Lab Assignment 9

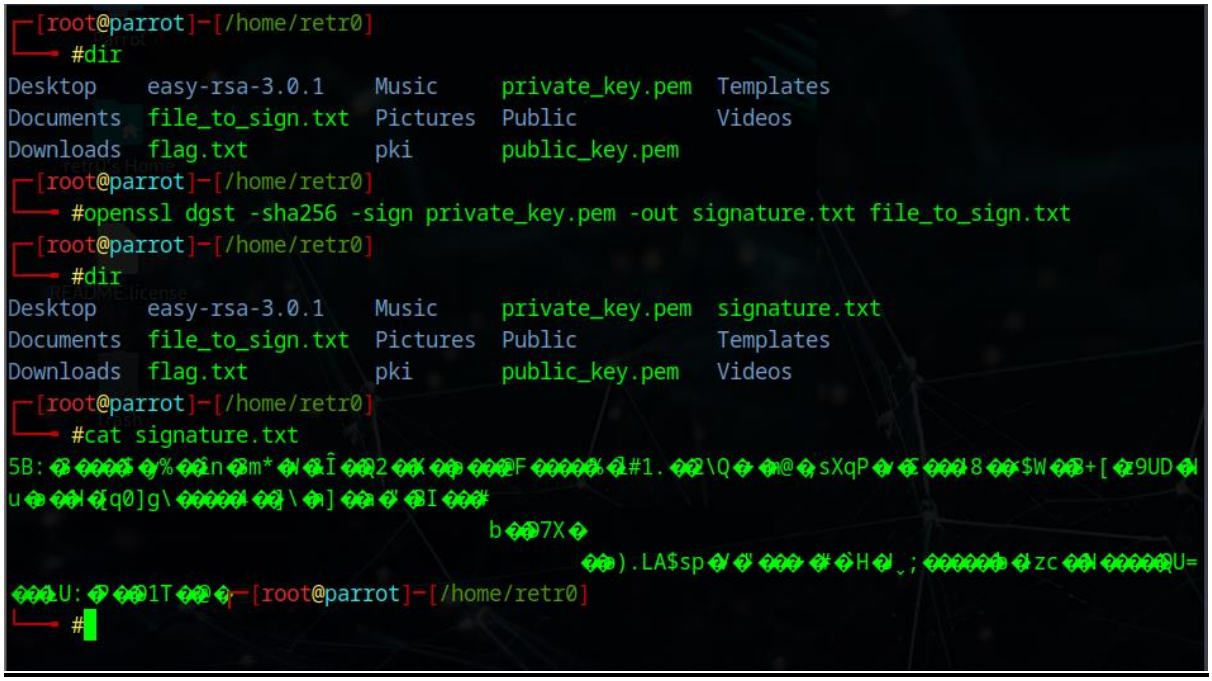
AP21110010302
Krish Srivastava
CSE – E
Network Security – CSE 315L

Please go through the lab manuals related to SSL/TLS and perform the following tasks using OpenSSL

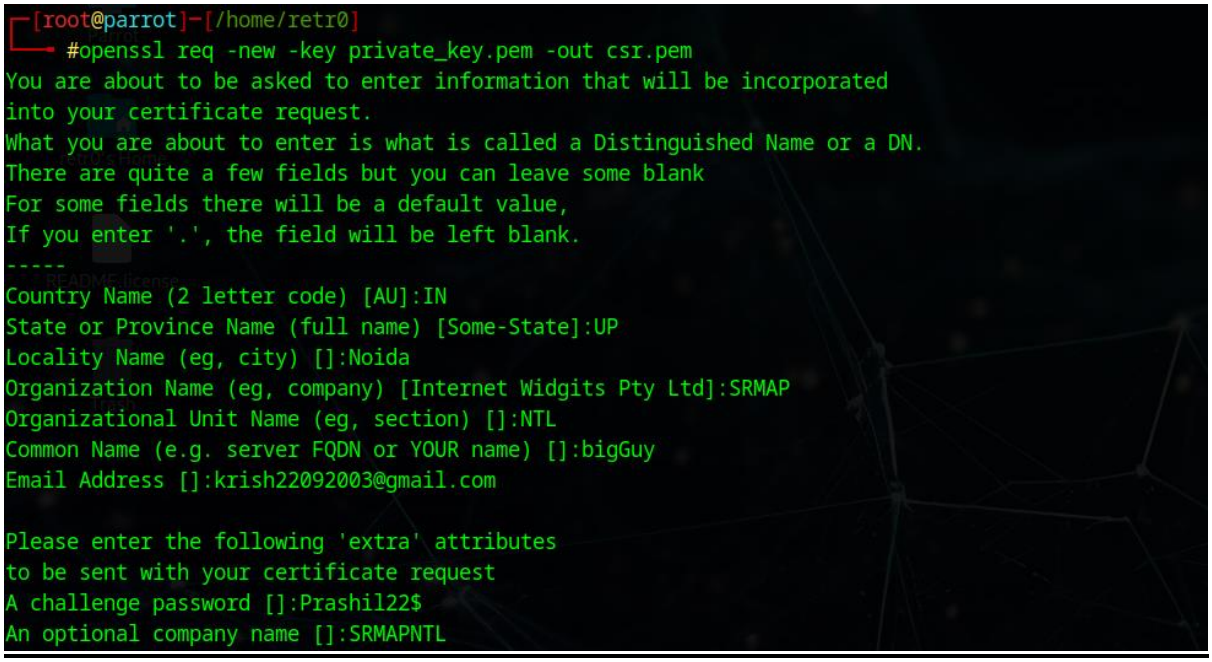
1) **Public and/or private keys**

```
┌─[root@parrot]─[/home/retr0]
└──╼ #openssl genrsa -out private_key.pem 2048
┌─[root@parrot]─[/home/retr0]
└──╼ #openssl rsa -in private_key.pem -pubout -out public_key.pem
writing RSA key
┌─[root@parrot]─[/home/retr0]
└──╼ #dir
Desktop    Downloads       flag.txt  Pictures  private_key.pem  public_key.pem  Videos
Documents  easy-rsa-3.0.1  Music     pki       Public           Templates
┌─[root@parrot]─[/home/retr0]
└──╼ #cat public_key.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwMUttiCTdCYwFeqQ3Wpi
WAdRRNCkdDNHCf7WZzeze9AfZjOtqrOxuO0wkSP1WWslQV53wzu+r6tSQMNLW3FY
G1PIjxPFHFj222/2x5xbgGpM7ZfBQbnXUObCRwHFlJERLJfiKYnedscnduGiPbXK
Kvcfbsm0T/tYt01QwcPpEiZVhn/2jC5DgDPtXG1R3AhsCkwGmr8Mi73byQiqncLp
itsJjgWg3HIERyy8YQ5kwrSv8iv3lDDMy01wNn1x2sSFPLZ+aKULC/Tjj1NZa8JB
uFCxsM4bqdKhczU/K6cZKIGUyOvrNQM2h6FRz5vzwJvYrW36PKmzDwMqLpVCNtVt
SQIDAQAB
-----END PUBLIC KEY-----
┌─[root@parrot]─[/home/retr0]
└──╼ #
```

2) Creating Digital Signatures



3) Certificate Signing Requests



```
┌[root@parrot]-[/home/retr0]
└─ #dir
csr.pem     Downloads         flag.txt  pki              public_key.pem  Videos
Desktop     easy-rsa-3.0.1    Music     private_key.pem  signature.txt
Documents   file_to_sign.txt  Pictures  Public           Templates
┌[root@parrot]-[/home/retr0]
└─ #cat csr.pem
-----BEGIN CERTIFICATE REQUEST-----
