Alec Howard

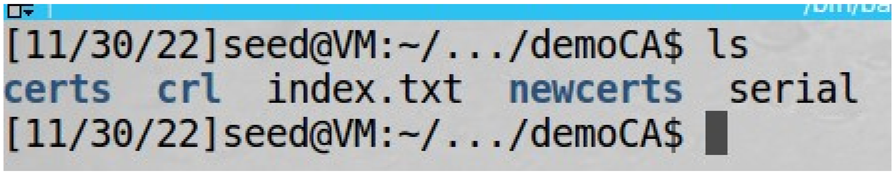
CYB-3363-FA/22

Dr. Pei

Lab 3: RSA, Public-Key Cryptography, & PKI

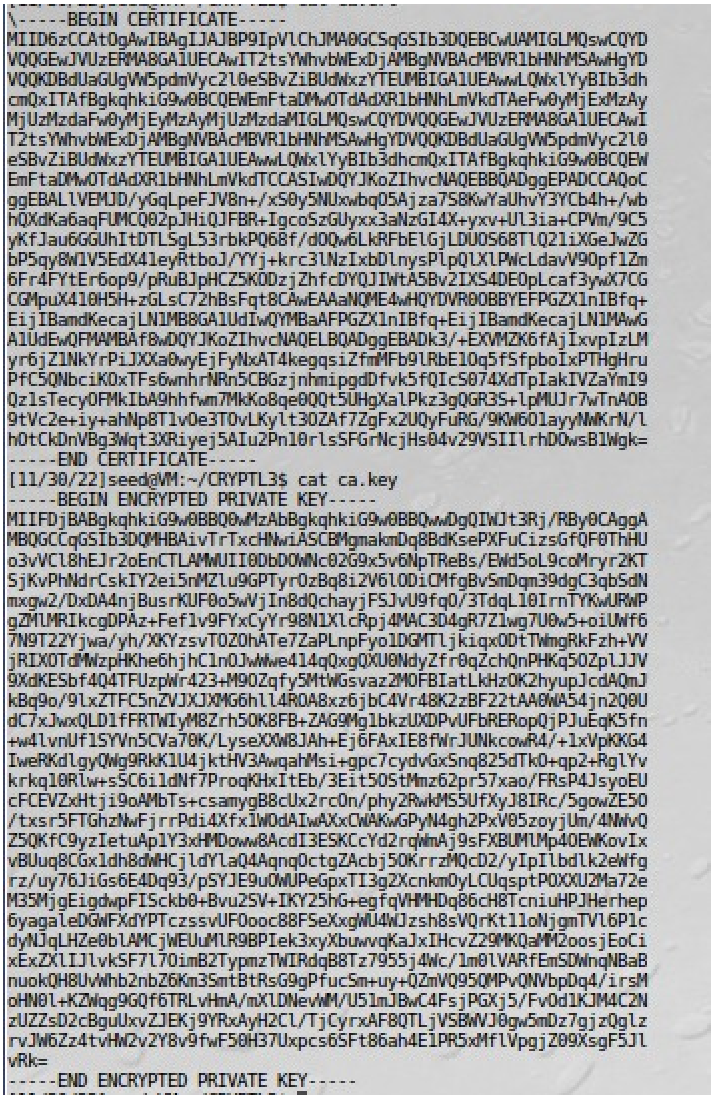
1. Become a CA

    a.



```
[11/30/22]seed@VM:~/.../demoCA$ ls
certs  crl  index.txt  newcerts  serial
[11/30/22]seed@VM:~/.../demoCA$ 
```

