

姓名：蔡佩蓉      學號：109511286

## Secret-Key Encryption Lab (Lab5)

### Task 1: Becoming a Certificate Authority (CA)

```
seed@VM: ~/Desktop
[05/23/24] seed@VM:~/Desktop$ cp /usr/lib/ssl/openssl.cnf .
[05/23/24] seed@VM:~/Desktop$ mkdir demoCA
[05/23/24] seed@VM:~/Desktop$ mkdir demoCA/certs
[05/23/24] seed@VM:~/Desktop$ mkdir demoCA/crl
[05/23/24] seed@VM:~/Desktop$ touch demoCA/index.txt
[05/23/24] seed@VM:~/Desktop$ mkdir demoCA/newcerts
[05/23/24] seed@VM:~/Desktop$ echo 1000 > demoCA/serial
[05/23/24] seed@VM:~/Desktop$ openssl req -x509 -newkey rsa:4096 -sha256 -days 3650 \
> -keyout ca.key -out ca.crt \
> -subj "/CN=www.demoCA.com/O=Demo CA LTD./C=TW" \
> -passout pass:dees
Generating a RSA private key
.....++++
.....++++
writing new private key to 'ca.key'
-----
```

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

```
seed@VM: ~/Desktop

X509v3 extensions:
  X509v3 Subject Key Identifier:
    0A:C4:D7:56:B0:F3:78:EC:9C:2E:0B:D7:37:EA:30:94:23:91:7A:0C
  X509v3 Authority Key Identifier:
    keyid:0A:C4:D7:56:B0:F3:78:EC:9C:2E:0B:D7:37:EA:30:94:23:91:7A:0C

  X509v3 Basic Constraints: critical
    CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
51:7a:32:17:6a:7e:88:23:5e:8c:8c:e1:54:fc:73:9d:86:ce:
f0:e4:4d:54:3e:80:04:11:cc:d9:f1:3c:9f:fc:d7:34:92:4a:
66:80:11:27:be:20:12:e6:33:93:33:20:bf:aa:30:88:d8:39:
c4:d8:da:d9:38:1d:dc:4b:82:67:47:c3:ee:f7:ac:9a:17:2c:
45:d4:f0:c3:0a:ca:38:b9:d7:12:7b:84:6d:72:a8:36:81:81:
20:c9:6f:95:4f:f8:74:b6:d3:bb:c7:94:e4:04:82:a7:7f:02:
53:b7:75:0f:e9:f7:76:6d:21:cb:2c:b8:c6:31:72:8c:b9:63:
9b:00:c3:15:f6:09:c8:ee:85:2a:e6:1c:be:de:2d:99:7f:4e:
```

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

```
seed@VM: ~/Desktop
[05/23/24] seed@VM:~/Desktop$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            56:c9:a0:ef:f3:e7:62:b8:51:2f:ea:ce:70:49:af:d3:05:b3:2a:9a
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.demoCA.com, O = Demo CA LTD., C = TW
        Validity
            Not Before: May 23 10:01:03 2024 GMT
            Not After : May 21 10:01:03 2024 GMT
        Subject: CN = www.demoCA.com, O = Demo CA LTD., C = TW
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public-Key: (4096 bit)
            Modulus:
                00:e0:63:2b:02:3c:41:28:60:cd:ee:2e:d4:5f:de:
```

Subject and Issuer panel contains the same information indicates that this is a self-signed certificate.

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.