MIIC+zCCAeMCAQAwgYExCzAJBgNVBAYTAklOMQswCQYDVQQIDAJVUDEOMAwGA1UE
BwwFTm9pZGExDjAMBgNVBAoMBVNSTUFQMQwwCgYDVQQLDANOVEwxDzANBgNVBAMM
BmJpZ0d1eTEmMCQGCSqGSIb3DQEJARYXa3Jpc2gyMjA5MjAwM0BnbWFpbC5jb20w
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDAxS22IJN0JjAV6pDdamJY
B1FE0KR0M0cJ/tZnN7N70B9mM62qs7G47TCRI/VZayVBXnfDO76vq1JAw0tbcVgb
U8iPE8UcWPbbb/bHnFuAakztl8FBuddQ5sJHAcWUkREsl+Ipid52xyd24aI9tcoq
9x9uybRP+1i3TVDBw+kSJlWGf/aMLkOAM+1cbVHcCGwKTAaavwyLvdvJCKqdwumK
2wmOBaDccgRHLLxhDmTCtK/yK/eUMMzLTXA2fXHaxIU8tn5opQsL9OOPU1lrwkG4
ULGwzhup0qFzNT8rpxkogZTI6+s1AzaHoVHPm/PAm9itbfo8qbMPAyoulUI21W1J
AgMBAAGgNDAXBgkqhkiG9w0BCQIxCgwIU1JNQVBOVEwwGQYJKoZIhvcNAQkHMQwM
ClByYXNoaWwyMiQwDQYJKoZIhvcNAQELBQADggEBALavlK2EcxO2QRZag7IN5ww9
19d5nYq++0emkUJAySVYbOV2LWpFD7XEj9xZcLCd6v0d9MI6cSwTAGBZei7xzWHD
sZadPt9Pzmt3U7559oUF8yG6gSGTwc0AxuCyt5vLLu59kKrJfw4fEBpzJAOLe1pG
G2mLse06h0t76ni3TOMl3XG44S6a2ECEZl932O49C5vFbMn0CKDqtOmulfxLJsnx
ePXpCu84cXeAAk06YcBmOU1ZcH8Evsu4F2+Tk9KM6ZI+XHHEGzk/2Azd3MhssSAd
r5SmOCrGyWovlzZQ2YZtqkA0KyE9ZafJTxUUcbgEWglkOqe1RsAp2jYwUV0B/Kw=
-----END CERTIFICATE REQUEST-----
┌[root@parrot]-[/home/retr0]
└─ #
```

4) Generating SSL Certificates

```
┌[root@parrot]-[/home/retr0]
└─ #openssl x509 -req -in csr.pem -signkey private_key.pem -out certificate.pem
Certificate request self-signature ok
subject=C = IN, ST = UP, L = Noida, O = SRMAP, OU = NTL, CN = bigGuy, emailAddress = krish22092003@gmail.com
┌[root@parrot]-[/home/retr0]
└─ #dir
certificate.pem  Documents       file_to_sign.txt  Pictures         Public          Templates
csr.pem          Downloads       flag.txt          pki              public_key.pem  Videos
