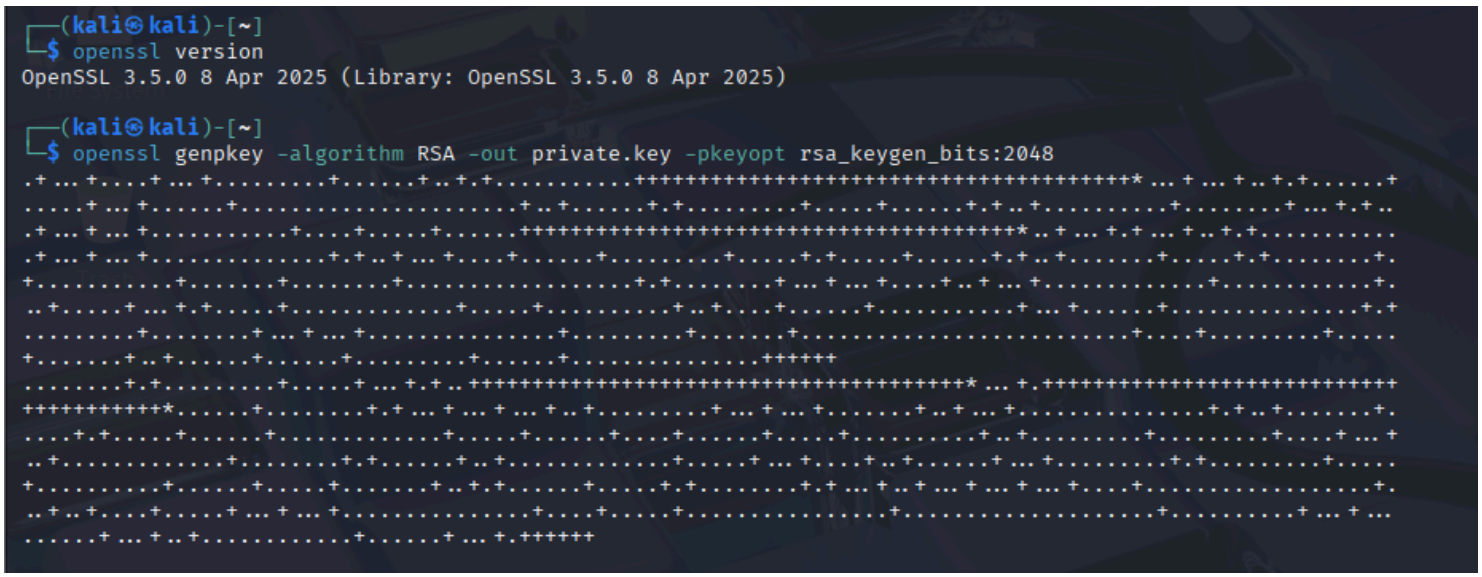
EXP 4

```
┌──(kali㉿kali)-[~]
└─$ openssl genpkey -algorithm RSA -out private.key -pkeyopt rsa_keygen_bits:2048
```



```
┌──(kali㉿kali)-[~]
└─$ openssl version
OpenSSL 3.5.0 8 Apr 2025 (Library: OpenSSL 3.5.0 8 Apr 2025)

┌──(kali㉿kali)-[~]
└─$ openssl genpkey -algorithm RSA -out private.key -pkeyopt rsa_keygen_bits:2048
```



```
File  Actions  Edit  View  Help
kali@kali: ~   kali@kali: ~

┌──(kali㉿kali)-[~]
└─$ openssl req -new -x509 -key private.key -out ritika.crt -days 365
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]:Jammu & Kashmir
Locality Name (eg, city) []:Jammu
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MIET
Organizational Unit Name (eg, section) []:CSE
Common Name (e.g. server FQDN or YOUR name) []:Ritika
Email Address []:rittika.jk@gmail.com
```

```
┌──(kali㉿kali)-[~]
└─$ openssl req -new -x509 -key private.key -out cert.pem -days 365 \
> -subj "/C=US/ST=State/L=City/O=Org/OU=Dept/CN=example.local"
```

kali@kali: ~ kali@kali: ~

```
└─$ openssl x509 -in ritika.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            47:6c:db:12:2d:89:d1:15:5c:4a:81:3c:e6:ec:68:58:cd:f9:c1:e7
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=IN, ST=Jammu & Kashmir, L=Jammu , O=MIET, OU=CSE, CN=Ritika, emailAddress=rittika.jk@gmail
.com
        Validity
            Not Before: Sep 16 05:16:18 2025 GMT
            Not After : Sep 16 05:16:18 2026 GMT
        Subject: C=IN, ST=Jammu & Kashmir, L=Jammu , O=MIET, OU=CSE, CN=Ritika, emailAddress=rittika.jk@gmai
l.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:db:6c:a0:78:ff:37:1b:ad:f2:15:81:1a:24:1d:
                    8e:13:a2:fc:46:b2:ba:d9:21:b1:c4:c7:6e:19:c9:
                    88:1e:b1:9c:4d:a6:3f:9e:e3:d5:6c:fa:01:40:c6:
                    e5:ed:71:86:eb:ee:a2:03:d4:25:19:ec:7d:9c:62:
                    98:ff:c6:42:2d:0c:e6:66:df:06:1e:fe:2b:b0:eb:
                    0e:f2:6c:8c:0c:74:ab:05:4e:e3:fa:6c:63:2b:c4:
                    c6:46:72:be:25:b3:5f:1d:02:96:71:30:67:6f:35:
                    ef:8e:4c:2c:04:23:81:cb:0b:b7:bd:16:14:44:0e:
                    ae:36:0b:8c:50:7b:24:3c:1f:e5:2b:13:f9:1b:62:
                    42:61:27:32:7c:04:35:c9:0a:ea:b3:1a:dc:f0:72:
                    64:5f:f1:1a:34:a4:c9:01:48:b0:73:8b:25:84:af:
                    aa:22:e4:70:1c:95:4e:9e:35:89:62:c1:6b:78:31:
                    6b:ff:41:eb:96:d0:b7:92:5d:74:09:10:2c:e5:ee:
                    fa:0d:40:4d:08:51:d7:eb:4d:84:14:3e:fe:6f:18:
                    c8:27:ec:04:6d:e2:8d:f0:ad:10:4d:7a:51:0d:10:
                    eb:19:19:13:36:7f:8a:14:1d:ec:d6:11:7f:0b:55:
                    21:98:67:cd:f1:33:1c:06:9f:62:c4:84:80:99:71:
                    35:eb
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                2B:42:F0:9D:66:D5:B0:C3:AA:2B:94:10:EA:20:89:A3:0F:A2:54:3C
