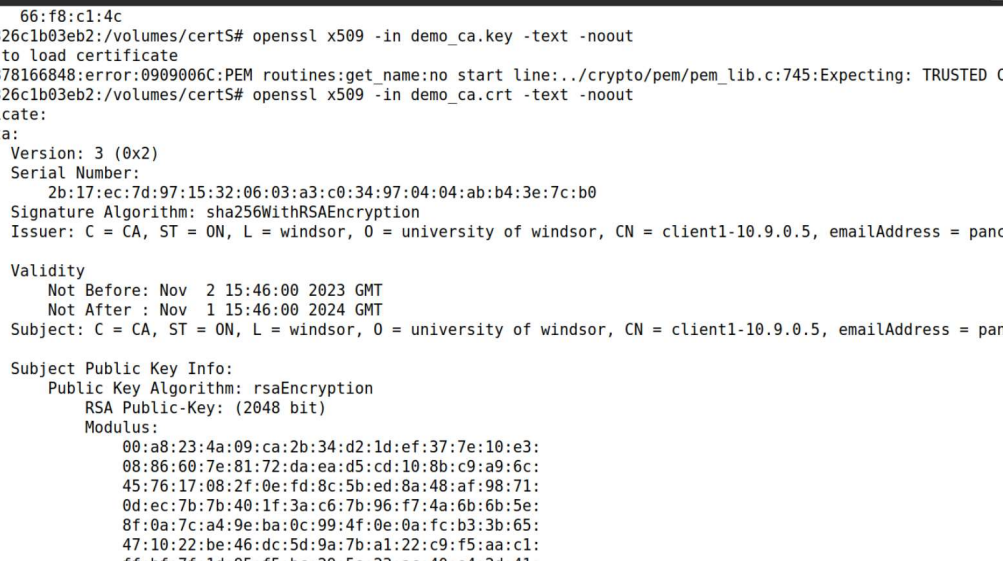


**SCREENSHOT OF SERVER CERTIFICATE:**

```
/*using openssl x509 -in your_server_cert -text -noout */
```



```
66:f8:c1:4c
root@8326c1b03eb2:/volumes/cert5# openssl x509 -in demo_ca.key -text -noout
unable to load certificate
139909878166848:error:0909006C:PEM routines:get_name:no start line:../crypto/pem/pem_lib.c:745:Expecting: TRUSTED CERTIFICATE
root@8326c1b03eb2:/volumes/cert5# openssl x509 -in demo_ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            2b:17:ec:7d:97:15:32:06:03:a3:c0:34:97:04:04:ab:b4:3e:7c:b0
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = CA, ST = ON, L = windsor, O = university of windsor, CN = client1-10.9.0.5, emailAddress = pancha16@uwindsor.ca
        Validity
            Not Before: Nov  2 15:46:00 2023 GMT
            Not After : Nov  1 15:46:00 2024 GMT
        Subject: C = CA, ST = ON, L = windsor, O = university of windsor, CN = client1-10.9.0.5, emailAddress = pancha16@uwindsor.ca
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public-Key: (2048 bit)
            Modulus:
                00:a8:23:4a:09:ca:2b:34:d2:1d:ef:37:7e:10:e3:
                08:86:60:7e:81:72:da:ea:d5:cd:10:8b:c9:a9:6c:
                45:76:17:08:2f:0e:fd:8c:5b:ed:8a:48:af:98:71:
                0d:ec:7b:7b:40:1f:3a:c6:7b:96:f7:4a:6b:6b:5e:
                8f:0a:7c:a4:9e:ba:0c:99:4f:0e:0a:fc:b3:3b:65:
                47:10:22:be:46:dc:5d:9a:7b:a1:22:c9:f5:aa:c1:
                ff:bf:7f:1d:95:f5:bc:29:5e:23:ac:40:e4:2d:41:
                ff:47:11:dd:fd:30:ff:4f:fb:4a:ef:90:b8:03:8f:
```

The screenshot shows a Kali Linux desktop environment with a terminal window titled "seed@VM: ~/.../lab6". The terminal displays the output of the command `openssl x509 -text` applied to a file named `cert.pem`. The output details the X509v3 extensions section of the certificate.

