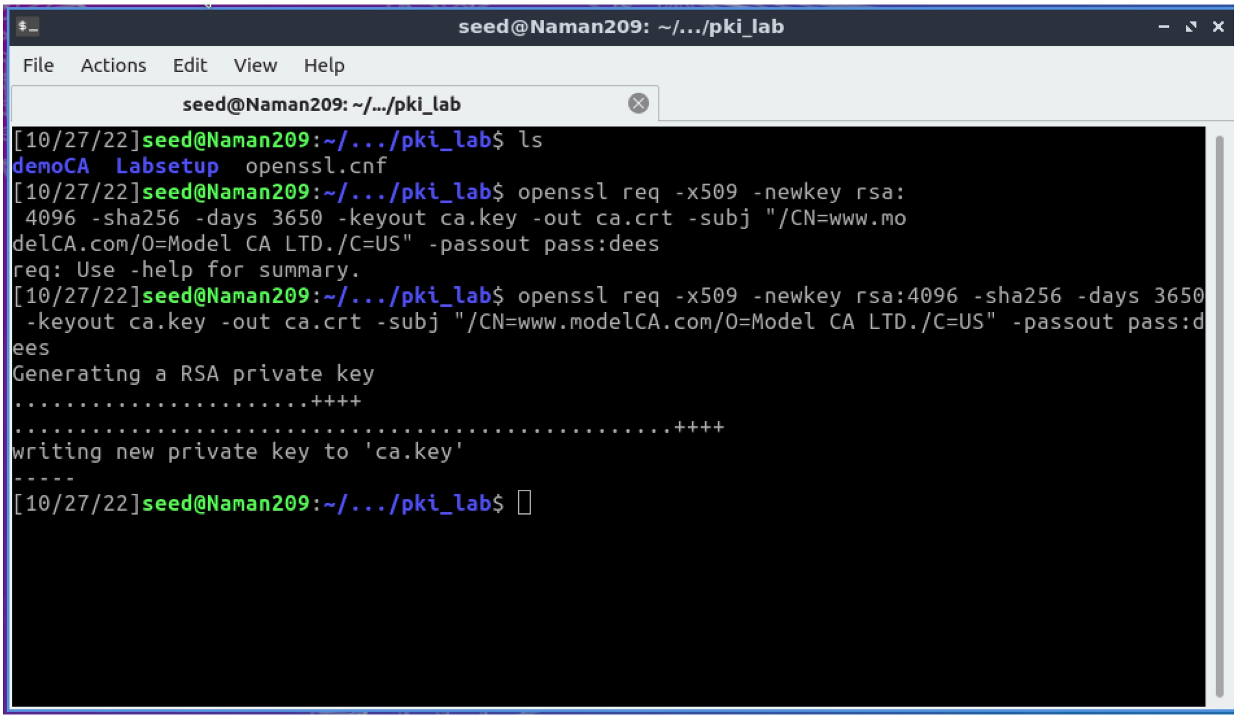
Applied Cryptography

Name	Naman Choudhary
SRN	PES2UG20CS209
Section	D

Public-Key Infrastructure

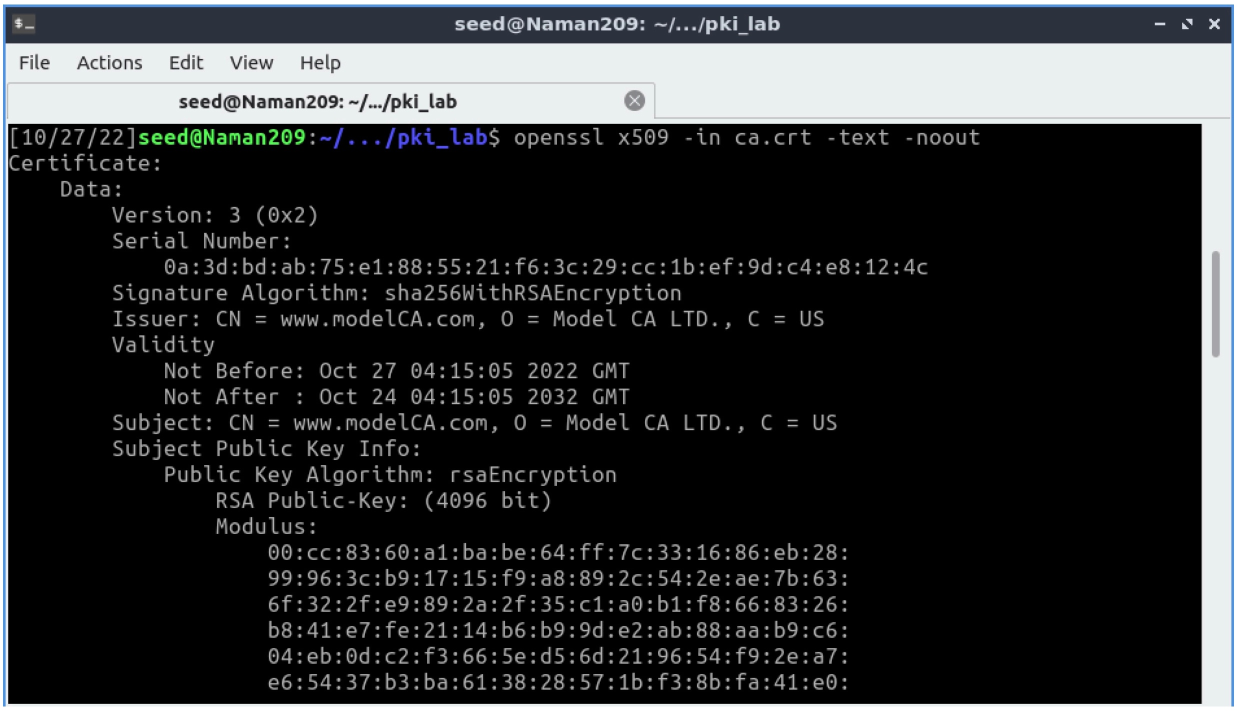
Task 1:Becoming a certificate authority (CA)

```bash
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
```



```
[10/27/22]seed@Naman209:~/.../pki_lab$ ls
demoCA  Labsetup  openssl.cnf
[10/27/22]seed@Naman209:~/.../pki_lab$ openssl req -x509 -newkey rsa:
 4096 -sha256 -days 3650 -keyout ca.key -out ca.crt -subj "/CN=www.mo
delCA.com/O=Model CA LTD./C=US" -passout pass:dees
req: Use -help for summary.
[10/27/22]seed@Naman209:~/.../pki_lab$ 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:d
ees
Generating a RSA private key
.......................++++
.......................................................++++
writing new private key to 'ca.key'
-----
[10/27/22]seed@Naman209:~/.../pki_lab$ 
```