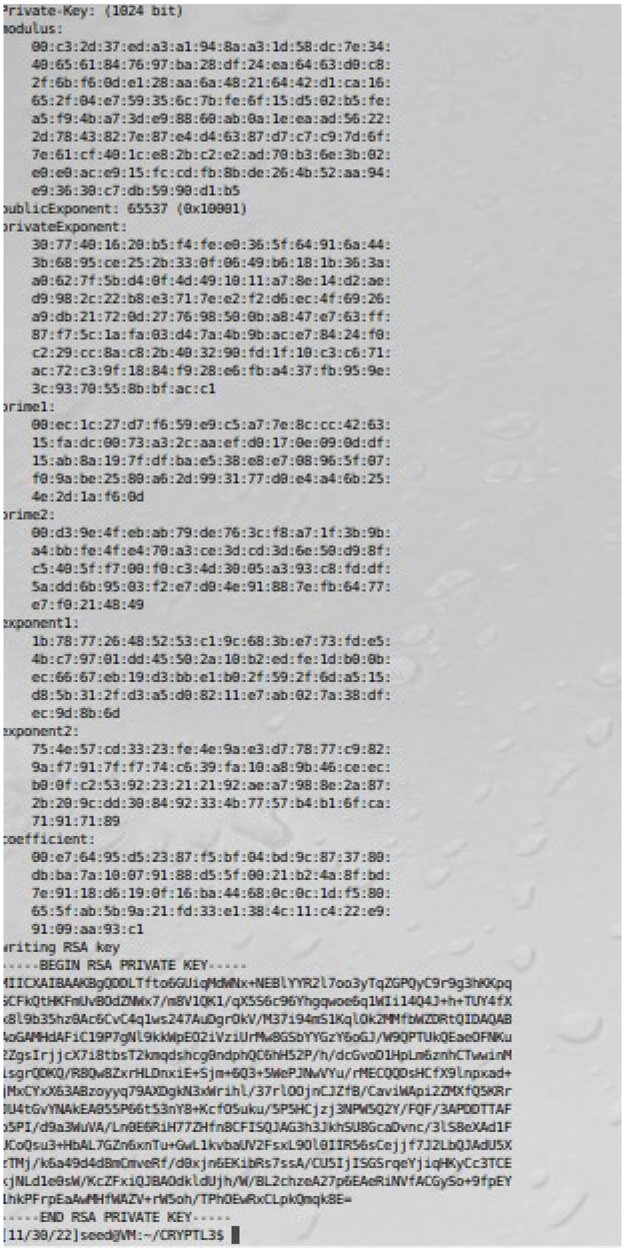
    b.



```
\-----BEGIN CERTIFICATE-----
MIID6zCCAtOgAwIBAgIJAJBP9IpVlChJMA0GCSqGSIb3DQEBCwUAMIGLMQswCQYD
VQQGEwJVUzERMABGA1UECAwIT2tsYWhvbWExDjAMBgNVBAcMBVR1bHNhMSAwHgYD
VQQKDBdUaGUgVW5pdmVyc2l0eSBvZiBUdWxzYTEUMBIGA1UEAwwLQWxlYyBIb3dh
cmQxITAfBgkqhkiG9w0BCQEWEmFtaDMwOTdAdXR1bHNhLmVkdTAeFw0yMjExMzAy
MjUzMzdaFw0yMjEyMzAyMjUzMzdaMIGLMQswCQYDVQQGEwJVUzERMABGA1UECAwI
T2tsYWhvbWExDjAMBgNVBAcMBVR1bHNhMSAwHgYDVQQKDBdUaGUgVW5pdmVyc2l0
eSBvZiBUdWxzYTEUMBIGA1UEAwwLQWxlYyBIb3dhcmQxITAfBgkqhkiG9w0BCQEW
EmFtaDMwOTdAdXR1bHNhLmVkdTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBALlVEMJD/yGqLpeFJV8n+/xS0y5NUxwbqO5Ajza7S8KwYaUhvY3YCb4h+/wb
hQXdKa6aqFUMCQ02pJHiQJFBR+IgcoSzGUyxx3aNzGI4X+yxv+Ul3ia+CPVm/9C5
yKfJau6GGUhItDTLSgL53rbkPQ68f/dOQw6LkRFbElGjLDUOS68TlQ21iXGeJwZG
bP5qy8WIV5EdX4leyRtboJ/YYj+krc3lNzIxbDlnysPlpQlXlPWcLdavV9Opf1Zm
6Fr4FYtEr6op9/pRuBJpHCZ5KODzjZhfcDYQJIWtA5Bv2IXS4DEOpLcaf3ywX7CG
CGMpuX410H5H+zGLsC72hBsFqt8CAwEAAaNQME4wHQYDVR0OBBYEFPGZX1nIBfq+
EijIBamdKecajLN1MB8GA1UdIwQYMBaAFPGZX1nIBfq+EijIBamdKecajLN1MAwG
A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBADk3/+EXVMZK6fAjIxvpIzLM
yr6jZ1NkYrPiJXXa0wyEjFyNxAT4keggsiZfmMFb9lRbE1Oq5fSfpboIxPTHgHru
PfC5QNbciKOxTFs6wnhrNRn5CBGzjnhmipgdDfvk5fQIcS074XdTpIakIVZaYmI9
QzlsTecyOFMkIbA9hhfwm7MkKo8qe0QQt5UHgXalPkz3gQGR3S+lpMUJr7wTnAOB
9tVc2e+iy+ahNp8TlvOe3TOvLKylt3OZAf7ZgFx2UQyFuRG/9KW6OlayyNWKrN/l
hOtCkDnVBg3Wqt3XRiyej5AIu2Pn10rlsSFGrNcjHs04v29VSIIlrhDOwsBlWgk=
-----END CERTIFICATE-----
[11/30/22]seed@VM:~/CRYPTL3$ cat ca.key
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIWJt3Rj/RBy0CAggA
MBQGCCqGSIb3DQMHBAivTrTxcHNwiASCBMgmakmDq8BdKsePXFuCizsGfQF0ThHU
