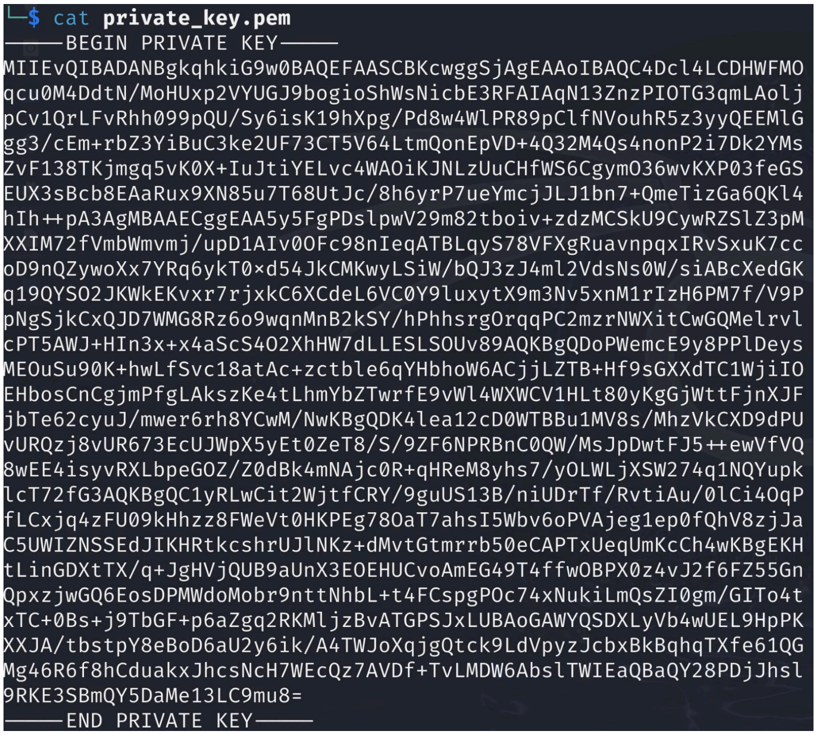
Malaika Sadiq
251686710

Information Security COMP 421
Section B
Assignment 2

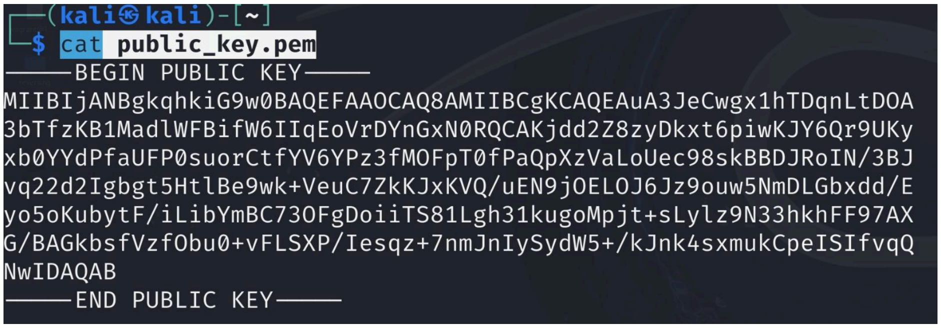
List of OpenSSL commands:

1) openssl genrsa -out private.key 2048
2) openssl rsa -in private.key -pubout -out public.key
3) cat private_key.pem
4) cat public_key.pem
5) openssl req -new -key private.key -out certificate.csr
6) openssl req -in certificate.csr -text -noout
7) openssl x509 -req -in certificate.csr -signkey private.key -out certificate.crt -days 365
8) openssl x509 -in certificate.crt -text -noout
9) openssl x509 -req -in certificate.csr -CA certificate.crt -CAkey private.key -CAcreateserial -out client.crt -days
10) openssl x509 -in client.crt -text -noout

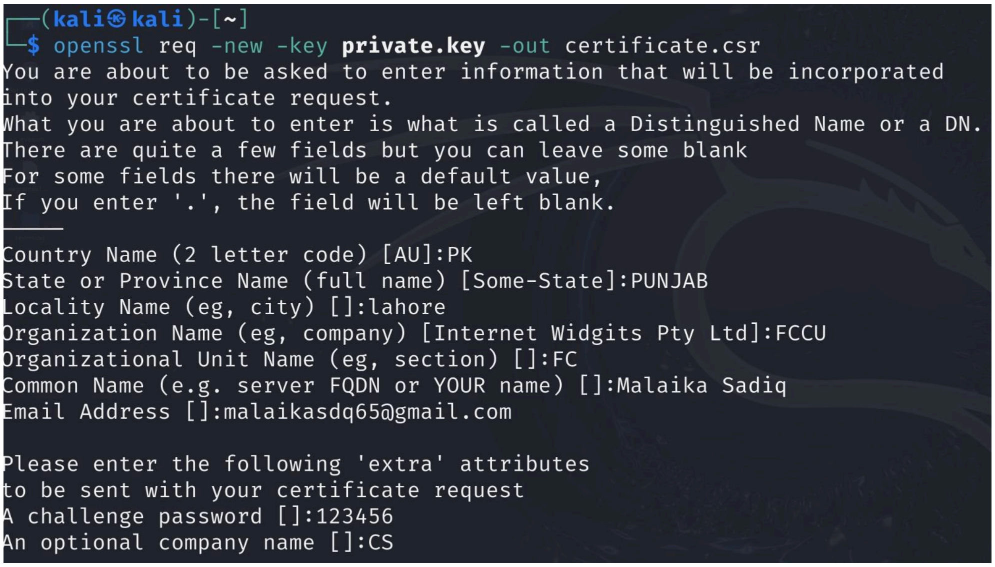
Screenshot of outputs:



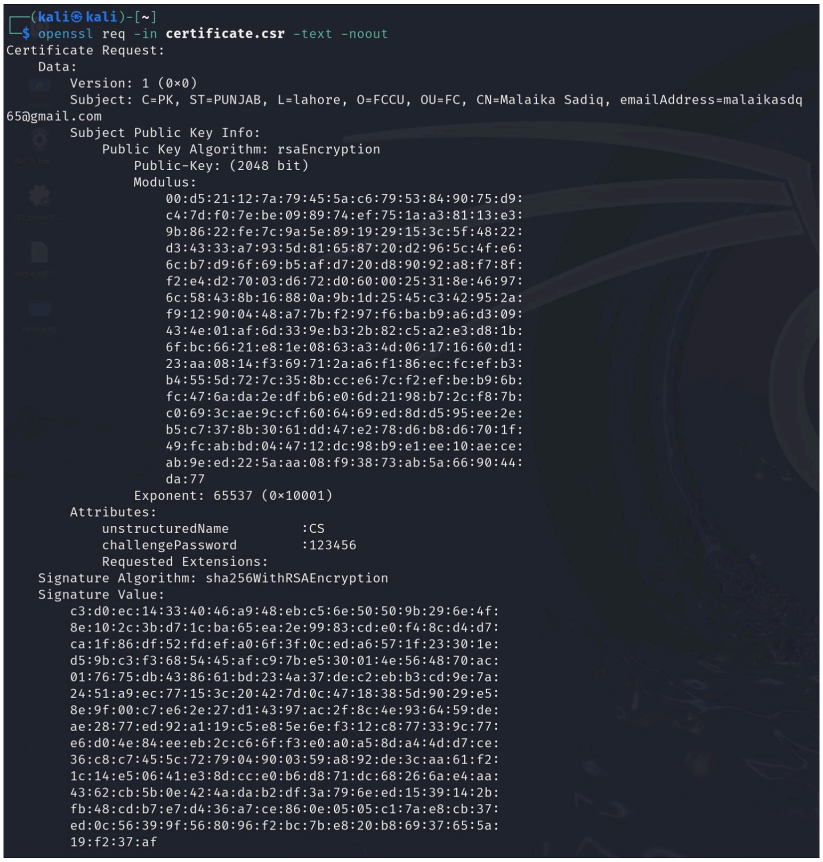
```
└─$ cat private_key.pem
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC4Dcl4LCDHWFMO
qcu0M4DdtN/MoHUxp2VYUGJ9bogioShWsNicbE3RFAIAqN13ZnzPIOTG3qmLAolj
pCv1QrLFvRhh099pQU/Sy6isK19hXpg/Pd8w4WlPR89pClfNVouhR5z3yyQEEMlG
gg3/cEm+rbZ3YiBuC3ke2UF73CT5V64LtmQonEpVD+4Q32M4Qs4nonP2i7Dk2YMs
ZvF138TKjmgq5vK0X+IuJtiYELvc4WAOiKJNLzUuCHfWS6CgymO36wvKXP03feGS
EUX3sBcb8EAaRux9XN85u7T68UtJc/8h6yrP7ueYmcjJLJ1bn7+QmeTizGa6QKl4
hIh++pA3AgMBAAECggEAA5y5FgPDslpwV29m82tboiv+zdzMCSkU9CywRZSlZ3pM
XXIM72fVmbWmvmj/upD1AIv0OFc98nIeqATBLqyS78VFXgRuavnpqxIRvSxuK7cc
oD9nQZywoXx7YRq6ykT0xd54JkCMKwyLSiW/bQJ3zJ4ml2VdsNs0W/siABcXedGK
q19QYSO2JKWkEKvxr7rjxkC6XCdeL6VC0Y9luxytX9m3Nv5xnM1rIzH6PM7f/V9P
