Experiment 5

Output:

```
student@ubuntu:~/Desktop$ cd
student@ubuntu:~$ sudo su
[sudo] password for student:
root@ubuntu:/home/student# nano /usr/lib/ssl/misc/CA.pl
root@ubuntu:/home/student# gedit /usr/lib/ssl/openssl.cnf
```

```
root@ubuntu:/home/student# ls
amar       dec         Downloads  msg       private.pem  snap
amar1      demoCA      enc        Music     Public       Templates
amar2      Desktop     krishna    Pictures  rohan.txt    user1.pem
bootcamp   Documents   milk.txt   pri       san          Videos
root@ubuntu:/home/student# /usr/lib/ssl/misc/CA.pl -newca
CA certificate filename (or enter to create)
prime
readline() on closed filehandle IN at /usr/lib/ssl/misc/CA.pl line 95.
readline() on closed filehandle IN at /usr/lib/ssl/misc/CA.pl line 95.
root@ubuntu:/home/student# /usr/lib/ssl/misc/CA.pl -newca
CA certificate filename (or enter to create)
```

```
readline() on closed filehandle IN at /usr/lib/ssl/misc/CA.pl line 95.
root@ubuntu:/home/student# /usr/lib/ssl/misc/CA.pl -newca
CA certificate filename (or enter to create)

Making CA certificate ...
====
openssl req  -new -keyout ./demoCA/private/cakey.pem -out ./demoCA/careq.pem
Generating a RSA private key
.....................................................+++++
.............+++++
writing new private key to './demoCA/private/cakey.pem'
Enter PEM pass phrase:
140188099069248:error:28078065:UI routines:UI_set_result_ex:result too small:../crypto/ui/ui_lib.c:905:You must type in 4 to
140188099069248:error:2807106B:UI routines:UI_process:processing error:../crypto/ui/ui_lib.c:545:while reading strings
140188099069248:error:0906406D:PEM routines:PEM_def_callback:problems getting password:../crypto/pem/pem_lib.c:59:
140188099069248:error:0907E06F:PEM routines:do_pk8pkey:read key:../crypto/pem/pem_pk8.c:83:
==> 256
====
root@ubuntu:/home/student# /usr/lib/ssl/misc/CA.pl -newca
CA certificate filename (or enter to create)

Making CA certificate ...
====
openssl req  -new -keyout ./demoCA/private/cakey.pem -out ./demoCA/careq.pem
Generating a RSA private key
.....................................................................................................................
```

```
.............+++++
writing new private key to './demoCA/private/cakey.pem'
Enter PEM pass phrase:
140599095825728:error:28078065:UI routines:UI_set_result_ex:result too small:../crypto/ui/ui_lib.c:905:You must type in 4 to
140599095825728:error:2807106B:UI routines:UI_process:processing error:../crypto/ui/ui_lib.c:545:while reading strings
```

```
Making CA certificate ...
====
openssl req  -new -keyout ./demoCA/private/cakey.pem -out ./demoCA/careq.pem
Generating a RSA private key
.....................................................................................................................
.............+++++
writing new private key to './demoCA/private/cakey.pem'
Enter PEM pass phrase:
140599095825728:error:28078065:UI routines:UI_set_result_ex:result too small:../crypto/ui/ui_lib.c:905:You must type in 4 to
140599095825728:error:2807106B:UI routines:UI_process:processing error:../crypto/ui/ui_lib.c:545:while reading strings
140599095825728:error:0906406D:PEM routines:PEM_def_callback:problems getting password:../crypto/pem/pem_lib.c:59:
140599095825728:error:0907E06F:PEM routines:do_pk8pkey:read key:../crypto/pem/pem_pk8.c:83:
==> 256
====
root@ubuntu:/home/student# /usr/lib/ssl/misc/CA.pl -newca
CA certificate filename (or enter to create)

Making CA certificate ...
====
openssl req  -new -keyout ./demoCA/private/cakey.pem -out ./demoCA/careq.pem
Generating a RSA private key
.....................................................................+++++
.....................................................+++++
writing new private key to './demoCA/private/cakey.pem'
```

```
writing new private key to './demoCA/private/cakey.pem'
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.
```

```
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]:IN
State or Province Name (full name) [Some-State]:Maharashtra
Locality Name (eg, city) []:Mumbai
Organization Name (eg, company) [Internet Widgits Pty Ltd]:XIE
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:Cloud
Email Address []:xie@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Cloud
An optional company name []:XIE
==> 0
====
====
```

```
openssl ca  -create_serial -out ./demoCA/cacert.pem -days 1095 -batch -keyfile ./demoCA/private/cakey.pem -selfsign -extensi
es ./demoCA/careq.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            36:61:1b:0b:87:dd:cb:b3:01:eb:70:bf:f2:ea:c9:44:97:5c:b9:1d
        Validity
```

```
openssl ca  -create_serial -out ./demoCA/cacert.pem -days 1095 -batch -keyfile ./demoCA/private/cakey.pem -selfsign -extensions v3_ca  -infil
es ./demoCA/careq.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            36:61:1b:0b:87:dd:cb:b3:01:eb:70:bf:f2:ea:c9:44:97:5c:b9:1d
        Validity
            Not Before: Sep 14 07:45:02 2022 GMT
            Not After : Sep 13 07:45:02 2025 GMT
        Subject:
            countryName               = IN
            stateOrProvinceName       = Maharashtra
            organizationName          = XIE
            organizationalUnitName    = IT
            commonName                = Cloud
            emailAddress              = xie@gmail.com
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                A8:6F:38:64:87:32:13:E4:4E:ED:93:6A:74:30:0D:24:20:AF:DD:4A
            X509v3 Authority Key Identifier:
                keyid:A8:6F:38:64:87:32:13:E4:4E:ED:93:6A:74:30:0D:24:20:AF:DD:4A

            X509v3 Basic Constraints: critical
                CA:TRUE
Certificate is to be certified until Sep 13 07:45:02 2025 GMT (1095 days)

Write out database with 1 new entries
Data Base Updated
==> 0
====
CA certificate is in ./demoCA/cacert.pem
root@ubuntu:/home/student# nano /usr/lib/ssl/misc/CA.pl
```

```
student@ubuntu:~$ sudo su
[sudo] password for student:
root@ubuntu:/home/student# cd
root@ubuntu:~# ls
demoCA  krishna  snap
root@ubuntu:~# mkdir xie
root@ubuntu:~# cd xie
root@ubuntu:~/xie# openssl req -new -keyout privatekey.pen -out requser.pem
Generating a RSA private key
.....................................................................................................................................
