:
    0e:8c:a1:5d:59:aa:89:b8:0a:38:a9:9b:38:67:95:
    fa:f9:97:49:85:0f:91:d9:e7
exponent1:
    00:b0:f1:c6:40:0f:ec:44:2c:65:62:a1:7f:59:4c:
    58:46:4c:b4:61:80:19:99:56:d3:e2:9f:d4:05:fe:
    8a:01:5e:b6:f7:b4:f5:1b:38:e0:35:40:54:22:10:
    46:19:a2:98:68:64:a4:b6:f4:1b:3c:5b:db:79:da:
    72:4c:56:a7:c0:59:bf:22:f9:30:a0:3d:bb:ab:ad:
    63:13:a6:ce:52:41:34:01:57:05:9f:f9:0f:c3:78:
    ca:44:3b:35:98:f3:c2:b8:6e:ca:6f:ca:8d:7b:39:
    fa:90:57:a3:48:ba:e0:83:96:7b:80:b0:91:eb:2f:
    ad:c3:96:68:29:f4:42:ca:01
exponent2:
    14:95:57:31:a6:ad:6e:02:20:e9:cd:c5:09:5c:df:
    27:59:a1:bc:89:3e:ca:81:5d:d0:2b:b3:7e:67:05:
    5c:27:e1:d9:84:78:e7:a5:a3:da:67:db:12:aa:c4:
    f3:f5:e1:96:41:80:d4:ef:3a:5c:a4:a4:76:3c:86:
    48:56:3b:59:08:0e:0f:03:4e:57:0d:58:c1:f1:13:
    a3:6b:e5:e1:d0:13:ae:f3:9a:16:2d:69:42:95:7f:
    e9:d9:05:61:71:7d:ce:be:19:b8:28:bf:8f:29:6b:
    e9:85:38:5d:39:03:78:e4:fb:1d:59:11:aa:4e:1d:
    b7:db:4c:57:43:03:3d:ab
coefficient:
    27:81:63:83:23:c4:b0:dc:c2:7c:fe:5e:21:66:95:
    ea:e0:d0:0b:b9:31:27:ae:3e:aa:2a:5e:7d:53:aa:
    a5:ad:5d:f6:43:e7:f9:43:bc:98:98:94:f8:15:70:
    95:ca:b0:f9:9f:5e:8d:70:c5:c2:95:f7:d7:5c:9a:
    89:d4:4a:d7:a3:13:0b:c8:c5:fa:b3:0b:fd:e7:23:
    0e:e6:e7:1c:11:ed:4c:53:7f:5c:ee:cb:2c:0b:2e:
    08:80:dd:d3:2f:57:eb:b4:ef:43:df:bf:b2:e1:5f:
    4c:de:55:bf:17:a4:66:51:d9:01:a4:37:17:28:a0:
    b6:2d:5b:1b:aa:4f:41:f0
```

Task 3: Generating a Certificate for your server

You need to submit a detailed lab report, with screenshots, to describe what you have done and what you have observed. You also need to provide explanation to the observations that are interesting or surprising. Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will not receive credits. In addition, answer any questions if any.

- **Turning the certificate signing request into X509 Certificate**

```
[03/10/24]seed@VM:~/.../Assignment4$ openssl ca -config openssl.cnf -policy poli
cy_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: 4097 (0x1001)
        Validity
            Not Before: Mar 10 09:42:01 2024 GMT
            Not After : Mar  8 09:42:01 2034 GMT
        Subject:
            countryName               = US
            organizationName          = YourCompany Inc.
            commonName                = www.yourserver.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                F2:E5:50:CF:5B:46:C4:3D:61:CA:1A:FF:3F:07:5C:89:FA:BF:F0:97
            X509v3 Authority Key Identifier:
                keyid:1E:20:F7:B4:15:C8:AE:11:6F:E5:67:07:42:86:04:4A:A0:CD:2B:8
1