```
seed@VM: ~/Desktop
publicExponent: 65537 (0x10001)
privateExponent:
    00:dd:4e:51:73:e1:f3:ad:9c:54:5e:af:07:3d:0a:
    b3:1b:72:60:6d:f5:f1:41:66:47:bf:ff:42:d1:44:
    a9:c1:51:3e:b9:18:db:f8:56:4a:f5:04:ef:23:a7:
    47:af:81:9b:3d:8e:c9:df:8c:93:cb:e2:14:e9:24:
    18:38:d3:a7:a1:ea:c8:c8:06:6d:63:5d:68:ea:2d:
    b0:e4:73:64:85:1d:1b:f2:d2:58:0a:d3:61:b5:74:
    f1:cd:f3:21:db:58:d1:62:2b:06:d1:43:e9:96:34:
    9f:3f:e1:7d:7a:92:35:b1:ac:ff:04:eb:8d:61:13:
    2c:bd:fb:5e:15:c5:58:3d:6e:0a:e7:cc:12:27:ec:
    9e:9f:ce:5b:ed:0d:f2:80:c5:4d:42:7f:70:d6:25:
    b1:be:43:77:3d:06:20:5b:f5:a6:68:65:f5:4a:ff:
    a0:ba:ce:08:59:83:66:96:b6:a0:9c:1d:9f:18:3f:
    4a:da:40:b9:98:fc:00:bc:10:e0:73:06:99:64:eb:
    99:52:b8:d3:33:cc:98:45:0f:d9:d5:7c:03:3e:e8:
    af:5b:52:e2:9b:95:8f:7d:71:8a:13:33:ad:99:1f:
    57:0b:27:ac:34:29:7c:6d:b9:99:7c:8d:b4:80:09:
    25:8e:f9:8f:02:88:be:00:d4:f9:f7:d7:6f:70:7d:
    77:4e:0e:6b:dc:6d:a2:46:48:ed:cf:f7:97:30:b5:
    96:c1:de:c4:94:bc:8c:f9:3d:f9:5c:00:85:96:cd:
    bc:0c:ec:d1:5c:85:97:5f:7e:a5:0f:01:86:32:49:
    c0:ee:f5:55:38:d6:10:e6:59:67:04:2c:c2:7a:f6:
    ce:41:0e:9b:15:5f:a5:36:01:4c:b8:c6:59:3b:f1:
    ae:72:c8:45:88:fe:2a:0f:e3:93:a3:07:c5:ab:b6:
    57:78:96:6e:b6:2d:e4:f9:e1:36:c7:b5:c3:95:cf:
    dd:dc:ab:69:d9:5e:b9:4c:59:9a:a4:e2:e0:0a:30:
    c0:c6:4b:a2:a9:c3:00:d6:3e:d0:d3:0f:94:11:e2:
    a8:78:2c:78:76:39:55:6e:37:07:fb:d4:cf:c8:9d:
    e1:48:b4:95:67:fb:47:be:24:b4:75:30:95:4d:80:
    8e:c5:20:03:1d:ba:5d:1c:82:ad:72:41:4c:9f:f3:
    b6:cc:bf:6b:53:63:63:89:45:9c:8c:b3:44:2b:75:
    01:23:2e:24:ec:5a:99:5f:d8:4f:81:dc:ca:7a:b0:
    c7:1b:e0:4c:a3:c0:65:58:c6:d3:27:7e:51:40:80:
    c6:f4:fa:0c:5f:4d:bc:b8:65:1b:76:e1:07:bd:f0:
    30:5d:fd:8a:e8:64:49:1c:92:75:5a:73:d7:05:56:
    fd:64:11
```

```
seed@VM: ~/Desktop
modulus:
    00:e0:63:2b:02:3c:41:28:60:cd:ee:2e:d4:5f:de:
    9a:e0:06:31:a0:9d:67:fb:7f:ba:b2:e9:4c:16:bb:
    4e:cb:b0:4c:25:c0:26:d9:a0:81:f3:aa:94:2e:f7:
    59:f7:ba:3d:c6:18:b0:20:d9:d0:3e:c2:45:03:94:
    94:21:1c:26:50:1d:c3:37:5a:98:8f:8a:e0:fb:aa:
    62:69:bd:9d:d9:d5:9a:2c:58:03:f3:09:e8:53:b4:
    9a:7d:6b:5f:e0:2a:e3:57:58:23:80:f8:a4:02:11:
    78:cf:c2:54:cb:d7:86:1f:e4:b0:ca:c2:9b:b5:6e:
    b1:8a:a1:f2:c8:ba:54:58:fa:c0:e9:4a:39:9c:4e:
    ae:dc:7d:47:ae:22:62:4d:ef:7e:0f:7d:17:9f:8b:
    cf:de:f1:1e:3d:af:fe:6c:8d:36:43:9b:c9:c6:89:
    1f:43:37:d0:27:86:8d:9d:6d:0d:48:63:70:69:a1:
    54:a5:cd:d5:af:1b:87:64:87:a4:db:d7:10:ab:0d:
    af:4c:ed:4b:3b:d2:e1:9f:fc:f4:32:e4:91:65:83:
    6a:c3:f0:52:e1:86:25:27:7a:ab:4c:4a:ab:03:59:
    b4:2e:3d:17:e6:c5:16:b5:f7:09:bd:5b:28:2b:cf:
    7f:44:0b:10:d8:3f:26:4d:13:a6:cf:9c:79:c7:94:
    c7:45:27:04:ed:73:ea:d4:89:51:c0:b0:cf:00:fb:
    38:5b:3b:ff:d7:63:25:ca:c6:8a:e1:1f:b3:95:01:
    b7:78:b7:fb:e4:e7:55:81:59:fa:8e:3d:f8:4e:50:
    cc:dd:cc:8c:a7:88:dc:20:e1:3f:c6:cf:46:de:e1:
    9e:b9:db:60:d5:1a:72:21:33:4e:7f:99:71:76:c8:
    6e:47:9b:37:0b:b0:8f:a0:79:0d:56:23:4a:a3:b9:
    48:b7:cb:e9:66:9d:61:65:52:db:19:23:a3:48:b7:
    93:f1:dc:fe:28:24:61:7f:64:38:2c:ad:0b:80:09:
    fa:37:76:8b:43:be:aa:b3:14:0e:6a:1c:c5:c3:e0:
    af:71:54:b2:73:0b:c2:49:a4:78:3b:f2:3c:3d:5d:
    c7:d8:79:9d:04:fd:d2:ad:00:aa:0c:c1:63:d0:19:
    22:ad:bb:97:a7:af:eb:84:f9:7e:93:5f:5d:13:d0:
    e5:e8:60:ae:a2:f8:65:7d:9d:7e:fb:fc:03:4e:5a:
    b1:86:a7:72:34:89:6e:b0:12:f4:27:12:71:1e:53:
    05:c5:be:56:21:67:f8:0a:d2:4f:b1:05:bd:fc:1b:
    8f:e5:f8:82:f2:a0:e9:5e:6c:37:d2:87:07:68:5d:
    e8:bf:f6:ab:6e:b2:6e:9f:06:4f:db:ba:39:81:3e:
    dd:1f:93
```

```
seed@VM: ~/Desktop
prime1:
00:fc:dc:e9:de:ac:2b:56:01:b7:9a:43:71:9e:84:
89:bf:ff:2e:43:c0:96:1b:a3:9d:9f:e8:37:80:d6:
ab:87:33:d1:47:06:d1:44:79:a0:63:e7:44:8b:6a:
19:82:3d:9d:1f:df:bd:00:a2:74:1d:9d:00:00:ab:
c7:ca:80:b0:9b:44:ba:67:8f:3d:a5:b4:6e:ab:2d:
4e:01:83:12:f8:1e:b7:85:56:ff:6d:b4:98:63:69:
e9:a9:5e:ef:c4:aa:30:bc:9c:9c:cf:3d:e4:cf:35:
8c:18:09:8d:d3:17:52:50:4f:4a:21:17:cd:7b:8f:
9b:7f:fb:9b:11:e2:dc:5f:36:3b:8d:dc:90:9e:04:
57:8c:32:e9:93:d9:c0:dd:a1:3a:5f:6f:5b:e4:16:
7a:d4:3e:0b:b9:5d:d0:e5:74:f2:01:0d:49:f3:5e:
98:8a:bb:cf:90:53:c8:62:a2:15:70:9d:33:09:15:
e1:65:e7:c7:bc:d1:2a:a3:55:fb:74:32:aa:95:71:
9b:06:b2:06:d2:2e:8c:b2:3d:ed:91:c5:22:fe:1b:
7b:37:a8:e8:0d:79:e2:e8:d1:3e:c5:7e:3f:0c:88:
99:71:d4:4a:08:93:a1:dd:35:b4:83:46:5b:8a:c5:
59:b5:0c:86:07:28:7a:c7:02:0d:97:85:75:b8:ce:
c5:c9
```

```
seed@VM: ~/Desktop
prime2:
00:e3:2b:d1:16:6c:99:9b:59:48:ab:6c:38:00:22:
46:ec:e5:a9:cf:ae:90:7d:68:e6:c6:4a:56:10:6e:
0f:98:1a:a1:30:7c:1a:7c:22:ca:9d:bf:01:e3:c2:
34:bb:e9:ce:bd:26:36:54:5c:6d:38:09:17:8b:a9:
38:4c:a7:ef:21:09:38:15:31:73:e6:11:02:bb:70:
14:8e:a5:d4:cc:98:a2:66:50:42:a1:ab:66:da:3d:
77:a1:dd:4a:17:f3:1c:2e:58:f8:69:98:8a:f7:13:
5e:c2:0e:e8:ea:bc:5e:02:d8:f9:2d:e9:87:c9:6d:
e1:67:00:8f:c2:9e:ef:d2:63:de:38:62:35:bf:ad:
bf:3e:9c:af:21:5e:fc:31:b1:0a:62:f4:3e:46:ec:
2c:94:31:8a:26:8f:24:fc:b2:5b:b6:6c:36:39:3c:
2e:42:1b:2b:c4:da:3e:44:77:2f:3c:a5:8d:13:87:
2a:a6:d3:fa:81:b0:9b:a4:30:45:c0:14:5a:d7:fa:
17:38:8e:2b:9a:4e:c5:51:b8:39:59:d7:46:e3:ff:
f6:fb:e4:55:d6:7c:7c:e1:b6:2f:ac:fb:d6:cb:60:
43:2f:e1:7c:bd:37:3a:49:b4:e3:d3:ec:76:4e:a1:
c4:d9:e6:c7:1e:42:6f:5f:8e:23:24:06:35:e2:cf:
58:7b
```

## Task 2: Generating a Certificate Request for Your Web Server

```
seed@VM: ~/Desktop
[05/23/24]seed@VM:~/Desktop$ openssl req -newkey rsa:2048 -sha256 -keyout pychua2024.key -out py
chua2024.csr -subj "/CN=www.pychua2024.com/O=PYChua2024 Inc./C=TW" -passout pass:dees -addext "s
ubjectAltName = DNS:www.pychua2024.com, DNS:www.pychua2024A.com, DNS:www.pychua2024B.com"
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'pychua2024.key'
-----
```

```
seed@VM: ~/Desktop
[05/23/24]seed@VM:~/Desktop$ openssl req -in pychua2024.csr -text -noout
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: CN = www.pychua2024.com, O = PYChua2024 Inc., C = TW
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
      RSA Public-Key: (2048 bit)
      Modulus:
        00:c5:12:e8:9e:dc:a3:f3:03:06:d4:0a:fb:0b:6d:
        3c:37:5a:7e:84:d3:f6:29:0d:75:32:70:f4:93:38:
        27:2c:01:96:0e:77:de:f4:71:7b:6b:7c:44:7a:45:
        9a:17:a3:ba:cc:ef:31:6d:2a:23:95:16:4b:5f:28:
        c0:dc:fa:77:5b:5e:84:89:f5:38:94:c4:06:90:f5:
        4f:c8:9e:09:0c:4f:7d:dc:2e:fc:8b:bb:7c:7c:13:
        37:1b:22:c4:5b:ba:df:89:42:33:4f:d3:b2:ef:82:
        3b:04:f5:3b:8c:34:f2:de:63:8a:b4:34:eb:6b:3d:
        b2:57:0a:63:21:50:fd:0d:f4:89:63:e0:e0:6a:4c:
        fe:3b:4c:95:f6:63:f8:d9:e7:33:32:18:81:d9:83:
        12:a0:09:e4:cb:c5:d1:53:2d:ca:27:df:b1:8e:4b:
        73:66:8b:07:47:58:15:74:d0:4c:6d:fb:e5:e4:ee:
        d9:b1:f0:32:bd:be:24:7c:27:42:e1:6d:fd:57:a0:
        4f:1b:1a:88:9c:8c:92:13:61:94:67:6f:0c:5c:44:
        25:11:a2:39:52:9e:83:ca:62:4e:e7:55:e2:6b:2e:
        06:42:09:26:a5:f0:8f:1d:d4:5a:f5:fa:fe:70:9b:
        5d:8a:8f:05:31:b9:18:c7:fa:ec:b9:66:4c:f4:56:
        7d:cd
      Exponent: 65537 (0x10001)
  Attributes:
    Requested Extensions:
      X509v3 Subject Alternative Name:
        DNS:www.pychua2024.com, DNS:www.pychua2024A.com, DNS:www.pychua2024B.com
  Signature Algorithm: sha256WithRSAEncryption
    b4:ff:b3:bf:9b:0a:cc:94:72:f2:06:74:b1:0e:5f:52:6e:71:
    a5:de:ad:32:b5:f5:16:b5:7e:dd:6f:fe:75:0b:64:80:f6:bc:
```

### Task 3: Generating a Certificate for your server

```
seed@VM: ~/Desktop
[05/23/24]seed@VM:~/Desktop$ openssl ca -config openssl.cnf -policy policy_anything \
> -md sha256 -days 3650 \
> -in psychua2024.csr -out psychua2024.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: May 23 10:04:36 2024 GMT
    Not After : May 21 10:04:36 2034 GMT
  Subject:
    countryName           = TW
    organizationName      = PYChua2024 Inc.
    commonName            = www.psychua2024.com
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    Netscape Comment:
      OpenSSL Generated Certificate
    X509v3 Subject Key Identifier:
      0D:CB:4E:C7:81:00:E5:F6:FF:88:4B:42:4A:73:89:FC:5E:B8:E0:9B
    X509v3 Authority Key Identifier:
      keyid:0A:C4:D7:56:B0:F3:78:EC:9C:2E:0B:D7:37:EA:30:94:23:91:7A:0C

    X509v3 Subject Alternative Name:
      DNS:www.psychua2024.com, DNS:www.psychua2024A.com, DNS:www.psychua2024B.com
Certificate is to be certified until May 21 10:04:36 2034 GMT (3650 days)

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

```
seed@VM: ~/Desktop