pNgSjkCxQJD7WMG8Rz6o9wqnMnB2kSY/hPhhsrgOrqqPC2mzrNWXitCwGQMelrvl
cPT5AWJ+HIn3x+x4aScS4O2XhHW7dLLESLSOUv89AQKBgQDoPWemcE9y8PPlDeys
MEOuSu90K+hwLfSvc18atAc+zctble6qYHbhoW6ACjjLZTB+Hf9sGXXdTC1WjiIO
EHbosCnCgjmPfgLAkszKe4tLhmYbZTwrfE9vWl4WXWCV1HLt80yKgGjWttFjnXJF
jbTe62cyuJ/mwer6rh8YCwM/NwKBgQDK4lea12cD0WTBBu1MV8s/MhzVkCXD9dPU
vURQzj8vUR673EcUJWpX5yEt0ZeT8/S/9ZF6NPRBnC0QW/MsJpDwtFJ5++ewVfVQ
8wEE4isyvRXLbpeGOZ/Z0dBk4mNAjc0R+qHReM8yhs7/yOLWLjXSW274q1NQYupk
lcT72fG3AQKBgQC1yRLwCit2WjtfCRY/9guUS13B/niUDrTf/RvtiAu/0lCi4OqP
fLCxjq4zFU09kHhzz8FWeVt0HKPEg78OaT7ahsI5Wbv6oPVAjeg1ep0fQhV8zjJa
C5UWIZNSSEdJIKHRtkcshrUJlNKz+dMvtGtmrrb50eCAPTxUeqUmKcCh4wKBgEKH
tLinGDXtTX/q+JgHVjQUB9aUnX3EOEHUCvoAmEG49T4ffwOBPX0z4vJ2f6FZ55Gn
QpxzjwGQ6EosDPMWdoMobr9nttNhbL+t4FCspgPOc74xNukiLmQsZI0gm/GITo4t
xTC+0Bs+j9TbGF+p6aZgq2RKMljzBvATGPSJxLUBAoGAWYQSDXLyVb4wUEL9HpPK
XXJA/tbstpY8eBoD6aU2y6ik/A4TWJoXqjgQtck9LdVpyzJcbxBkBqhqTXfe61QG
Mg46R6f8hCduakxJhcsNcH7WEcQz7AVDf+TvLMDW6AbslTWIEaQBaQY28PDjJhsl
9RKE3SBmQY5DaMe13LC9mu8=
-----END PRIVATE KEY-----
```



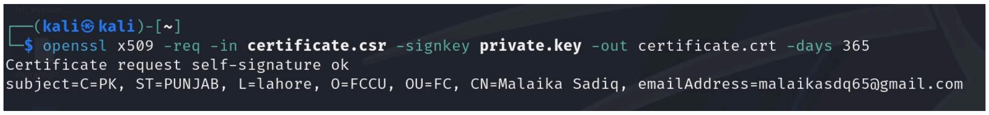
```
┌──(kali㉿kali)-[~]
└─$ cat public_key.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuA3JeCwgx1hTDqnLtDOA
3bTfzKB1MadlWFBifW6IIqEoVrDYnGxN0RQCAKjdd2Z8zyDkxt6piwKJY6Qr9UKy
xb0YYdPfaUFP0suorCtfYV6YPz3fMOFpT0fPaQpXzVaLoUec98skBBDJRoIN/3BJ
vq22d2Igbgt5HtlBe9wk+VeuC7ZkKJxKVQ/uEN9jOELOJ6Jz9ouw5NmDLGbxdd/E
yo5oKubytF/iLibYmBC73OFgDoiiTS81Lgh31kugoMpjt+sLylz9N33hkhFF97AX
G/BAGkbsfVzfObu0+vFLSXP/Iesqz+7nmJnIySydW5+/kJnk4sxmukCpeISIfvqQ
NwIDAQAB