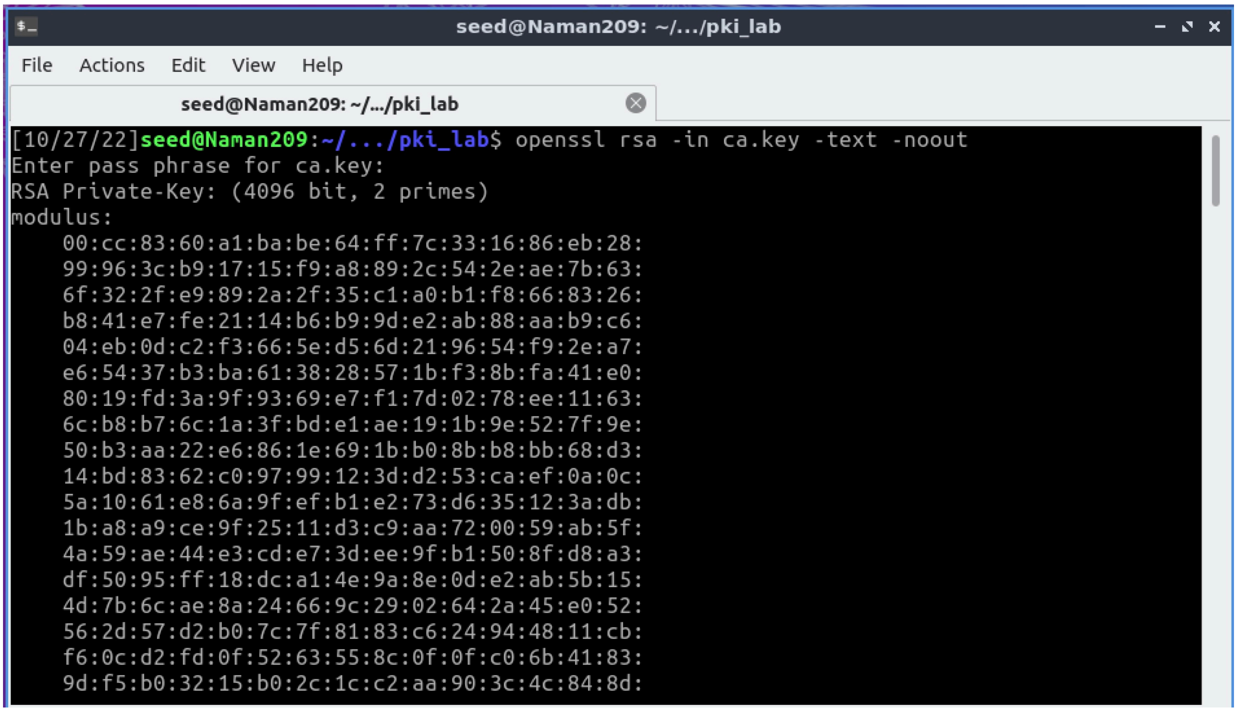
```bash
openssl x509 -in ca.crt -text -noout
```



```
[10/27/22]seed@Naman209:~/.../pki_lab$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0a:3d:bd:ab:75:e1:88:55:21:f6:3c:29:cc:1b:ef:9d:c4:e8:12:4c
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: Oct 27 04:15:05 2022 GMT
            Not After : Oct 24 04:15:05 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:cc:83:60:a1:ba:be:64:ff:7c:33:16:86:eb:28:
                    99:96:3c:b9:17:15:f9:a8:89:2c:54:2e:ae:7b:63:
                    6f:32:2f:e9:89:2a:2f:35:c1:a0:b1:f8:66:83:26:
                    b8:41:e7:fe:21:14:b6:b9:9d:e2:ab:88:aa:b9:c6:
                    04:eb:0d:c2:f3:66:5e:d5:6d:21:96:54:f9:2e:a7:
                    e6:54:37:b3:ba:61:38:28:57:1b:f3:8b:fa:41:e0:
```