[05/23/24]seed@VM:~/Desktop$ openssl x509 -in psychua2024.crt -text -noout
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 4096 (0x1000)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: CN = www.demoCA.com, O = Demo CA LTD., C = TW
    Validity
      Not Before: May 23 10:04:36 2024 GMT
      Not After : May 21 10:04:36 2034 GMT
    Subject: C = TW, O = PYChua2024 Inc., CN = www.psychua2024.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (2048 bit)
      Modulus:
        00:c5:12:e8:9e:dc:a3:f3:03:06:d4:0a:fb:0b:6d:
        3c:37:5a:7e:84:d3:f6:29:0d:75:32:70:f4:93:38:
        27:2c:01:96:0e:77:de:f4:71:7b:6b:7c:44:7a:45:
        9a:17:a3:ba:cc:ef:31:6d:2a:23:95:16:4b:5f:28:
        c0:dc:fa:77:5b:5e:84:89:f5:38:94:c4:06:90:f5:
        4f:c8:9e:09:0c:4f:7d:dc:2e:fc:8b:bb:7c:7c:13:
        37:1b:22:c4:5b:ba:df:89:42:33:4f:d3:b2:ef:82:
        3b:04:f5:3b:8c:34:f2:de:63:8a:b4:34:eb:6b:3d:
        b2:57:0a:63:21:50:fd:0d:f4:89:63:e0:e0:6a:4c:
        fe:3b:4c:95:f6:63:f8:d9:e7:33:32:18:81:d9:83:
        12:a0:09:e4:cb:c5:d1:53:2d:ca:27:df:b1:8e:4b:
        73:66:8b:07:47:58:15:74:d0:4c:6d:fb:e5:e4:ee:
        d9:b1:f0:32:bd:be:24:7c:27:42:e1:6d:fd:57:a0:
        4f:1b:1a:88:9c:8c:92:13:61:94:67:6f:0c:5c:44:
        25:11:a2:39:52:9e:83:ca:62:4e:e7:55:e2:6b:2e:
        06:42:09:26:a5:f0:8f:1d:d4:5a:f5:fa:fe:70:9b:
        5d:8a:8f:05:31:b9:18:c7:fa:ec:b9:66:4c:f4:56:
        7d:cd
      Exponent: 65537 (0x10001)
    X509v3 extensions:
```

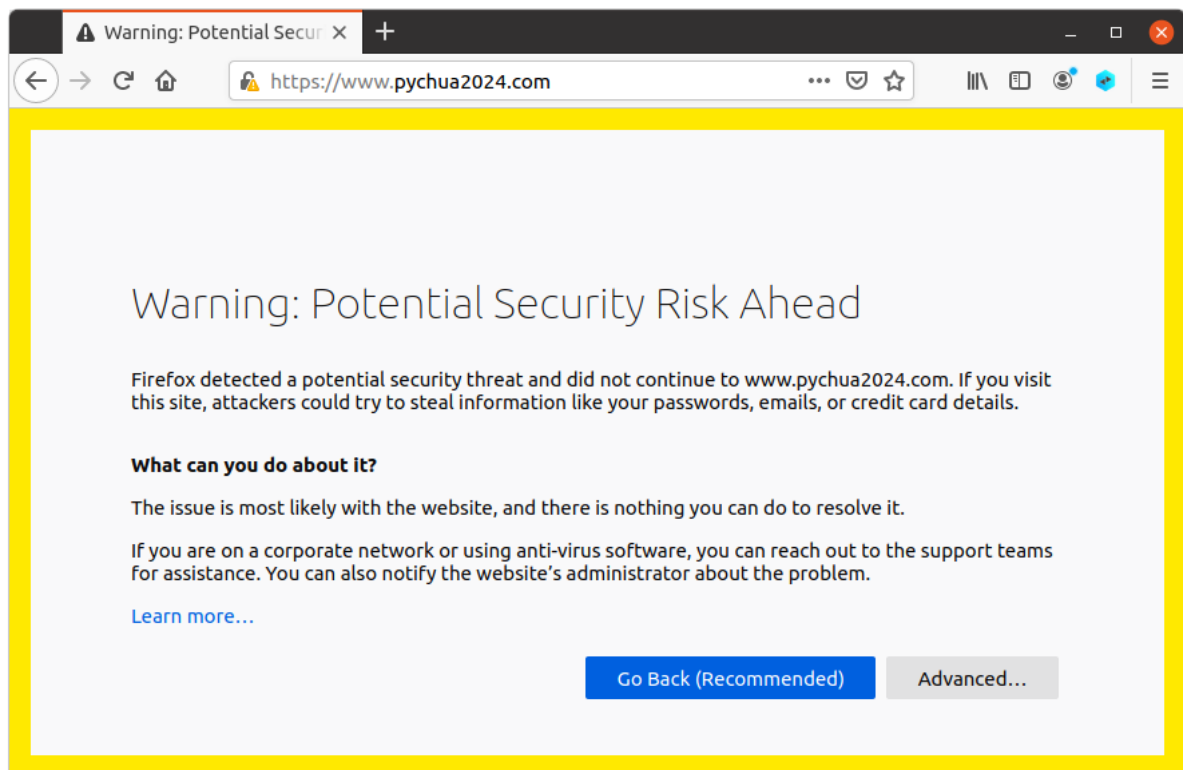
## Task 4: Deploying Certificate in an Apache-Based HTTPS Website

```
seed@VM: ~/Desktop
[05/23/24] seed@VM:~/Desktop$ sudo nano /etc/hosts
[05/23/24] seed@VM:~/Desktop$ cp pychua2024.key pychua2024.pem
[05/23/24] seed@VM:~/Desktop$ cat pychua2024.crt >> pychua2024.pem
[05/23/24] seed@VM:~/Desktop$ openssl s_server -cert pychua2024.pem -www
Enter pass phrase for pychua2024.pem:
Using default temp DH parameters
ACCEPT
```

Edit /etc/hosts file. Then, combine the secret key and the certificate into one file to configure the web server. Then launch our web server using pychua2024.pem.