            X509v3 Authority Key Identifier:
                2B:42:F0:9D:66:D5:B0:C3:AA:2B:94:10:EA:20:89:A3:0F:A2:54:3C
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
```

```
  GNU nano 8.6
[ req ]
distinguished_name = req_distinguished_name
req_extensions = req_ext
prompt = no

[ req_distinguished_name ]
C = US
ST = State
L = City
O = Org
OU = Dept
CN = example.local

[ req_ext ]
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = example.local
DNS.2 = localhost
IP.1 = 192.168.226.128
```

```
┌──(kali㉿kali)-[~]
└─$ openssl x509 -in ritika.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            47:6c:db:12:2d:89:d1:15:5c:4a:81:3c:e6:ec:68:58:cd:f9:c1:e7
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=IN, ST=Jammu & Kashmir, L=Jammu , O=MIET, OU=CSE, CN=Ritika, emailAddress=rittika.jk@gmail
.com
        Validity
            Not Before: Sep 16 05:16:18 2025 GMT
            Not After : Sep 16 05:16:18 2026 GMT
        Subject: C=IN, ST=Jammu & Kashmir, L=Jammu , O=MIET, OU=CSE, CN=Ritika, emailAddress=rittika.jk@gmai
l.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:db:6c:a0:78:ff:37:1b:ad:f2:15:81:1a:24:1d:
                    8e:13:a2:fc:46:b2:ba:d9:21:b1:c4:c7:6e:19:c9:
                    88:1e:b1:9c:4d:a6:3f:9e:e3:d5:6c:fa:01:40:c6:
                    e5:ed:71:86:eb:ee:a2:03:d4:25:19:ec:7d:9c:62:
                    98:ff:c6:42:2d:0c:e6:66:df:06:1e:fe:2b:b0:eb:
                    0e:f2:6c:8c:0c:74:ab:05:4e:e3:fa:6c:63:2b:c4:
                    c6:46:72:be:25:b3:5f:1d:02:96:71:30:67:6f:35:
                    ef:8e:4c:2c:04:23:81:cb:0b:b7:bd:16:14:44:0e:
                    ae:36:0b:8c:50:7b:24:3c:1f:e5:2b:13:f9:1b:62:
                    42:61:27:32:7c:04:35:c9:0a:ea:b3:1a:dc:f0:72:
                    64:5f:f1:1a:34:a4:c9:01:48:b0:73:8b:25:84:af:
                    aa:22:e4:70:1c:95:4e:9e:35:89:62:c1:6b:78:31:
                    6b:ff:41:eb:96:d0:b7:92:5d:74:09:10:2c:e5:ee:
                    fa:0d:40:4d:08:51:d7:eb:4d:84:14:3e:fe:6f:18:
                    c8:27:ec:04:6d:e2:8d:f0:ad:10:4d:7a:51:0d:10:
                    eb:19:19:13:36:7f:8a:14:1d:ec:d6:11:7f:0b:55:
                    21:98:67:cd:f1:33:1c:06:9f:62:c4:84:80:99:71:
                    35:eb
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                2B:42:F0:9D:66:D5:B0:C3:AA:2B:94:10:EA:20:89:A3:0F:A2:54:3C
            X509v3 Authority Key Identifier:
                2B:42:F0:9D:66:D5:B0:C3:AA:2B:94:10:EA:20:89:A3:0F:A2:54:3C
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        96:6e:8d:c0:9b:29:20:03:8f:31:1a:53:25:07:94:95:f0:cf:
        62:18:83:af:07:de:65:94:68:cb:89:cd:5a:a6:a3:65:eb:02:
        3d:bb:83:df:fd:0f:2f:b1:b2:13:90:30:ea:04:38:9e:89:a7:
        ee:d0:70:fb:1b:71:cd:e6:40:71:4b:37:66:a8:45:fd:02:15:
        50:db:ef:91:47:86:04:5b:26:4c:61:d9:90:b4:c1:6e:cf:ed:
        ad:1c:8d:d5:0a:7e:6c:2e:68:ed:ee:52:bc:f6:ef:00:b1:e1:
        d4:c7:16:f2:cc:f4:41:03:57:0a:ae:7b:69:e2:d4:ec:59:58:
        f0:5f:f5:a6:a1:a3:f8:62:20:dd:c4:65:b3:9b:65:cf:a2:97:
        ea:b0:ee:af:c0:42:35:89:13:9a:92:5b:23:9b:f9:cf:e6:85:
        bb:29:91:f0:94:52:09:f2:e8:29:48:14:a8:de:86:8b:5c:ed:
        20:1c:12:ea:32:c2:4d:75:bc:34:7c:24:32:97:b6:fb:30:c6:
        6a:c7:da:a6:18:b0:49:55:c4:2c:c0:e2:16:23:95:fb:c6:37:
        b8:14:3e:b9:49:20:64:20:2d:ad:3d:8e:20:cb:59:f5:f9:80:
        38:c6:0a:8c:eb:0b:71:08:e5:bd:e2:01:c4:67:e3:d4:be:63:
        b6:f9:66:ae
```

```
┌──(kali㉿kali)-[~]
└─$ openssl verify -CAfile ritika.crt ritika.crt
ritika.crt: OK
```

```
┌──(kali㉿kali)-[~]
└─$ openssl x509 -in cert.pem -noout -modulus -pubkey
Modulus=981E9E64641194C1ACD03AACF9817D0CCDB3C6D916B32AACD947A44123A2ADCD554CF53936D7B50E3A6123F9B9C266D7211
1C6643418E3C94AAE420CECACD86BC0FF5B06921D4F079D400EC1F506FE0B19523059B5595679D6F6AC6A8A7DA8D6DA1E6EF64A1116
F47EF845CDE5154A6055F23EB4A3A6DD04D9A49947DC0D397D54A9E4A7962E46EA07BCAB16043ED80EECEC6F53D5CBB251A6CA1B943
66703F97E26ECE26EE783E63A9036536B4A41919CD92DB46460CCC02BB4E518427808825E7C082383C0F0CB020312BDEAA98872E710
5F68B8ADF5459E6B3F9565D41D32BEE2C6DA01FDC7B0214D466C94AFAB0CFDFB3693690C08AFEEDA88DE08F66427
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmB6eZGQRlMGs0Dqs+YF9
DM2zxtkWsyqs2UekQSOirc1VTPU5Nte1DjphI/m5wmbXIRHGZDQY48lKrkIM7KzY
a8D/WwaSHU8HnUAOwfUG/gsZUjBZtVlWedb2rGqKfajW2h5u9koRFvR++EXN5RVK
YFXyPrSjpt0E2aSZR9wNOX1UqeSnli5G6ge8qxYEPtgO7OxvU9XLslGmyhuUNmcD
+X4m7OJu54PmOpA2U2tKQZGc2S20ZGDMwCu05RhCeAiCXnwII4PA8MsCAxK96qmI
cucQX2i4rfVFnms/lWXUHTK+4sbaAf3HsCFNRmyUr6sM/fs2k2kMCK/u2ojeCPZk
JwIDAQAB
-----END PUBLIC KEY-----
```

```
┌──(kali㉿kali)-[~]
└─$ openssl s_server -cert cert.pem -key private.key -accept 8443 -WWW
Using default temp DH parameters
ACCEPT
```

```
┌──(kali㉿kali)-[~]
└─$ import http.server, ssl
```

```
 GNU nano 8.6                                    python.py *
import http.server, ssl

httpd = http.server.HTTPServer(('0.0.0.0', 4443), http.server.SimpleHTTPRequestHandler)
httpd.socket = ssl.wrap_socket(httpd.socket, certfile='cert.pem', keyfile='private.key', server_side=True)
print("Serving on https://0.0.0.0:4443")
httpd.serve_forever()
```

```
 GNU nano 8.6                                    python.py *
import http.server, ssl

httpd = http.server.HTTPServer(('0.0.0.0', 4443), http.server.SimpleHTTPRequestHandler)
httpd.socket = ssl.wrap_socket(httpd.socket, certfile='cert.pem', keyfile='private.key', server_side=True)
print("Serving on https://0.0.0.0:4443")
httpd.serve_forever()
```

```
┌──(kali㉿kali)-[~]
└─$ openssl pkcs12 -export -out cert.pfx -inkey private.key -in cert.pem -password pass:yourpassword
```

```
┌──(kali㉿kali)-[~]
└─$ openssl x509 -in cert.pem -outform der -out cert.der
```