            X509v3 Subject Alternative Name:
                DNS:www.naim2024.com, DNS:www.rouaanaim.com, DNS:www.rouaa.com
Certificate is to be certified until Mar  8 09:42:01 2034 GMT (3650 days)

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

- **Checking if alternative names are included by running the command: openssl x509 -in server.crt -text -noout**

```
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
            F2:E5:50:CF:5B:46:C4:3D:61:CA:1A:FF:3F:07:5C:89:FA:BF:F0:97
        X509v3 Authority Key Identifier:
            keyid:1E:20:F7:B4:15:C8:AE:11:6F:E5:67:07:42:86:04:4A:A0:CD:2B:8


        X509v3 Subject Alternative Name:
            DNS:www.naim2024.com, DNS:www.rouaanaim.com, DNS:www.rouaa.com
```

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

You need to submit a detailed lab report, with screenshots, to describe what you have done and what you have observed. You also need to provide explanation to the observations that are interesting or surprising. Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will not receive credits. In addition, answer any questions if any.

- **Note: all work is done through the root**
- **Go to /etc/apache2/sites-available and add a new file for our website "ourname_apache_ssl.conf"**
- **Edit the file while referring to the bank32's conf file content:**

```
<VirtualHost *:443>
    DocumentRoot /var/www/gelban2024
    ServerName www.gelban2024.com
    ServerAlias www.gelban2024A.com
    ServerAlias www.gelban2024B.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/server.crt
    SSLCertificateKeyFile /certs/server.key
</VirtualHost>

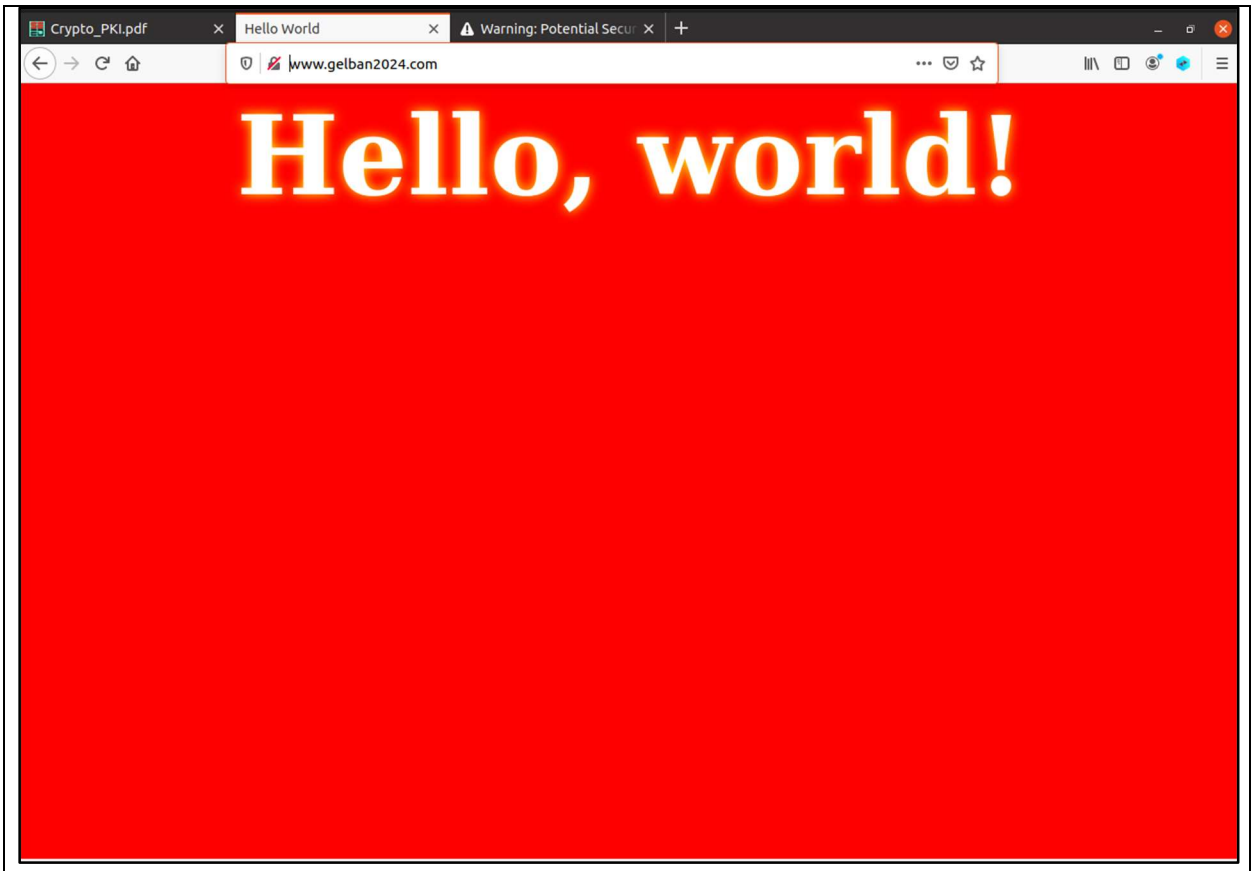
<VirtualHost *:80>
    DocumentRoot /var/www/gelban2024
    ServerName www.gelban2024.com
    DirectoryIndex index_red.html
</VirtualHost>
```