This server can be accessed by typing `https://www.pychua2024.com` in Firefox but we will get an error that connection is not secure.

**Before adding certificate to the Firefox browser:**



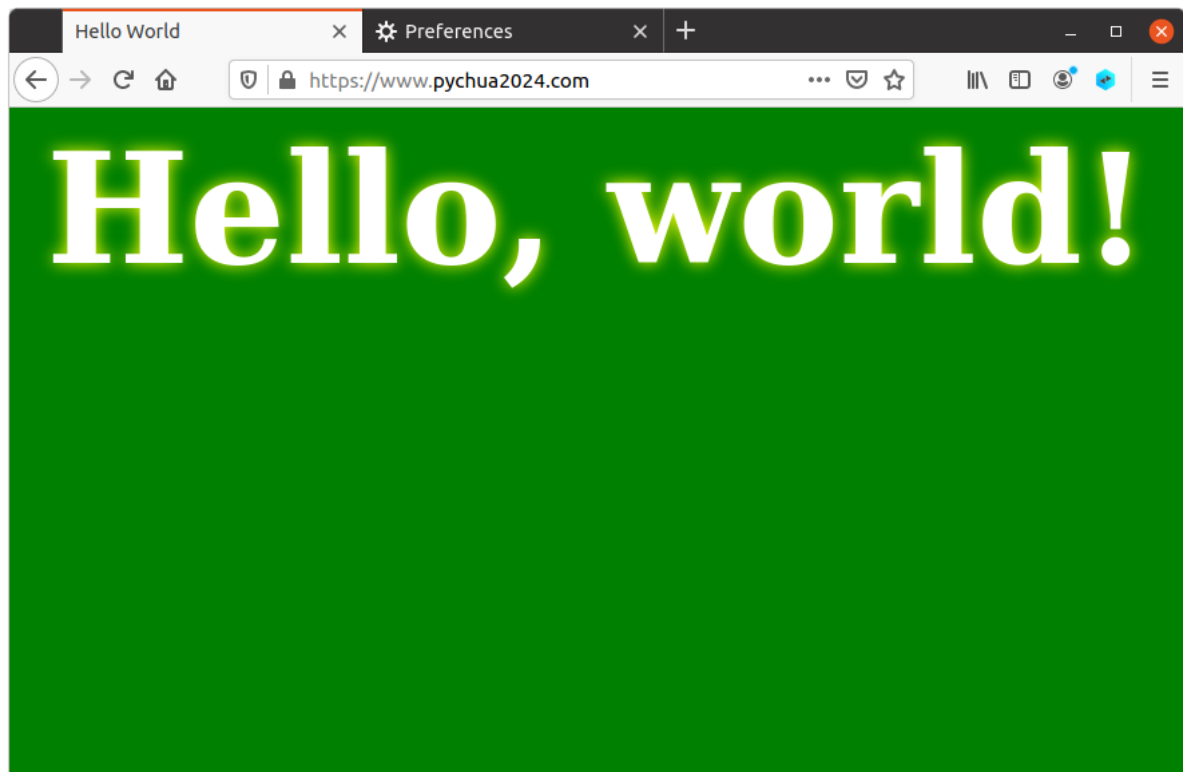
The connection is not secure due to an invalid security certificate. As the certificate issuer is unknown to Firefox (self-signed). Hence, we need to add our certificate to the browser so that it is recognized as a legitimate certificate.