Bash

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

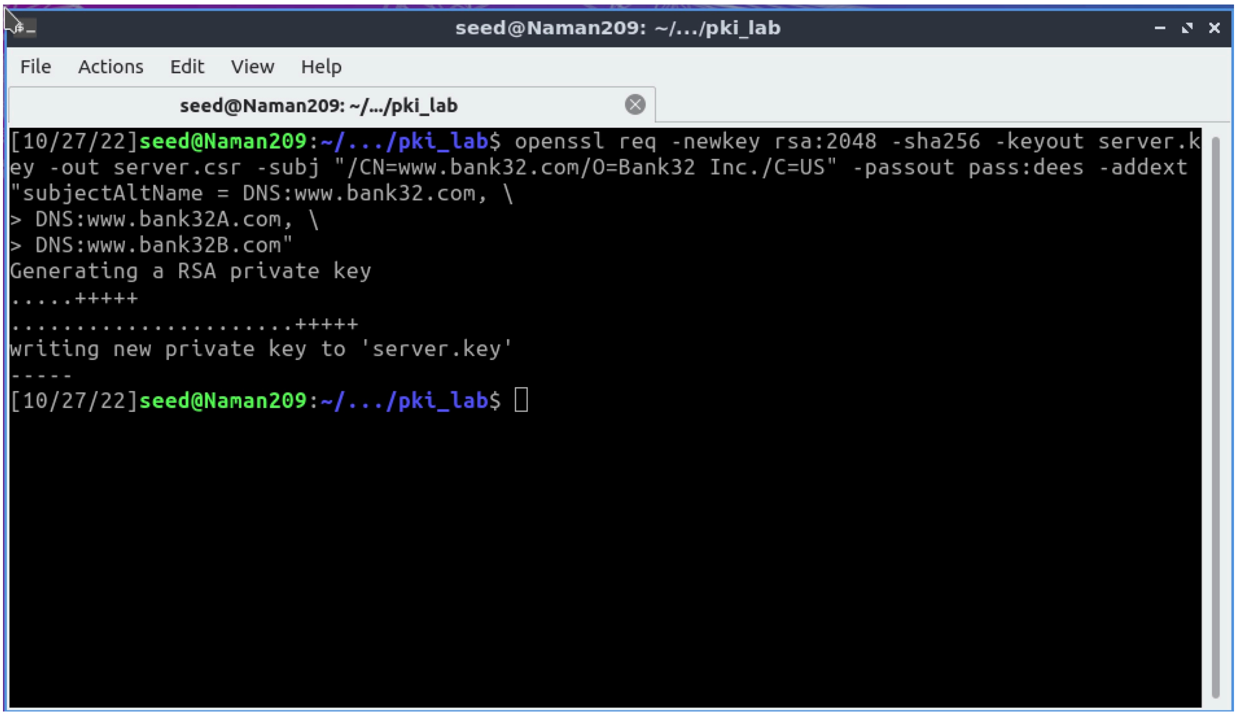


```
[10/27/22]seed@Naman209:~/.../pki_lab$ openssl rsa -in ca.key -text -noout
Enter pass phrase for ca.key:
RSA Private-Key: (4096 bit, 2 primes)
modulus:
    00:cc:83:60:a1:ba:be:64:ff:7c:33:16:86:eb:28:
    99:96:3c:b9:17:15:f9:a8:89:2c:54:2e:ae:7b:63:
    6f:32:2f:e9:89:2a:2f:35:c1:a0:b1:f8:66:83:26:
    b8:41:e7:fe:21:14:b6:b9:9d:e2:ab:88:aa:b9:c6:
    04:eb:0d:c2:f3:66:5e:d5:6d:21:96:54:f9:2e:a7:
    e6:54:37:b3:ba:61:38:28:57:1b:f3:8b:fa:41:e0:
    80:19:fd:3a:9f:93:69:e7:f1:7d:02:78:ee:11:63:
    6c:b8:b7:6c:1a:3f:bd:e1:ae:19:1b:9e:52:7f:9e:
    50:b3:aa:22:e6:86:1e:69:1b:b0:8b:b8:bb:68:d3:
    14:bd:83:62:c0:97:99:12:3d:d2:53:ca:ef:0a:0c:
    5a:10:61:e8:6a:9f:ef:b1:e2:73:d6:35:12:3a:db:
    1b:a8:a9:ce:9f:25:11:d3:c9:aa:72:00:59:ab:5f:
    4a:59:ae:44:e3:cd:e7:3d:ee:9f:b1:50:8f:d8:a3:
    df:50:95:ff:18:dc:a1:4e:9a:8e:0d:e2:ab:5b:15:
    4d:7b:6c:ae:8a:24:66:9c:29:02:64:2a:45:e0:52:
    56:2d:57:d2:b0:7c:7f:81:83:c6:24:94:48:11:cb:
    f6:0c:d2:fd:0f:52:63:55:8c:0f:0f:c0:6b:41:83:
    9d:f5:b0:32:15:b0:2c:1c:c2:aa:90:3c:4c:84:8d:
```

Task 2:Generating a Certificate Request for the web server

Bash

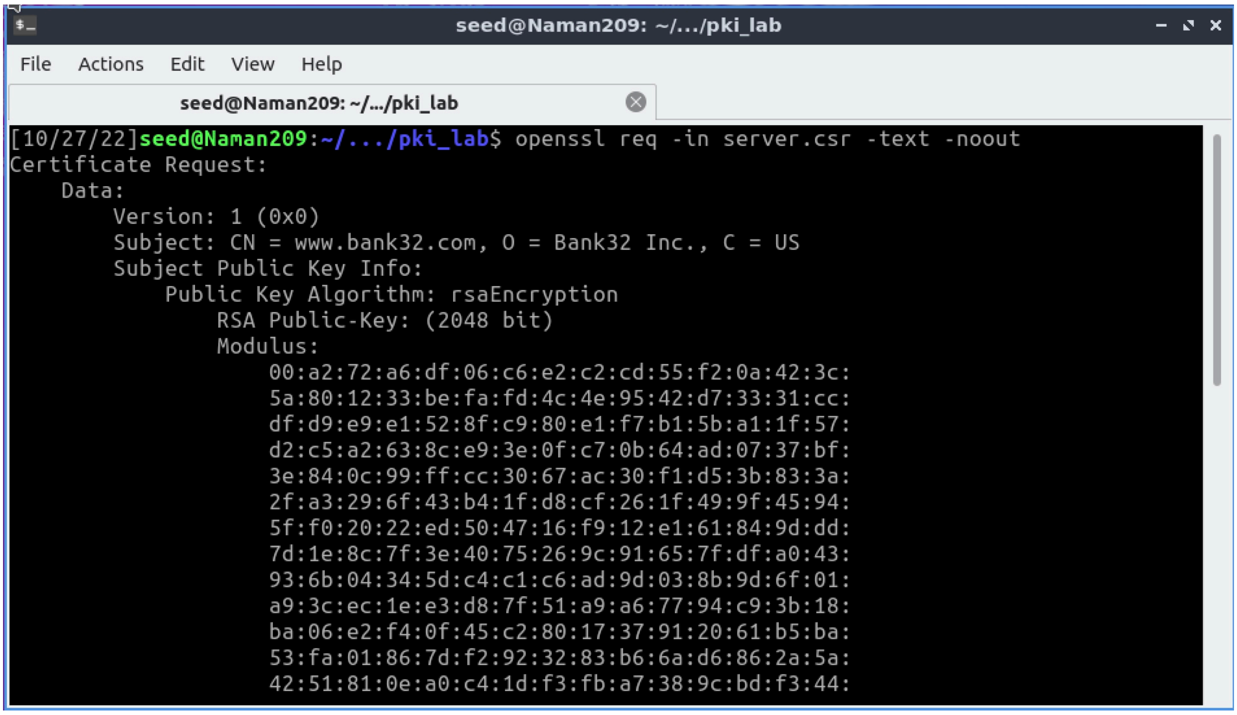
```
openssl req -newkey rsa:2048 -sha256
-keyout server.key
-out server.csr
-subj "/CN=www.bank32.com/O=Bank32 Inc./C=US"
-passout pass:dees
-addext "subjectAltName = DNS:www.bank32.
DNS:www.bank32A.com, \
DNS:www.bank32B.com"
```



```
[10/27/22]seed@Naman209:~/.../pki_lab$ openssl req -newkey rsa:2048 -sha256 -keyout server.k
ey -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'
-----
[10/27/22]seed@Naman209:~/.../pki_lab$ 
```