- **We made a directory for our website in /var/www/, then we proceeded to copy the index files in /var/www/bank32/ into our directory.**
- **We copied the server.key and server.cert generated earlier, into the /certs directory**
- **We stopped then started the apache again.**
- **Then we ran those commands:**

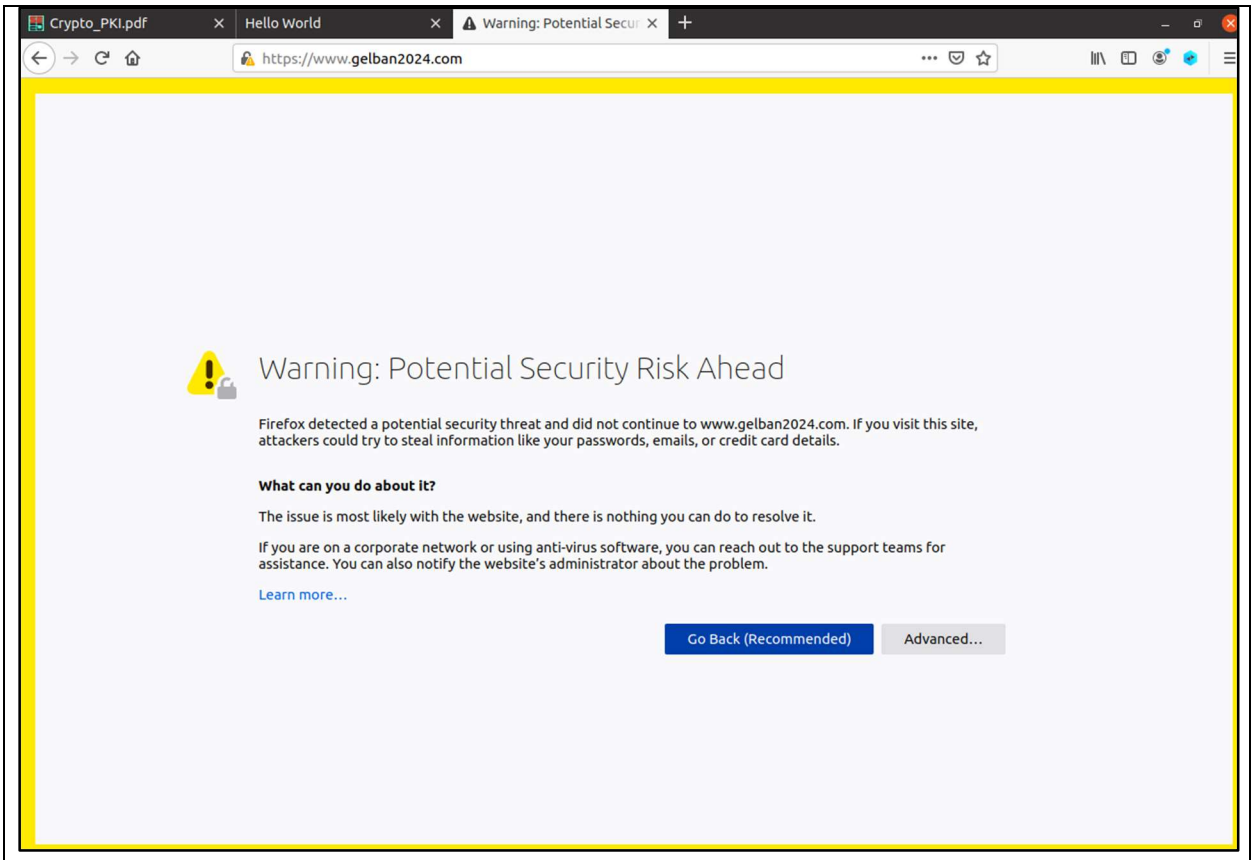
```
# a2enmod ssl                    // Enable the SSL module
# a2ensite bank32_apache_ssl     // Enable the sites described in this file
```