For that we will go to preferences, security and then in the end view certificates and add our certificate there. Make sure to check the box saying that “Trust this CA to identify websites”.

Now when we run our website it will be accessed without error.



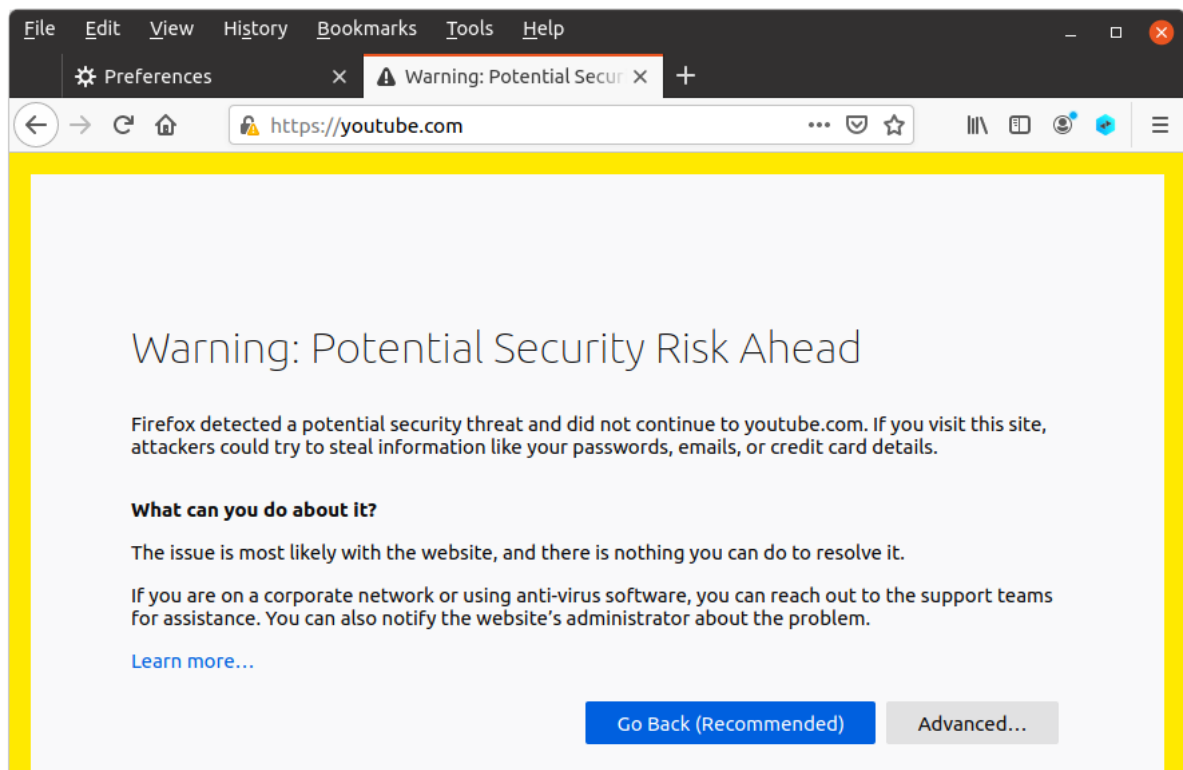
**After adding certificate:**



The terminal will also print accept each time the website is reloaded.

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

Edit /etc/hosts file. [10.9.0.80 youtube.com]



We accessed the server we built, but the certificate is not trusted.