-----END PUBLIC KEY-----
```



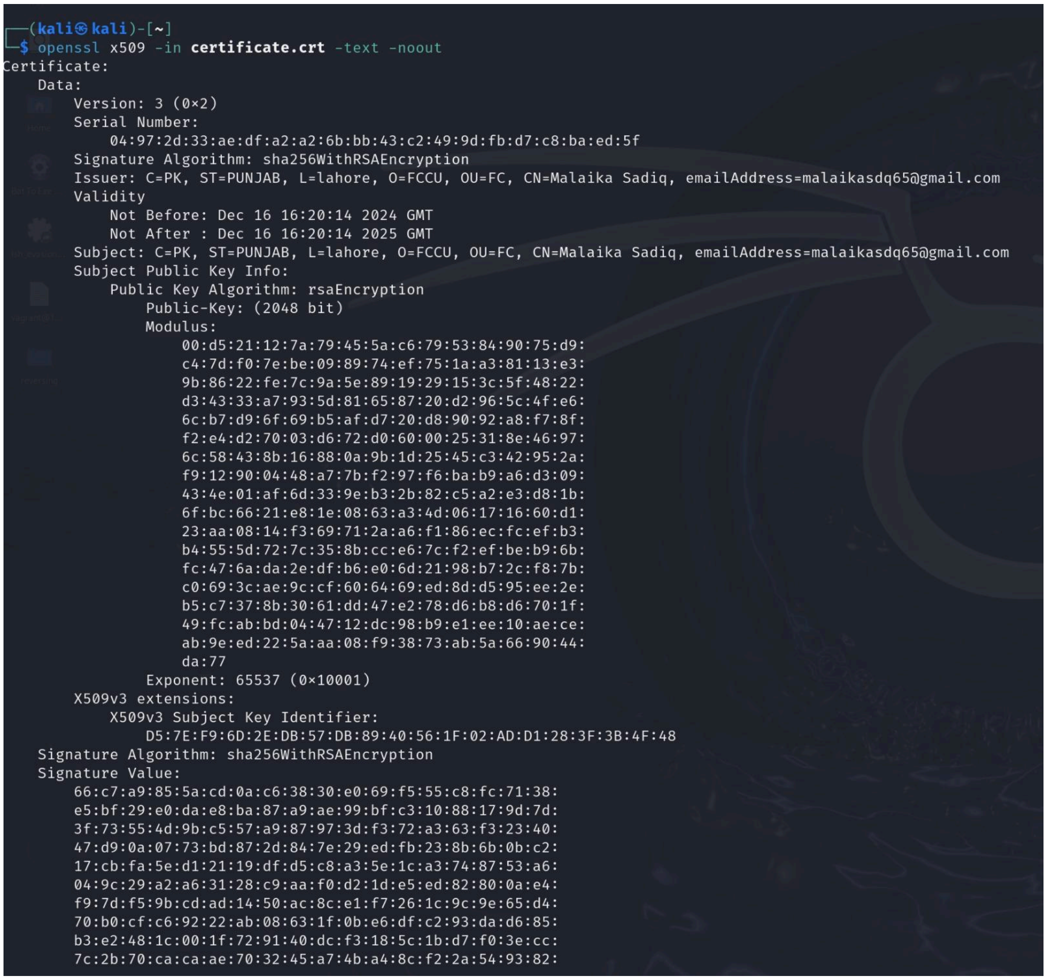
```
┌──(kali㉿kali)-[~]
└─$ openssl req -new -key private.key -out certificate.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can 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]:PK
State or Province Name (full name) [Some-State]:PUNJAB
Locality Name (eg, city) []:lahore
Organization Name (eg, company) [Internet Widgits Pty Ltd]:FCCU
Organizational Unit Name (eg, section) []:FC
Common Name (e.g. server FQDN or YOUR name) []:Malaika Sadiq
Email Address []:malaikasdq65@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:CS
```



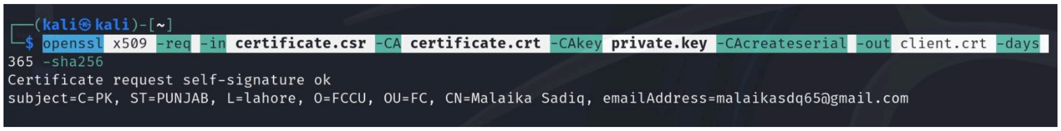
```
┌──(kali㉿kali)-[~]
└─$ openssl req -in certificate.csr -text -noout
Certificate Request:
    Data:
        Version: 1 (0×0)
        Subject: C=PK, ST=PUNJAB, L=lahore, O=FCCU, OU=FC, CN=Malaika Sadiq, emailAddress=malaikasdq
65@gmail.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d5:21:12:7a:79:45:5a:c6:79:53:84:90:75:d9:
                    c4:7d:f0:7e:be:09:89:74:ef:75:1a:a3:81:13:e3:
                    9b:86:22:fe:7c:9a:5e:89:19:29:15:3c:5f:48:22:
                    d3:43:33:a7:93:5d:81:65:87:20:d2:96:5c:4f:e6:
                    6c:b7:d9:6f:69:b5:af:d7:20:d8:90:92:a8:f7:8f:
                    f2:e4:d2:70:03:d6:72:d0:60:00:25:31:8e:46:97:
                    6c:58:43:8b:16:88:0a:9b:1d:25:45:c3:42:95:2a:
                    f9:12:90:04:48:a7:7b:f2:97:f6:ba:b9:a6:d3:09:
                    43:4e:01:af:6d:33:9e:b3:2b:82:c5:a2:e3:d8:1b:
                    6f:bc:66:21:e8:1e:08:63:a3:4d:06:17:16:60:d1:
                    23:aa:08:14:f3:69:71:2a:a6:f1:86:ec:fc:ef:b3:
                    b4:55:5d:72:7c:35:8b:cc:e6:7c:f2:ef:be:b9:6b:
                    fc:47:6a:da:2e:df:b6:e0:6d:21:98:b7:2c:f8:7b:
                    c0:69:3c:ae:9c:cf:60:64:69:ed:8d:d5:95:ee:2e:
                    b5:c7:37:8b:30:61:dd:47:e2:78:d6:b8:d6:70:1f:
                    49:fc:ab:bd:04:47:12:dc:98:b9:e1:ee:10:ae:ce:
                    ab:9e:ed:22:5a:aa:08:f9:38:73:ab:5a:66:90:44:
                    da:77
                Exponent: 65537 (0×10001)
        Attributes:
            unstructuredName         :CS
            challengePassword        :123456
            Requested Extensions:
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        c3:d0:ec:14:33:40:46:a9:48:eb:c5:6e:50:50:9b:29:6e:4f:
        8e:10:2c:3b:d7:1c:ba:65:ea:2e:99:83:cd:e0:f4:8c:d4:d7:
        ca:1f:86:df:52:fd:ef:a0:6f:3f:0c:ed:a6:57:1f:23:30:1e:
        d5:9b:c3:f3:68:54:45:af:c9:7b:e5:30:01:4e:56:48:70:ac:
        01:76:75:db:43:86:61:bd:23:4a:37:de:c2:eb:b3:cd:9e:7a:
        24:51:a9:ec:77:15:3c:20:42:7d:0c:47:18:38:5d:90:29:e5:
        8e:9f:00:c7:e6:2e:27:d1:43:97:ac:2f:8c:4e:93:64:59:de:
        ae:28:77:ed:92:a1:19:c5:e8:5e:6e:f3:12:c8:77:33:9c:77:
        e6:d0:4e:84:ee:eb:2c:c6:6f:f3:e0:a0:a5:8d:a4:4d:d7:ce:
        36:c8:c7:45:5c:72:79:04:90:03:59:a8:92:de:3c:aa:61:f2:
        1c:14:e5:06:41:e3:8d:cc:e0:b6:d8:71:dc:68:26:6a:e4:aa:
        43:62:cb:5b:0e:42:4a:da:b2:df:3a:79:6e:ed:15:39:14:2b:
        fb:48:cd:b7:e7:d4:36:a7:ce:86:0e:05:05:c1:7a:e8:cb:37:
        ed:0c:56:39:9f:56:80:96:f2:bc:7b:e8:20:b8:69:37:65:5a:
        19:f2:37:af
```



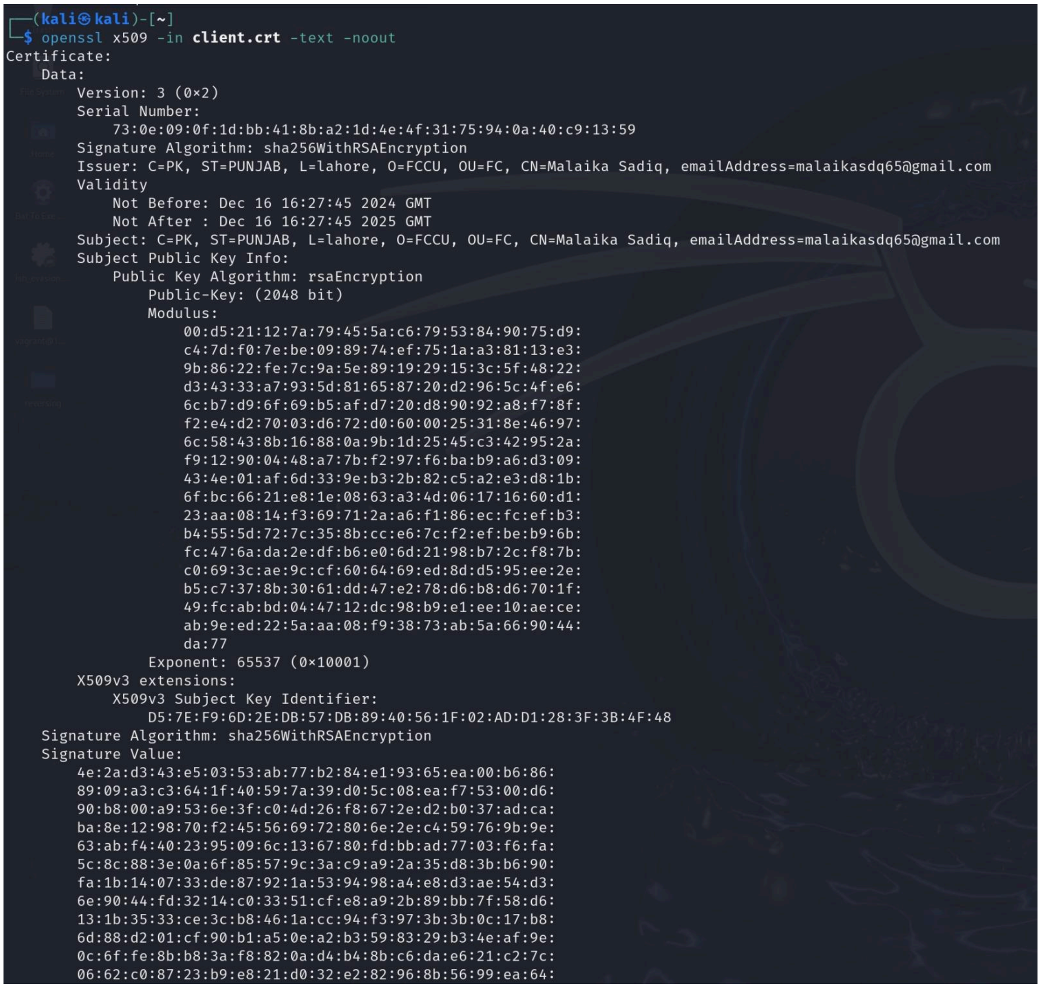
```
┌──(kali㉿kali)-[~]
└─$ openssl x509 -req -in certificate.csr -signkey private.key -out certificate.crt -days 365
Certificate request self-signature ok
subject=C=PK, ST=PUNJAB, L=lahore, O=FCCU, OU=FC, CN=Malaika Sadiq, emailAddress=malaikasdq65@gmail.com
```



```
┌──(kali㉿kali)-[~]
└─$ openssl x509 -in certificate.crt -text -noout
Certificate:
    Data:
        Version: 3 (0×2)
        Serial Number:
            04:97:2d:33:ae:df:a2:a2:6b:bb:43:c2:49:9d:fb:d7:c8:ba:ed:5f
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=PK, ST=PUNJAB, L=lahore, O=FCCU, OU=FC, CN=Malaika Sadiq, emailAddress=malaikasdq65@gmail.com
        Validity
            Not Before: Dec 16 16:20:14 2024 GMT
            Not After : Dec 16 16:20:14 2025 GMT
        Subject: C=PK, ST=PUNJAB, L=lahore, O=FCCU, OU=FC, CN=Malaika Sadiq, emailAddress=malaikasdq65@gmail.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d5:21:12:7a:79:45:5a:c6:79:53:84:90:75:d9:
                    c4:7d:f0:7e:be:09:89:74:ef:75:1a:a3:81:13:e3:
                    9b:86:22:fe:7c:9a:5e:89:19:29:15:3c:5f:48:22:
                    d3:43:33:a7:93:5d:81:65:87:20:d2:96:5c:4f:e6:
                    6c:b7:d9:6f:69:b5:af:d7:20:d8:90:92:a8:f7:8f:
                    f2:e4:d2:70:03:d6:72:d0:60:00:25:31:8e:46:97:
                    6c:58:43:8b:16:88:0a:9b:1d:25:45:c3:42:95:2a:
                    f9:12:90:04:48:a7:7b:f2:97:f6:ba:b9:a6:d3:09:
                    43:4e:01:af:6d:33:9e:b3:2b:82:c5:a2:e3:d8:1b:
                    6f:bc:66:21:e8:1e:08:63:a3:4d:06:17:16:60:d1:
                    23:aa:08:14:f3:69:71:2a:a6:f1:86:ec:fc:ef:b3:
                    b4:55:5d:72:7c:35:8b:cc:e6:7c:f2:ef:be:b9:6b:
                    fc:47:6a:da:2e:df:b6:e0:6d:21:98:b7:2c:f8:7b:
                    c0:69:3c:ae:9c:cf:60:64:69:ed:8d:d5:95:ee:2e:
                    b5:c7:37:8b:30:61:dd:47:e2:78:d6:b8:d6:70:1f:
                    49:fc:ab:bd:04:47:12:dc:98:b9:e1:ee:10:ae:ce:
                    ab:9e:ed:22:5a:aa:08:f9:38:73:ab:5a:66:90:44:
                    da:77
                Exponent: 65537 (0×10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                D5:7E:F9:6D:2E:DB:57:DB:89:40:56:1F:02:AD:D1:28:3F:3B:4F:48
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        66:c7:a9:85:5a:cd:0a:c6:38:30:e0:69:f5:55:c8:fc:71:38:
        e5:bf:29:e0:da:e8:ba:87:a9:ae:99:bf:c3:10:88:17:9d:7d:
        3f:73:55:4d:9b:c5:57:a9:87:97:3d:f3:72:a3:63:f3:23:40:
        47:d9:0a:07:73:bd:87:2d:84:7e:29:ed:fb:23:8b:6b:0b:c2:
        17:cb:fa:5e:d1:21:19:df:d5:c8:a3:5e:1c:a3:74:87:53:a6:
        04:9c:29:a2:a6:31:28:c9:aa:f0:d2:1d:e5:ed:82:80:0a:e4:
        f9:7d:f5:9b:cd:ad:14:50:ac:8c:e1:f7:26:1c:9c:9e:65:d4:
        70:b0:cf:c6:92:22:ab:08:63:1f:0b:e6:df:c2:93:da:d6:85:
        b3:e2:48:1c:00:1f:72:91:40:dc:f3:18:5c:1b:d7:f0:3e:cc:
        7c:2b:70:ca:ca:ae:70:32:45:a7:4b:a4:8c:f2:2a:54:93:82:
```



```
┌──(kali㉿kali)-[~]
└─$ openssl x509 -req -in certificate.csr -CA certificate.crt -CAkey private.key -CAcreateserial -out client.crt -days
365 -sha256
Certificate request self-signature ok
subject=C=PK, ST=PUNJAB, L=lahore, O=FCCU, OU=FC, CN=Malaika Sadiq, emailAddress=malaikasdq65@gmail.com
```



```
┌──(kali㉿kali)-[~]
└─$ openssl x509 -in client.crt -text -noout
Certificate:
    Data:
        Version: 3 (0×2)
        Serial Number:
            73:0e:09:0f:1d:bb:41:8b:a2:1d:4e:4f:31:75:94:0a:40:c9:13:59
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=PK, ST=PUNJAB, L=lahore, O=FCCU, OU=FC, CN=Malaika Sadiq, emailAddress=malaikasdq65@gmail.com
        Validity
            Not Before: Dec 16 16:27:45 2024 GMT
            Not After : Dec 16 16:27:45 2025 GMT
        Subject: C=PK, ST=PUNJAB, L=lahore, O=FCCU, OU=FC, CN=Malaika Sadiq, emailAddress=malaikasdq65@gmail.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d5:21:12:7a:79:45:5a:c6:79:53:84:90:75:d9:
                    c4:7d:f0:7e:be:09:89:74:ef:75:1a:a3:81:13:e3:
                    9b:86:22:fe:7c:9a:5e:89:19:29:15:3c:5f:48:22:
                    d3:43:33:a7:93:5d:81:65:87:20:d2:96:5c:4f:e6:
                    6c:b7:d9:6f:69:b5:af:d7:20:d8:90:92:a8:f7:8f:
                    f2:e4:d2:70:03:d6:72:d0:60:00:25:31:8e:46:97:
                    6c:58:43:8b:16:88:0a:9b:1d:25:45:c3:42:95:2a:
                    f9:12:90:04:48:a7:7b:f2:97:f6:ba:b9:a6:d3:09:
                    43:4e:01:af:6d:33:9e:b3:2b:82:c5:a2:e3:d8:1b:
                    6f:bc:66:21:e8:1e:08:63:a3:4d:06:17:16:60:d1:
                    23:aa:08:14:f3:69:71:2a:a6:f1:86:ec:fc:ef:b3:
                    b4:55:5d:72:7c:35:8b:cc:e6:7c:f2:ef:be:b9:6b:
                    fc:47:6a:da:2e:df:b6:e0:6d:21:98:b7:2c:f8:7b:
                    c0:69:3c:ae:9c:cf:60:64:69:ed:8d:d5:95:ee:2e:
                    b5:c7:37:8b:30:61:dd:47:e2:78:d6:b8:d6:70:1f:
                    49:fc:ab:bd:04:47:12:dc:98:b9:e1:ee:10:ae:ce:
                    ab:9e:ed:22:5a:aa:08:f9:38:73:ab:5a:66:90:44:
                    da:77
                Exponent: 65537 (0×10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                D5:7E:F9:6D:2E:DB:57:DB:89:40:56:1F:02:AD:D1:28:3F:3B:4F:48
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        4e:2a:d3:43:e5:03:53:ab:77:b2:84:e1:93:65:ea:00:b6:86:
        89:09:a3:c3:64:1f:40:59:7a:39:d0:5c:08:ea:f7:53:00:d6:
        90:b8:00:a9:53:6e:3f:c0:4d:26:f8:67:2e:d2:b0:37:ad:ca:
        ba:8e:12:98:70:f2:45:56:69:72:80:6e:2e:c4:59:76:9b:9e:
        63:ab:f4:40:23:95:09:6c:13:67:80:fd:bb:ad:77:03:f6:fa:
        5c:8c:88:3e:0a:6f:85:57:9c:3a:c9:a9:2a:35:d8:3b:b6:90:
        fa:1b:14:07:33:de:87:92:1a:53:94:98:a4:e8:d3:ae:54:d3:
        6e:90:44:fd:32:14:c0:33:51:cf:e8:a9:2b:89:bb:7f:58:d6:
        13:1b:35:33:ce:3c:b8:46:1a:cc:94:f3:97:3b:3b:0c:17:b8:
        6d:88:d2:01:cf:90:b1:a5:0e:a2:b3:59:83:29:b3:4e:af:9e:
        0c:6f:fe:8b:b8:3a:f8:82:0a:d4:b4:8b:c6:da:e6:21:c2:7c:
        06:62:c0:87:23:b9:e8:21:d0:32:e2:82:96:8b:56:99:ea:64:
```