Change this to match our apache's file

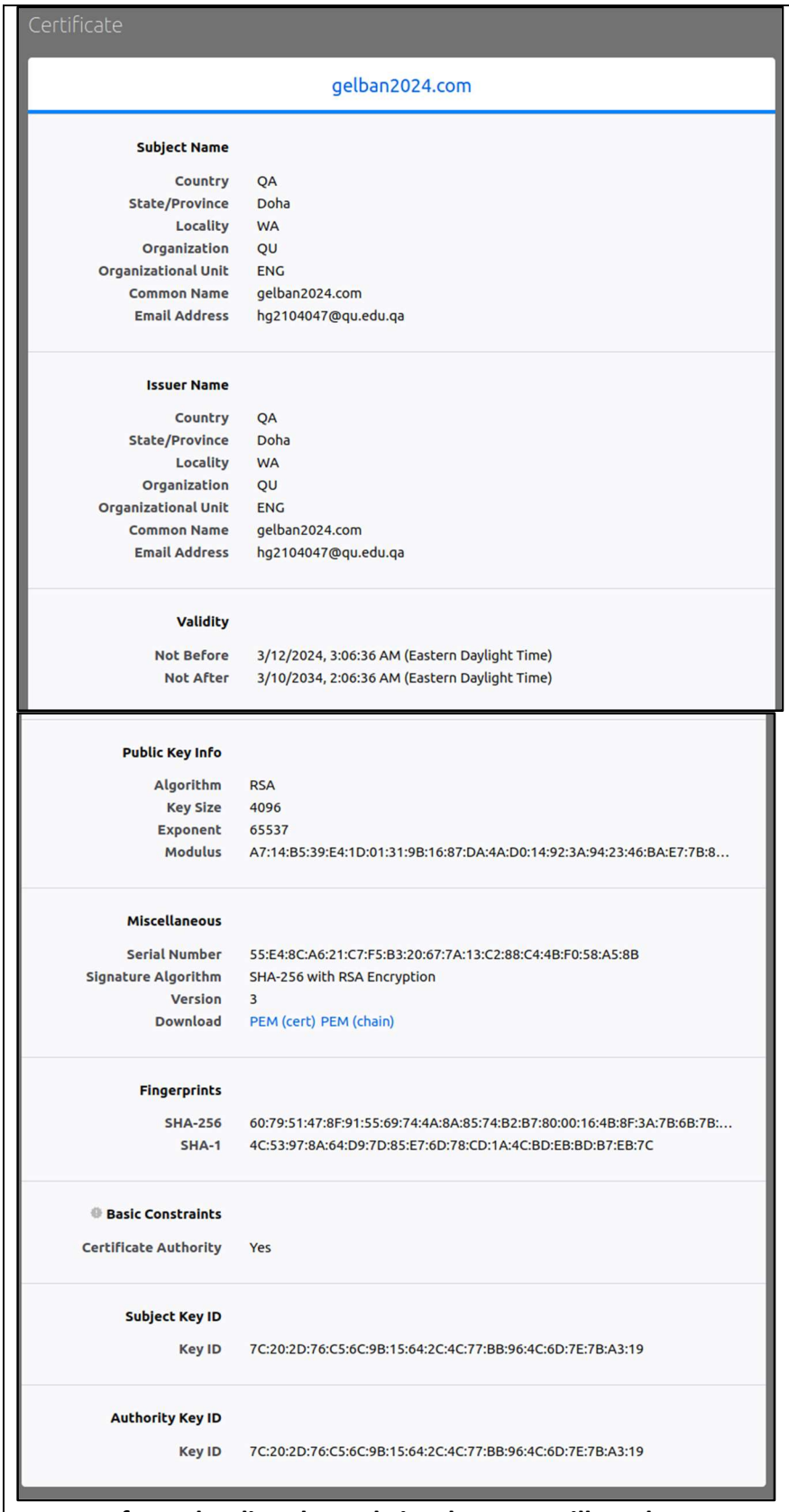
- **Next we ran "http://gelban2024.com"**