```
Nov 2 14:13  
seed@VM: ~/.../lab6  
47:10:22:be:46:dc:5d:9a:7b:a1:22:c9:f5:aa:c1:  
ff:bf:7f:1d:95:f5:bc:29:5e:23:ac:40:e4:2d:41:  
ff:47:11:dd:f3:00:ff:4f:fb:4a:ef:90:b8:03:8f:  
bb:61:de:a8:c4:17:a3:59:49:be:76:bb:d3:fd:00:  
85:3c:61:b1:56:a3:74:c8:4c:9c:e0:c0:55:19:74:  
6f:80:bb:34:8f:c6:46:65:1b:a6:16:89:1f:22:f2:  
4d:ae:4a:9f:29:43:06:9e:10:d0:7c:bf:2a:43:64:  
f5:f5:66:f0:9e:b9:a0:94:ec:e2:c6:50:56:f6:3a:  
5c:ab:23:31:fd:38:ef:ec:94:d1:d6:ff:dc:7b:ac:  
1a:bf:d9:a6:08:be:98:23:f9:66:95:ce:7d:ec:23:  
47:f9:04:8b:04:14:12:04:bd:5c:6c:57:6c:73:ac:  
e0:4d:61:b7:a3:fe:5c:1e:8b:98:e3:08:21:da:95:  
42:2b  
Exponent: 65537 (0x10001)  
X509v3 extensions:  
    X509v3 Subject Key Identifier:  
        9C:C0:EB:B1:2F:5C:54:C7:6C:83:5A:81:DC:86:A4:6A:56:D1:1C:01  
    X509v3 Authority Key Identifier:  
        keyid:9C:C0:EB:B1:2F:5C:54:C7:6C:83:5A:81:DC:86:A4:6A:56:D1:1C:01  
  
    X509v3 Basic Constraints: critical  
        CA:TRUE  
Signature Algorithm: sha256WithRSAEncryption  
34:85:4c:3c:fd:a3:10:22:d2:34:28:26:8c:25:fc:76:6f:da:  
db:94:e0:d4:d0:29:76:59:ea:84:bb:4d:84:8e:8b:01:8f:60:  
a4:b0:84:4a:db:61:f0:e8:40:64:83:a5:78:6d:45:7b:df:45:  
83:30:3e:af:35:96:22:fa:1a:05:39:c5:5b:cf:45:7c:05:84:  
fa:2e:08:6a:39:97:29:3c:1f:95:98:9d:8f:c8:64:7c:bf:37:  
b4:65:40:79:c1:4e:c3:0d:05:d2:c1:37:02:ef:04:61:c2:08:  
20:fb:6a:1d:a1:c9:ca:80:97:74:c9:07:65:ca:17:a5:ac:da:
```

```
SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
Activities Terminal Nov 2 14:13
seed@VM: ~/lab6

1a:bf:d9:a6:08:be:98:23:f9:66:95:ce:7d:ec:23:
47:f9:04:8b:04:14:12:04:bd:5c:6c:57:6c:73:ac:
e0:4d:61:b7:a3:fe:5c:1e:8b:98:e3:08:21:da:95:
42:2b
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
9C:C0:EB:B1:2F:5C:54:C7:6C:83:5A:81:DC:86:A4:6A:56:D1:1C:01
X509v3 Authority Key Identifier:
keyid:9C:C0:EB:B1:2F:5C:54:C7:6C:83:5A:81:DC:86:A4:6A:56:D1:1C:01

X509v3 Basic Constraints: critical
CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
34:85:4c:3c:fd:a3:10:22:d2:34:28:26:8c:25:fc:76:6f:da:
db:94:e0:d4:d0:29:76:59:ea:84:bb:4d:84:8e:8b:01:8f:60:
a4:b0:84:4a:db:61:f0:e8:40:64:83:a5:78:6d:45:7b:df:45:
83:30:3e:af:35:96:22:fa:1a:05:39:c5:5b:cf:45:7c:05:84:
fa:2e:08:6a:39:97:29:3c:1f:95:98:9d:8f:c8:64:7c:bf:37:
b4:65:40:79:c1:4e:c3:0d:05:d2:c1:37:02:ef:04:61:c2:08:
20:fb:6a:1d:a1:c9:ca:80:97:74:c9:07:65:ca:17:a5:ac:da:
36:30:8b:d2:6e:d5:c0:0b:40:49:5c:78:66:fa:5b:e5:fb:85:
7e:b7:e7:0d:fa:e6:96:b1:02:75:a0:f7:6d:8e:4b:ed:7c:e5:
07:b4:de:fc:44:eb:3a:b7:61:17:56:45:a0:5b:f6:16:f2:db:
04:a8:99:a0:e2:b8:c7:5d:a9:80:4c:16:8a:a7:10:25:0e:72:
9a:b3:ae:38:f6:42:4e:94:d4:13:4a:99:ab:47:e9:06:69:03:
9b:8c:45:3b:9f:8d:e0:52:87:20:d4:48:c2:89:55:f6:33:52:
28:aa:0c:b2:b2:2f:0e:43:dd:47:f5:53:67:4a:25:05:4b:f8:
66:f8:c1:4c
root@8326c1b03eb2:/volumes/certS#
```