Bash

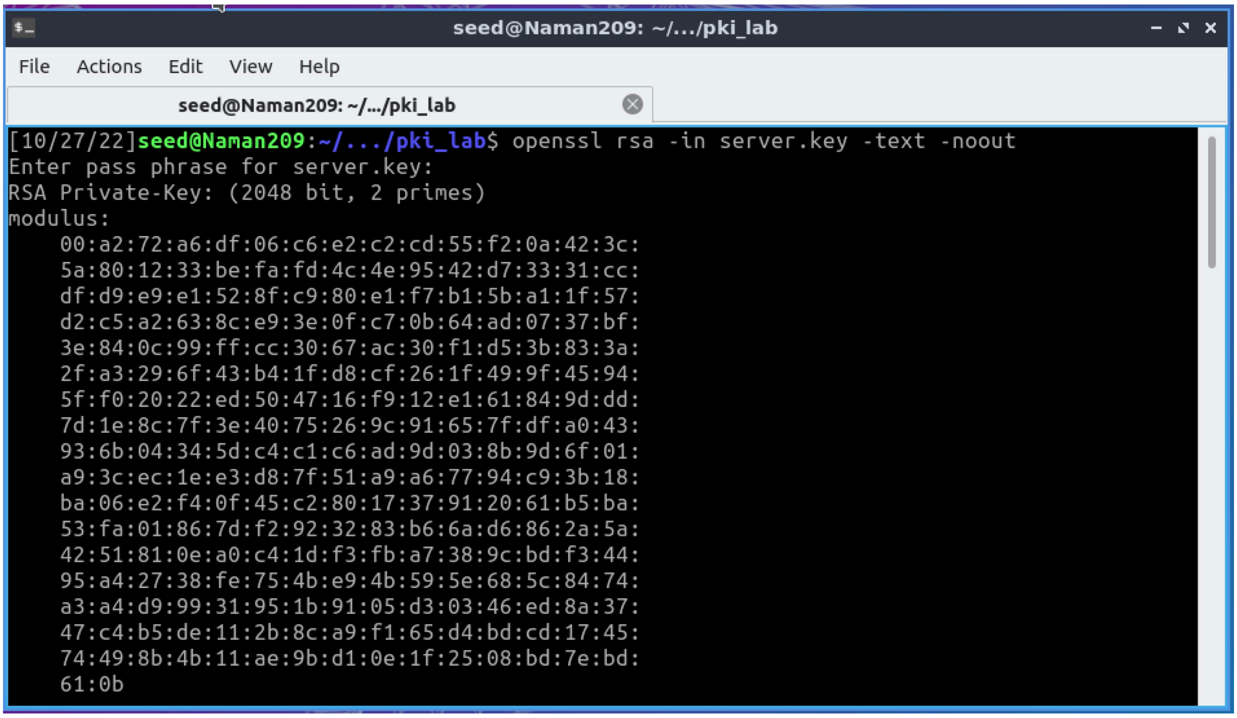
```
openssl req -in server.csr -text -noout
```



```
[10/27/22]seed@Naman209:~/.../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:a2:72:a6:df:06:c6:e2:c2:cd:55:f2:0a:42:3c:
                    5a:80:12:33:be:fa:fd:4c:4e:95:42:d7:33:31:cc:
                    df:d9:e9:e1:52:8f:c9:80:e1:f7:b1:5b:a1:1f:57:
                    d2:c5:a2:63:8c:e9:3e:0f:c7:0b:64:ad:07:37:bf:
                    3e:84:0c:99:ff:cc:30:67:ac:30:f1:d5:3b:83:3a:
                    2f:a3:29:6f:43:b4:1f:d8:cf:26:1f:49:9f:45:94:
                    5f:f0:20:22:ed:50:47:16:f9:12:e1:61:84:9d:dd:
                    7d:1e:8c:7f:3e:40:75:26:9c:91:65:7f:df:a0:43:
                    93:6b:04:34:5d:c4:c1:c6:ad:9d:03:8b:9d:6f:01:
                    a9:3c:ec:1e:e3:d8:7f:51:a9:a6:77:94:c9:3b:18:
                    ba:06:e2:f4:0f:45:c2:80:17:37:91:20:61:b5:ba:
                    53:fa:01:86:7d:f2:92:32:83:b6:6a:d6:86:2a:5a:
                    42:51:81:0e:a0:c4:1d:f3:fb:a7:38:9c:bd:f3:44:
```