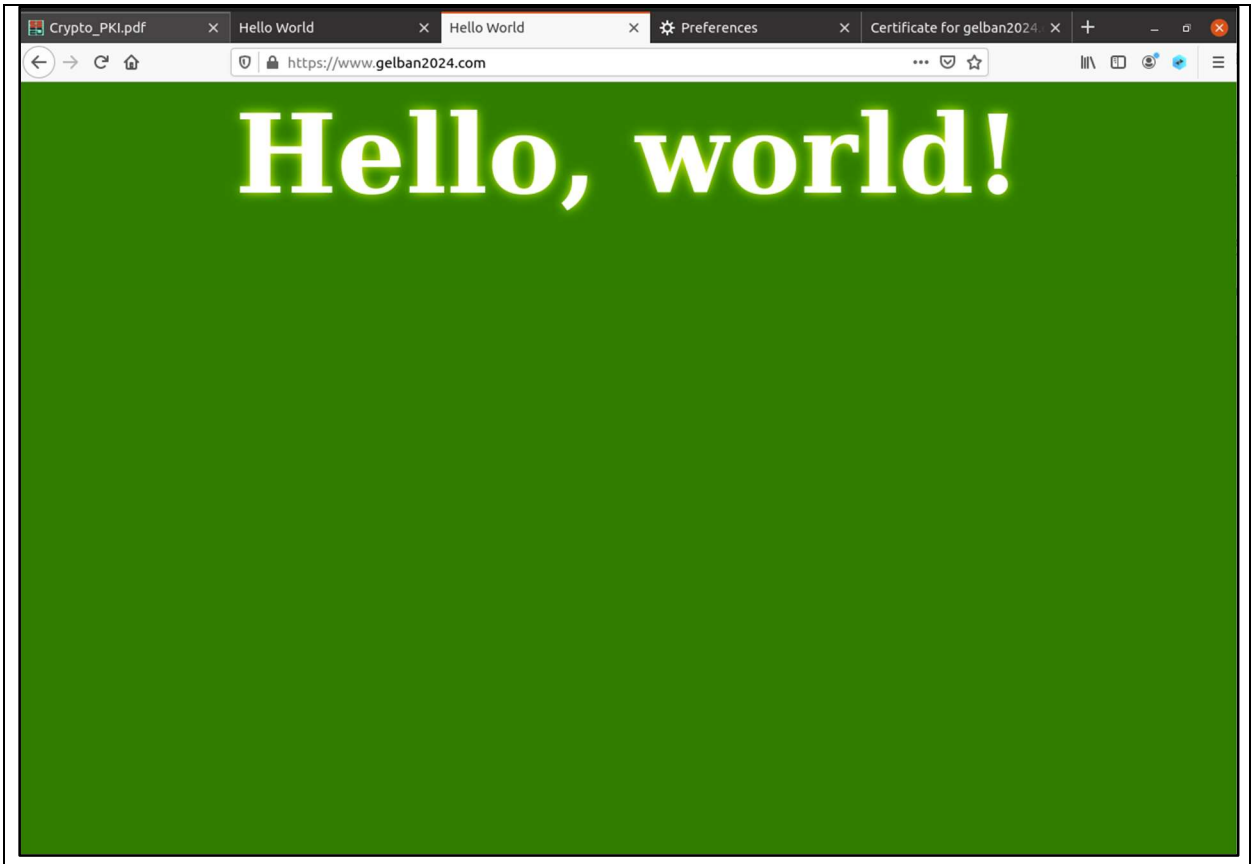
- **When running https://gelban2024, we got this warning page:**