Desktop          easy-rsa-3.0.1  Music             private_key.pem  signature.txt
┌[root@parrot]-[/home/retr0]
└─ #cat certificate.pem
-----BEGIN CERTIFICATE-----
MIIDizCCAnMCFAt3O+iLaJAETL85LClRi/WrLVXvMA0GCSqGSIb3DQEBCwUAMIGB
MQswCQYDVQQGEwJJTjELMAkGA1UECAwCVVAxDjAMBgNVBAcMBU5vaWRhMQ4wDAYD
VQQKDAVTUk1BUDEMMAoGA1UECwwDTlRMMQ8wDQYDVQQDDAZiaWdHdXkxJjAkBgkq
hkiG9w0BCQEWF2tyaXNoMjIwOTIwMDNAZ21haWwuY29tMB4XDTI0MDQxNjA0MzYw
NVoXDTI0MDUxNjA0MzYwNVowgYExCzAJBgNVBAYTAklOMQswCQYDVQQIDAJVUDEO
MAwGA1UEBwwFTm9pZGExDjAMBgNVBAoMBVNSTUFQMQwwCgYDVQQLDANOVEwxDzAN
BgNVBAMMBmJpZ0d1eTEmMCQGCSqGSIb3DQEJARYXa3Jpc2gyMjA5MjAwM0BnbWFp
bC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDAxS22IJN0JjAV
6pDdamJYB1FE0KR0M0cJ/tZnN7N70B9mM62qs7G47TCRI/VZayVBXnfDO76vq1JA
w0tbcVgbU8iPE8UcWPbbb/bHnFuAakztl8FBuddQ5sJHAcWUkREsl+Ipid52xyd2
4aI9tcoq9x9uybRP+1i3TVDBw+kSJlWGf/aMLkOAM+1cbVHcCGwKTAaavwyLvdvJ
CKqdwumK2wmOBaDccgRHLLxhDmTCtK/yK/eUMMzLTXA2fXHaxIU8tn5opQsL9OOP
U1lrwkG4ULGwzhup0qFzNT8rpxkogZTI6+s1AzaHoVHPm/PAm9itbfo8qbMPAyou
lUI21W1JAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAFa6uXjtDPs8KxS4kZ23Q5+s
yMh4cSAUPqeGz0/Kr3jtpxsJ1CBBkjdNFsDKb+S3xqLUEhQB9SEIF6sGgEvhaCiC
uBCDCsMeevR24UimePbs1iLuo19vtuKi5329KYG9vnrxdhpS7WRTUtxDHg5BvxFx
FjKDzNKEbKp0/eoHyGhTf8JNBwtwrmwcnNHBWnFpQJPK1i70iIk29mQvir9H04Hc
W3dv/urI91ZLZQu7we2KKZPUQxJMvx2rsyWj7AFrjaf9lPnIqyhZD5rPUzYa1IWX
DMXRosDJSp3rInPMlnR0M5n36LkzptVhgIIBscpu7/TybY3fcg8z91DYgEnrnwY=
-----END CERTIFICATE-----
```

5) Viewing Certificates

```
┌──[root@parrot]─[/home/retr0]
└─── #openssl x509 -in certificate.pem -text -noout
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            0b:77:3b:e8:8b:68:90:04:4c:bf:39:2c:29:51:8b:f5:ab:2d:55:ef