++
.......+++++
writing new private key to 'privatekey.pen'
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]:IN
State or Province Name (full name) [Some-State]:Maharashtra
Locality Name (eg, city) []:Mumbai
Organization Name (eg, company) [Internet Widgits Pty Ltd]:XIE
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:XIE
Email Address []:xie@gmail.com
```

```
70NVvT0qw0ax/UVOxDZdz/hLbVjVr3zPXcCFRK8wFDETkhvw+h/L1wbADv8XLeV9
9ZyyPRcSE/8kqhl6he5/i95Jh+KrzXa808cRcDunM4U/QjaL6fX5fXf2RnjCWCuh
P1veMF5eJJl9Kb/HpGrWucJNgYcqzOgfOzXmXdU0mhSwb06d4CiKfGQKf/c8zBin
DxNycqQUNUIC6QOQsXJBDJbvlHVfA1GnpWCYhRhaQMGLPfy3MFmjwL5IglGNzI7d
NxCZSLiqvEy/aaEm5RwDi/74OGuY92T0CA==
-----END CERTIFICATE-----
Data Base Updated
root@ubuntu:~/krishna# cd demoCA/
bash: cd: demoCA/: No such file or directory
root@ubuntu:~/krishna# ls
privatekey.pen  requser.pem
root@ubuntu:~/krishna# cd ..
root@ubuntu:~# cd demoCA/
root@ubuntu:~/demoCA# ls
cacert.pem  certs  crlnumber  index.txt.attr      index.txt.old  private  serial.old
careq.pem   crl    index.txt  index.txt.attr.old  newcerts       serial
root@ubuntu:~/demoCA# cd newcerts/
root@ubuntu:~/demoCA/newcerts# ls
19A9C50B3DC233A99E29691D0DBE3E0A3B686AEB.pem  19A9C50B3DC233A99E29691D0DBE3E0A3B686AEC.pem  19A9C50B3DC233A99E29691D0DBE3E0A3B686AED.pem
root@ubuntu:~/demoCA/newcerts# cd
root@ubuntu:~# openssl verify -CAfile demoCA/cacert.pem demoCA/newcerts/19A9C50B3DC233A99E29691D0DBE3E0A3B686AEB.pem
C = in, ST = maha, O = xie, OU = bachc, CN = amari, emailAddress = amarsingh@gmail.com
error 18 at 0 depth lookup: self signed certificate
error demoCA/newcerts/19A9C50B3DC233A99E29691D0DBE3E0A3B686AEB.pem: verification failed
root@ubuntu:~# openssl verify -CAfile demoCA/cacert.pem demoCA/newcerts/9A9C50B3DC233A99E29691D0DBE3E0A3B686AED.pem
Can't open demoCA/newcerts/9A9C50B3DC233A99E29691D0DBE3E0A3B686AED.pem for reading, No such file or directory
140033959703872:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:69:fopen('demoCA/newcerts/9A9C50B3DC23
3A99E29691D0DBE3E0A3B686AED.pem','r')
140033959703872:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:
unable to load certificate
root@ubuntu:~# openssl verify -CAfile demoCA/cacert.pem demoCA/newcerts/19A9C50B3DC233A99E29691D0DBE3E0A3B686AEC.pem
demoCA/newcerts/19A9C50B3DC233A99E29691D0DBE3E0A3B686AEC.pem: OK
root@ubuntu:~# openssl verify -CAfile demoCA/cacert.pem demoCA/newcerts/19A9C50B3DC233A99E29691D0DBE3E0A3B686AED.pem
demoCA/newcerts/19A9C50B3DC233A99E29691D0DBE3E0A3B686AED.pem: OK
```

```
student@ubuntu:~$ gedit krishna.txt
student@ubuntu:~$ gedit milk.txt
^C
student@ubuntu:~$ sha256sum milk.txt
5891b5b522d5df086d0ff0b110fbd9d21bb4fc7163af34d08286a2e846f6be03  milk.txt
student@ubuntu:~$ ls
amar   bootcamp  Documents  krishna   Music     Public     snap
amar1  dec       Downloads  milk.txt  Pictures  rohan.txt  Templates
amar2  Desktop   enc        msg       pri       san        Videos
student@ubuntu:~$ gedit milk.txt
^C
student@ubuntu:~$ sha256sum milk.txt
815fb346d129829cf8056d7ce8475275df28dc9bf3c37d1208e30a18c2341949  milk.txt
student@ubuntu:~$
```