- **To fix this we must Go to Preferences in the browser window, scroll down to the "View Certificates" tile, click on "View Certificates", Click on the "Import" tab, In the prompt, check mark the option "Trust this CA to identify websites"**



- **After reloading the website the page will work:**



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

You need to submit a detailed lab report, with screenshots, to describe what you have done and what you have observed. You also need to provide explanation to the observations that are interesting or surprising. Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will not receive credits. In addition, answer any questions if any.

The site chosen is google (www.google.com)
Task 4 instruction:

1. **Add a virtual host to Apache'ssl confeguration file:**

```
root@2566d76863b4:/etc/apache2/sites-available# ls
000-default.conf        default-ssl.conf          google_apache_ssl.conf
bank32_apache_ssl.conf  gelban24_apache_ssl.conf
root@2566d76863b4:/etc/apache2/sites-available# cat google_apache_ssl.conf
<VirtualHost *:443>
    DocumentRoot /var/www/gelban2024
    ServerName www.google.com
    ServerAlias www.googleA.com
    ServerAlias www.googleB.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/server.crt
    SSLCertificateKeyFile /certs/server.key
</VirtualHost>
```

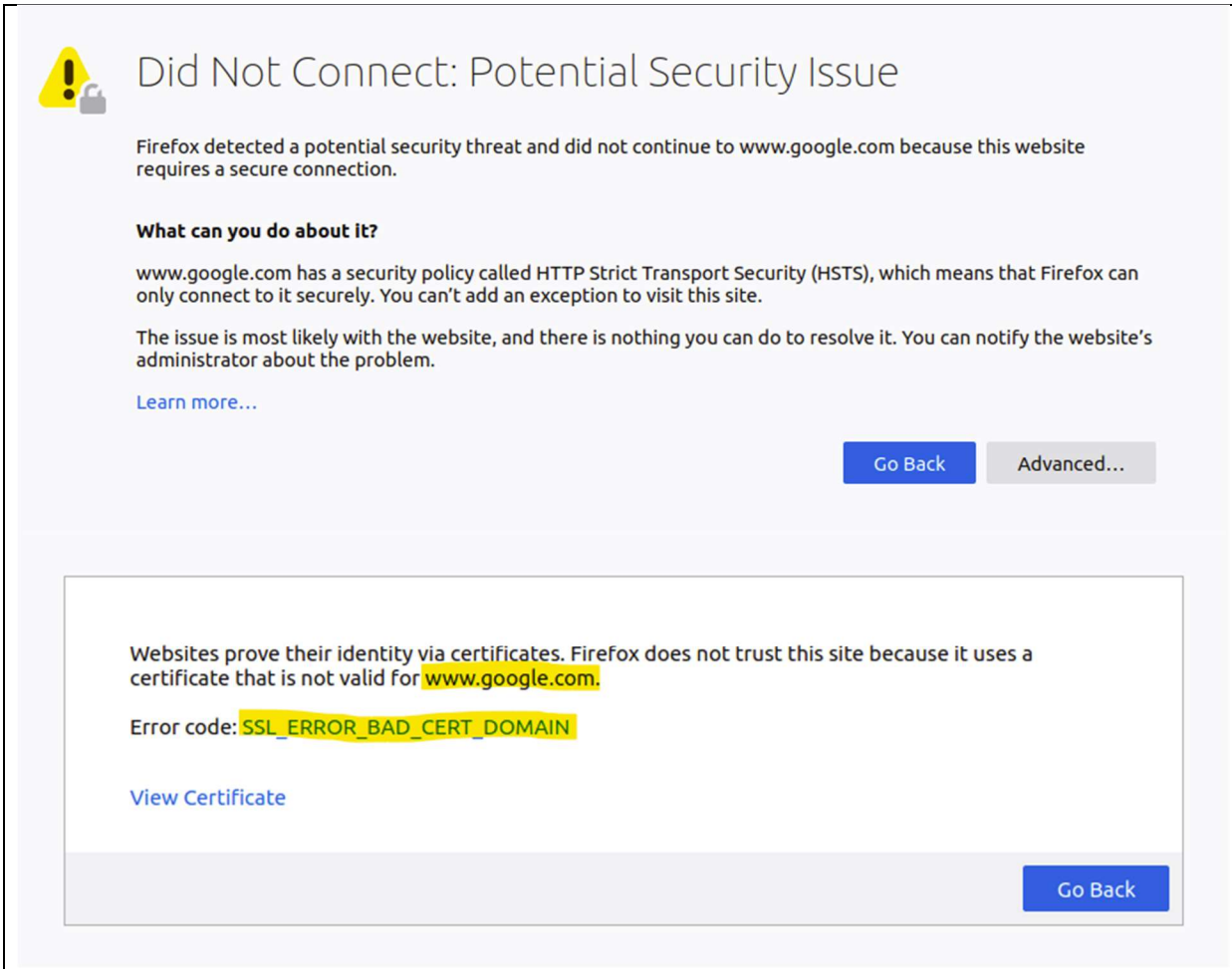
2. Change the server's name and keep the rest of the configuration

3. Using the certificate that was issued for gelban2024.com to secure the page and to access it.

Step2:
DNS attack

```
# For DNS Rebinding Lab
192.168.60.80   www.seedIoT32.com
10.9.0.80 www.bank32.com
10.9.0.80 www.gelban2024.com
10.9.0.80 www.google.com
```

Step 3:
Browsing the website



Observation:
The error message indicates a mismatch between the domain name the browser tried to connect to, and the domain names listed in the certificate presented by the server.