Bash

```bash
openssl rsa -in server.key -text -noout
```

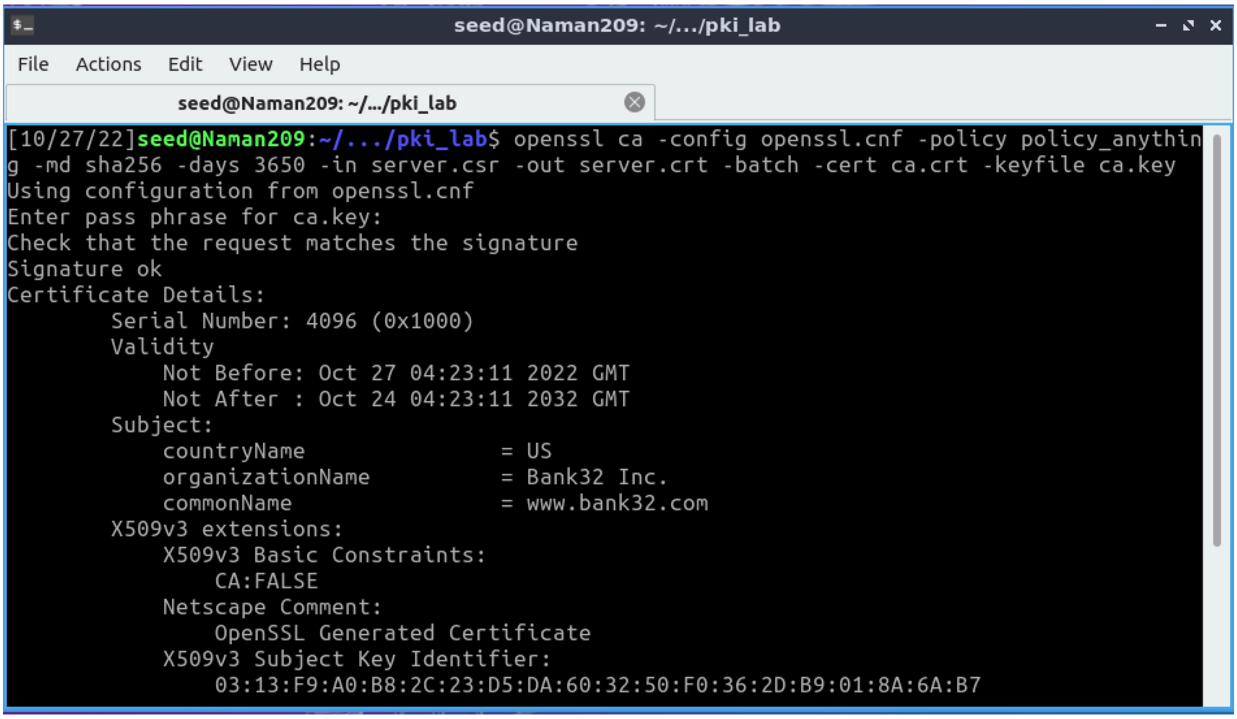


```
[10/27/22]seed@Naman209:~/.../pki_lab$ openssl rsa -in server.key -text -noout
Enter pass phrase for server.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
    00:a2:72:a6:df:06:c6:e2:c2:cd:55:f2:0a:42:3c:
    5a:80:12:33:be:fa:fd:4c:4e:95:42:d7:33:31:cc:
    df:d9:e9:e1:52:8f:c9:80:e1:f7:b1:5b:a1:1f:57:
    d2:c5:a2:63:8c:e9:3e:0f:c7:0b:64:ad:07:37:bf:
    3e:84:0c:99:ff:cc:30:67:ac:30:f1:d5:3b:83:3a:
    2f:a3:29:6f:43:b4:1f:d8:cf:26:1f:49:9f:45:94:
    5f:f0:20:22:ed:50:47:16:f9:12:e1:61:84:9d:dd:
    7d:1e:8c:7f:3e:40:75:26:9c:91:65:7f:df:a0:43:
    93:6b:04:34:5d:c4:c1:c6:ad:9d:03:8b:9d:6f:01:
    a9:3c:ec:1e:e3:d8:7f:51:a9:a6:77:94:c9:3b:18:
    ba:06:e2:f4:0f:45:c2:80:17:37:91:20:61:b5:ba:
    53:fa:01:86:7d:f2:92:32:83:b6:6a:d6:86:2a:5a:
    42:51:81:0e:a0:c4:1d:f3:fb:a7:38:9c:bd:f3:44:
    95:a4:27:38:fe:75:4b:e9:4b:59:5e:68:5c:84:74:
    a3:a4:d9:99:31:95:1b:91:05:d3:03:46:ed:8a:37:
    47:c4:b5:de:11:2b:8c:a9:f1:65:d4:bd:cd:17:45:
    74:49:8b:4b:11:ae:9b:d1:0e:1f:25:08:bd:7e:bd:
    61:0b
```

Task 3:Generating a Certificate for your server

Bash

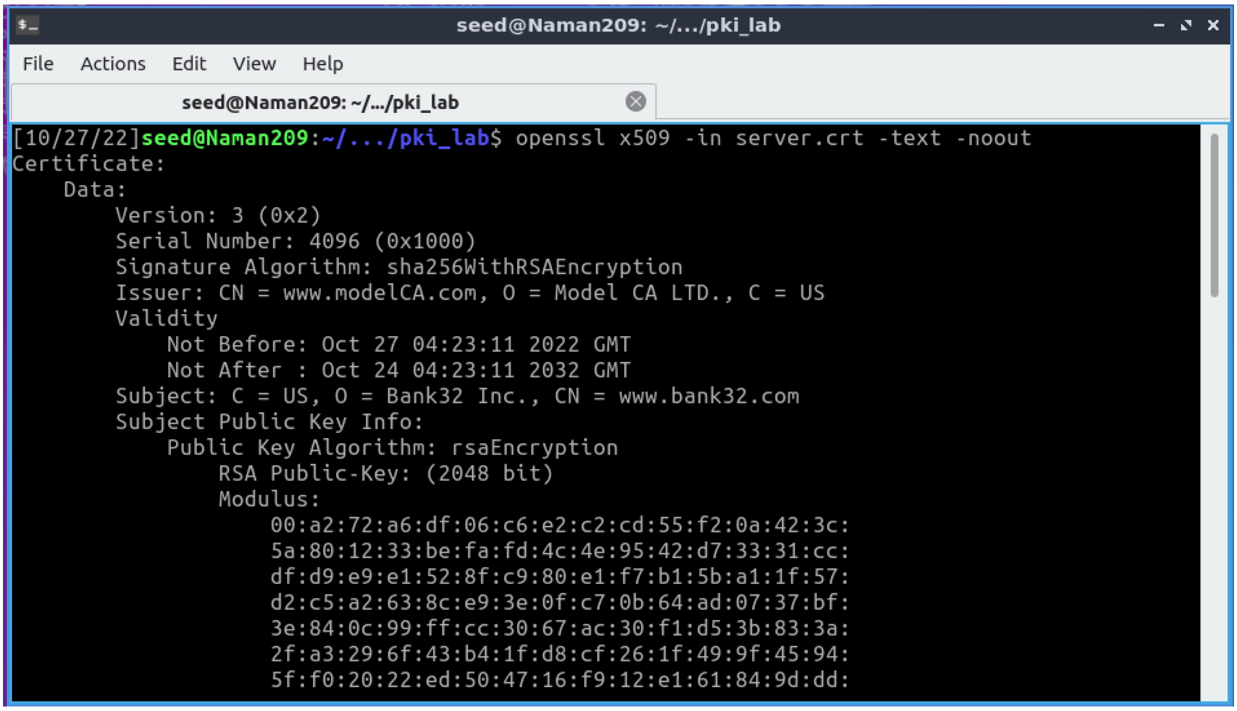
```bash
openssl ca -config openssl.cnf
-policy policy_anything -md sha256 -days 3650
-in server.csr -out server.crt
-batch -cert ca.crt
-keyfile ca.key
```



```
[10/27/22]seed@Naman209:~/.../pki_lab$ openssl ca -config openssl.cnf -policy policy_anythin
g -md sha256 -days 3650 -in server.csr -out server.crt -batch -cert ca.crt -keyfile ca.key
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Oct 27 04:23:11 2022 GMT
            Not After : Oct 24 04:23:11 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:
                03:13:F9:A0:B8:2C:23:D5:DA:60:32:50:F0:36:2D:B9:01:8A:6A:B7
```