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = IN, ST = UP, L = Noida, O = SRMAP, OU = NTL, CN = bigGuy, emailAddress = krish22092003@gmail.com
        Validity
            Not Before: Apr 16 04:36:05 2024 GMT
            Not After : May 16 04:36:05 2024 GMT
        Subject: C = IN, ST = UP, L = Noida, O = SRMAP, OU = NTL, CN = bigGuy, emailAddress = krish22092003@gmail.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c0:c5:2d:b6:20:93:74:26:30:15:ea:90:dd:6a:
                    62:58:07:51:44:d0:a4:74:33:47:09:fe:d6:67:37:
                    b3:7b:d0:1f:66:33:ad:aa:b3:b1:b8:ed:30:91:23:
                    f5:59:6b:25:41:5e:77:c3:3b:be:af:ab:52:40:c3:
                    4b:5b:71:58:1b:53:c8:8f:13:c5:1c:58:f6:db:6f:
                    f6:c7:9c:5b:80:6a:4c:ed:97:c1:41:b9:d7:50:e6:
                    c2:47:01:c5:94:91:11:2c:97:e2:29:89:de:76:c7:
                    27:76:e1:a2:3d:b5:ca:2a:f7:1f:6e:c9:b4:4f:fb:
                    58:b7:4d:50:c1:c3:e9:12:26:55:86:7f:f6:8c:2e:
                    43:80:33:ed:5c:6d:51:dc:08:6c:0a:4c:06:9a:bf:
                    0c:8b:bd:db:c9:08:aa:9d:c2:e9:8a:db:09:8e:05:
                    a0:dc:72:04:47:2c:bc:61:0e:64:c2:b4:af:f2:2b:
                    f7:94:30:cc:cb:4d:70:36:7d:71:da:c4:85:3c:b6:
                    7e:68:a5:0b:0b:f4:e3:8f:53:59:6b:c2:41:b8:50:
                    b1:b0:ce:1b:a9:d2:a1:73:35:3f:2b:a7:19:28:81:
                    94:c8:eb:eb:35:03:36:87:a1:51:cf:9b:f3:c0:9b:
```

```
                    f6:c7:9c:5b:80:6a:4c:ed:97:c1:41:b9:d7:50:e6:
                    c2:47:01:c5:94:91:11:2c:97:e2:29:89:de:76:c7:
                    27:76:e1:a2:3d:b5:ca:2a:f7:1f:6e:c9:b4:4f:fb:
                    58:b7:4d:50:c1:c3:e9:12:26:55:86:7f:f6:8c:2e:
                    43:80:33:ed:5c:6d:51:dc:08:6c:0a:4c:06:9a:bf:
                    0c:8b:bd:db:c9:08:aa:9d:c2:e9:8a:db:09:8e:05:
                    a0:dc:72:04:47:2c:bc:61:0e:64:c2:b4:af:f2:2b:
                    f7:94:30:cc:cb:4d:70:36:7d:71:da:c4:85:3c:b6:
                    7e:68:a5:0b:0b:f4:e3:8f:53:59:6b:c2:41:b8:50:
                    b1:b0:ce:1b:a9:d2:a1:73:35:3f:2b:a7:19:28:81:
                    94:c8:eb:eb:35:03:36:87:a1:51:cf:9b:f3:c0:9b:
                    d8:ad:6d:fa:3c:a9:b3:0f:03:2a:2e:95:42:36:d5:
                    6d:49
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        56:ba:b9:78:ed:0c:fb:3c:2b:14:b8:91:9d:b7:43:9f:ac:c8:
        c8:78:71:20:14:3e:a7:86:cf:4f:ca:af:78:ed:a7:1b:09:d4:
        20:41:92:37:4d:16:c0:ca:6f:e4:b7:c6:a2:d4:12:14:01:f5:
        21:08:17:ab:06:80:4b:e1:68:28:82:b8:10:83:0a:c3:1e:7a:
        f4:76:e1:48:a6:78:f6:ec:d6:22:ee:a3:5f:6f:b6:e2:a2:e7:
        7d:bd:29:81:bd:be:7a:f1:76:1a:52:ed:64:53:52:dc:43:1e:
        0e:41:bf:11:71:16:32:83:cc:d2:84:6c:aa:74:fd:ea:07:c8:
        68:53:7f:c2:4d:07:0b:70:ae:6c:1c:9c:d1:c1:5a:71:69:40:
        93:ca:d6:2e:f4:88:89:36:f6:64:2f:8a:bf:47:d3:81:dc:5b:
        77:6f:fe:ea:c8:f7:56:4b:65:0b:bb:c1:ed:8a:29:93:d4:43:
        12:4c:bf:1d:ab:b3:25:a3:ec:01:6b:8d:a7:fd:94:f9:c8:ab:
        28:59:0f:9a:cf:53:36:1a:d4:85:97:0c:c5:d1:a2:c0:c9:4a:
        9d:eb:22:73:cc:96:74:74:33:99:f7:e8:b9:33:a6:d5:61:80:
        82:01:b1:ca:6e:ef:f4:f2:6d:8d:df:72:0f:33:f7:50:d8:80:
        49:eb:9f:06
```