Browsers and other clients perform a check on the certificate presented by the server during the SSL/TLS handshake process. This check ensures that the certificate is not only valid and trusted but also corresponds to the site the user is trying to access. This mechanism is crucial for preventing MITM attacks, where an attacker could intercept or redirect traffic to a malicious site. If the certificate's domain doesn't match the site's domain, it's a strong indication of something amiss, prompting the browser to block the connection and warn the user.

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

You need to submit a detailed lab report, with screenshots, to describe what you have done and what you have observed. You also need to provide explanation to the observations that are interesting or surprising. Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will not receive credits. In addition, answer any questions if any.

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

```
- Generate a new certificate request:
openssl req -newkey rsa:2048 -sha256 -keyout server.key -out server.csr -subj
"/CN=www.fake24.com/O=Fake Inc./C=QA" -passout pass:dees -addext
"subjectAltName = DNS:www.fake24.com, DNS:www.fake24A.com, DNS:www.fake24B.com"

- Generating a Certificate:
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

- copy server.crt & server.key to the "volumes" directory

- add 10.9.0.80    www.amazon.com inside /etc/hosts
```

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

```
INSIDE THE CONTAINER
- under the volumes directory: cp server* /certs

- cd /etc/apache2/sites-available/
create a new file, and add this
```

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

<VirtualHost *:80>
    DocumentRoot /var/www/fake
    ServerName www.amazon.com
    DirectoryIndex index_red.html
</VirtualHost>
```

- restart the Apache server
 >> service apache2 restart