Bash

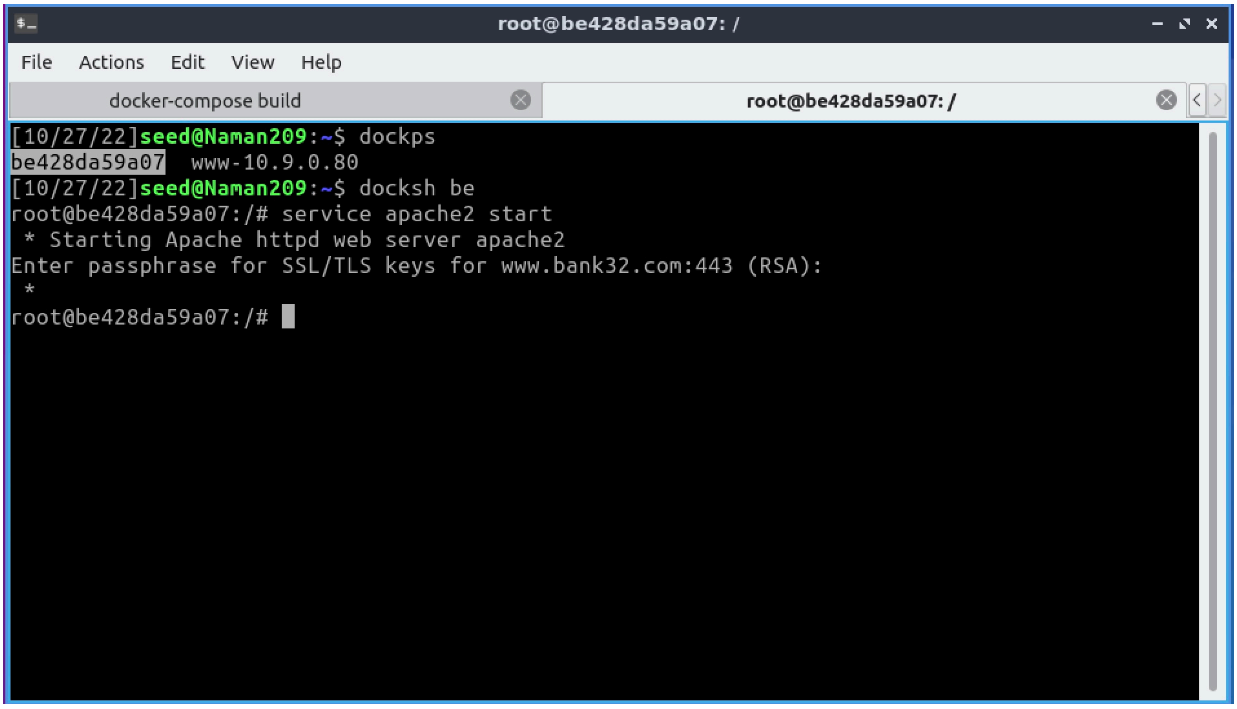
```bash
openssl x509 -in server.crt -text -noout
```



```
[10/27/22]seed@Naman209:~/.../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: Oct 27 04:23:11 2022 GMT
            Not After : Oct 24 04:23:11 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:a2:72:a6:df:06:c6:e2:c2:cd:55:f2:0a:42:3c:
                    5a:80:12:33:be:fa:fd:4c:4e:95:42:d7:33:31:cc:
                    df:d9:e9:e1:52:8f:c9:80:e1:f7:b1:5b:a1:1f:57:
                    d2:c5:a2:63:8c:e9:3e:0f:c7:0b:64:ad:07:37:bf:
                    3e:84:0c:99:ff:cc:30:67:ac:30:f1:d5:3b:83:3a:
                    2f:a3:29:6f:43:b4:1f:d8:cf:26:1f:49:9f:45:94:
                    5f:f0:20:22:ed:50:47:16:f9:12:e1:61:84:9d:dd:
```

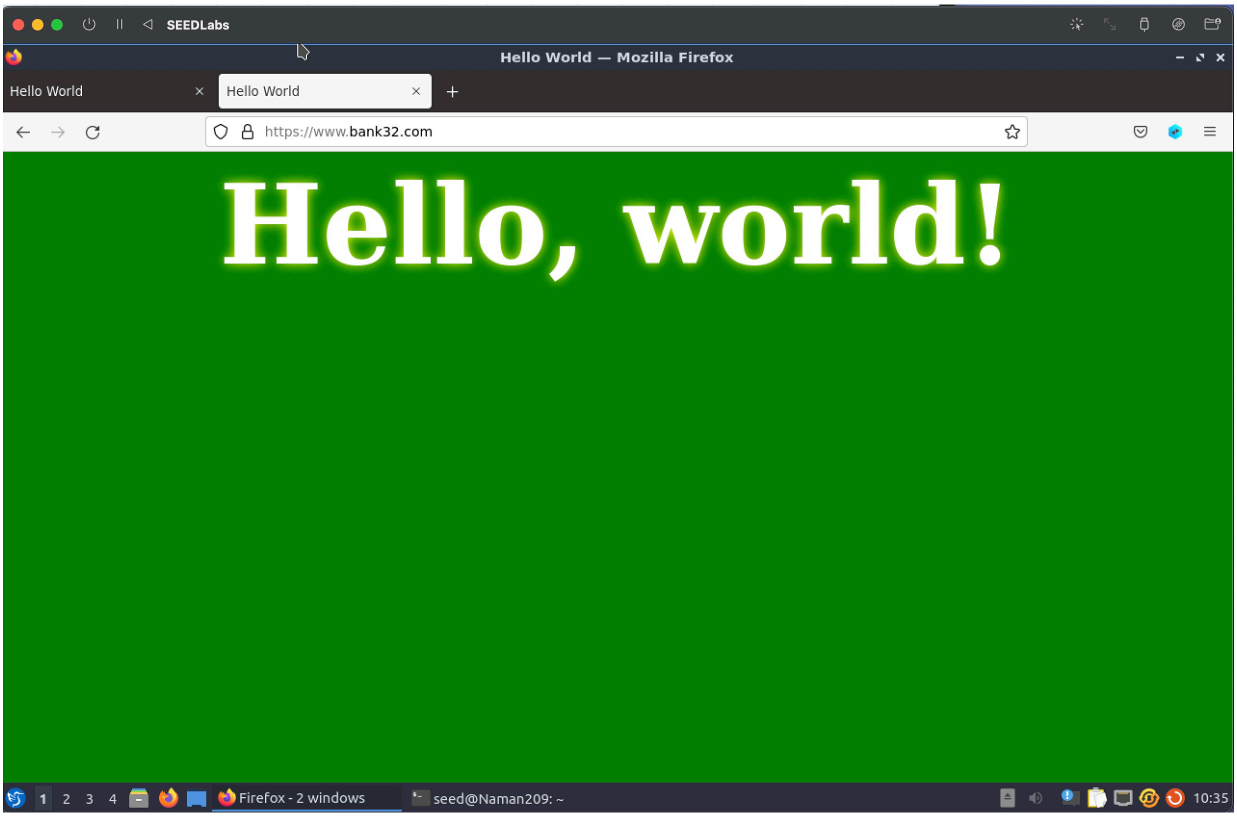
Task 4:Deploying Certificate in an Apache-Based HTTPS Website

```bash
dock ps
docksh <id of container>
```

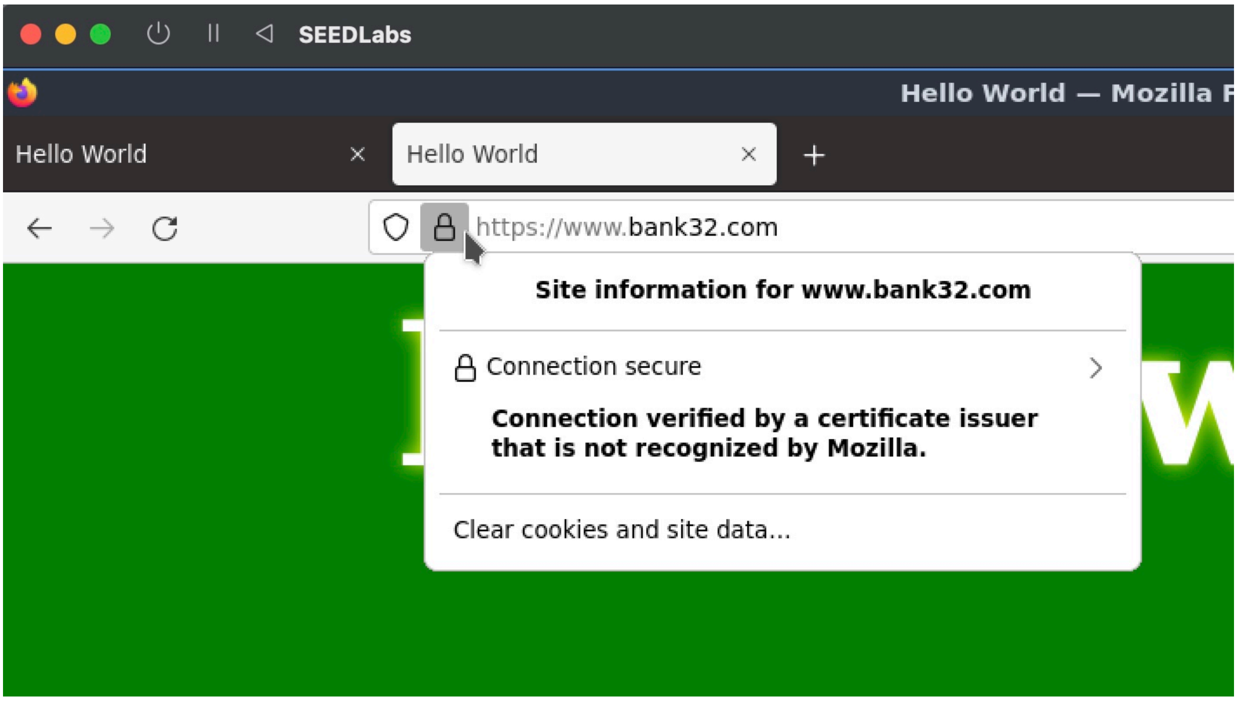


```
[10/27/22]seed@Naman209:~$ dockps
be428da59a07  www-10.9.0.80
[10/27/22]seed@Naman209:~$ docksh be
root@be428da59a07:/# service apache2 start
 * Starting Apache httpd web server apache2
Enter passphrase for SSL/TLS keys for www.bank32.com:443 (RSA):
 *
root@be428da59a07:/# 
```

Open `bank32.com`



Security:

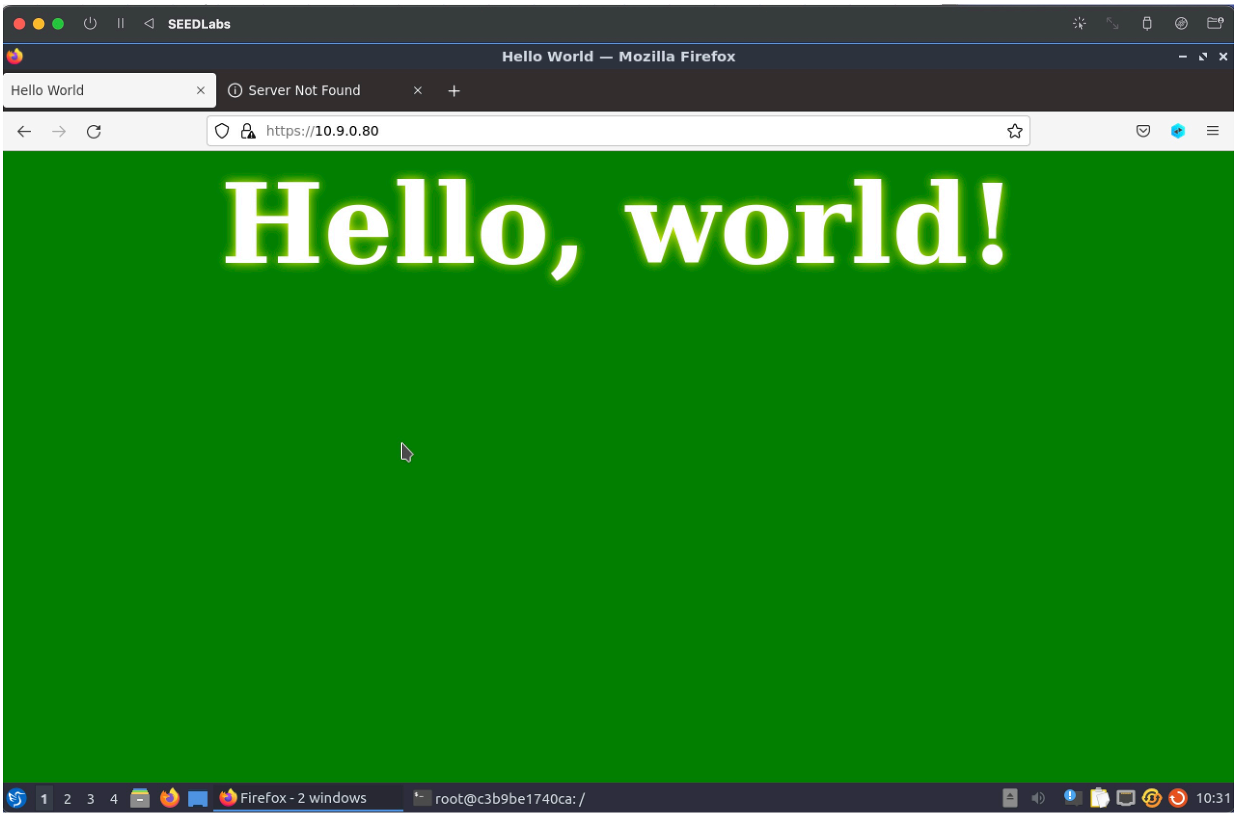


Site information for www.bank32.com

Connection secure

Connection verified by a certificate issuer that is not recognized by Mozilla.

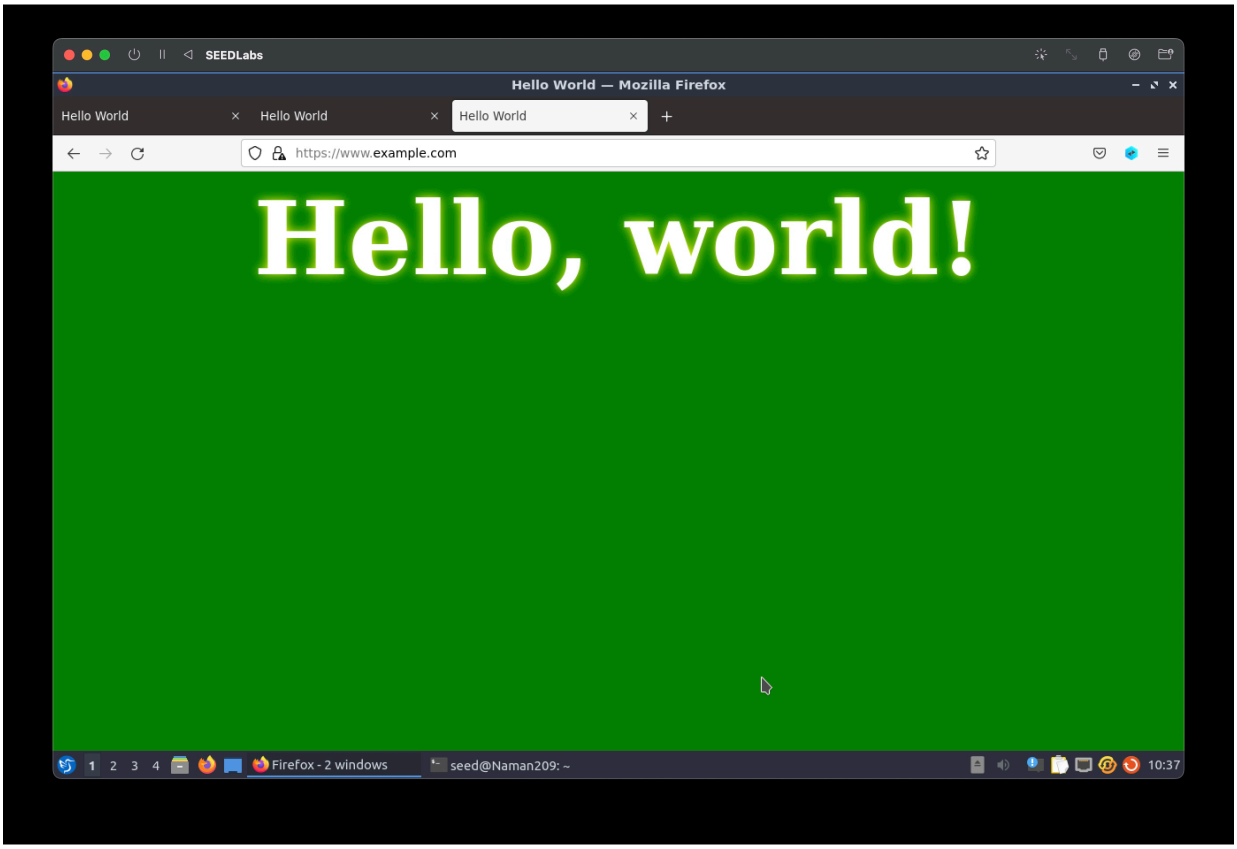
Open `10.9.0.80`



Observation: We are taken to the same website after entering the ip address of the website directly

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

Open `example.com`



Observation: Now, in spite of example.com being a valid domain of a different website, we are still taken to our malicious website with the ip `10.9.0.80` , this shows that the attack was successful.