o3vVCl8hEJr2oEnCTLAMWUII0DbDOWNc02G9x5v6NpTReBs/EWd5oL9coMryr2KT
SjKvPhNdrCskIY2ei5nMZlu9GPTyrOzBq8i2V6lODiCMfgBvSmDqm39dgC3qbSdN
mxgw2/DxDA4njBusrKUF0o5wVjIn8dQchayjFSJvU9fqO/3TdqL10IrnTYKwURWP
gZMlMRIkcgDPAz+Feflv9FYxCyYr98N1XlcRpj4MAC3D4gR7Zlwg7U0w5+oiUWf6
7N9T22Yjwa/yh/XKYzsvTOZOhATe7ZaPLnpFyolDGMTljkiqxODtTWmgRkFzh+VV
jRIXOTdMWzpHKhe6hjhClnOJwWwe4l4qQxgQXU0NdyZfr0qZchQnPHKq5OZplJJV
9XdKESbf4Q4TFUzpWr423+M9OZqfy5MtWGsvaz2MOFBIatLkHzOK2hyupJcdAQmJ
kBq9o/9lxZTFC5nZVJXJXMG6hll4ROA8xz6jbC4Vr48K2zBF22tAA0WA54jn2Q0U
dC7xJwxQLD1fFRTWIyM8Zrh5OK8FB+ZAG9Mg1bkzUXDPvUFbRERopQjPJuEqK5fn
+w4lvnUf1SYVn5CVa70K/LyseXXW8JAh+Ej6FAxIE8fWrJUNkcowR4/+1xVpKKG4
IweRKdlgyQWg9RkK1U4jktHV3AwqahMsi+gpc7cydvGxSnq825dTkO+qp2+RglYv
krkq10Rlw+sSC6ildNf7ProqKHxItEb/3Eit5OStMmz62pr57xao/FRsP4JsyoEU
cFCEVZxHtji9oAMbTs+csamygB8cUx2rcOn/phy2RwkMS5UfXyJ8IRc/5gowZE5O
/txsr5FTGhzNwFjrrPdi4Xfx1WOdAIwAXxCWAKwGPyN4gh2PxV05zoyjUm/4NWvQ
Z5QKfC9yzIetuAplY3xHMDoww8AcdI3ESKCcYd2rqWmAj9sFXBUMlMp4OEWKovIx
vBUuq8CGx1dh8dWHCjldYlaQ4AqnqOctgZAcbj5OKrrzMQcD2/yIpIlbdlk2eWfg
rz/uy76JiGs6E4Dq93/pSYJE9uOWUPeGpxTI3g2XcnkmOyLCUqsptPOXXU2Ma72e
M35MjgEigdwpFISckb0+Bvu2SV+IKY25hG+egfqVHMHDq86cH8TcniuHPJHerhep
6yagaleDGWFXdYPTczssvUFOooc88FSeXxgWU4WJzsh8sVQrKtlloNjgmTVl6P1c
dyNJqLHZe0blAMCjWEUuMlR9BPIek3xyXbuwvqKaJxIHcvZ29MKQaMM2oosjEoCi
xExZXlIJlvkSF7l7OimB2TypmzTWIRdqB8Tz7955j4Wc/1m0lVARfEmSDWnqNBaB
nuokQH8UvWhb2nbZ6Km3SmtBtRsG9gPfucSm+uy+QZmVQ95QMPvQNVbpDq4/irsM
oHN0l+KZWqg9GQf6TRLvHmA/mXlDNevWM/U51mJBwC4FsjPGXj5/FvOd1KJM4C2N
zUZZsD2cBguUxvZJEKj9YRxAyH2Cl/TjCyrxAF8QTLjVSBWVJ0gw5mDz7gjzQglz
rvJW6Zz4tvHW2v2Y8v9fwF50H37Uxpcs6SFt86ah4E1PR5xMflVpgjZ09XsgF5Jl
vRk=
-----END ENCRYPTED PRIVATE KEY-----
```

2. Creating a Certificate for SEEDPKILab2020.com

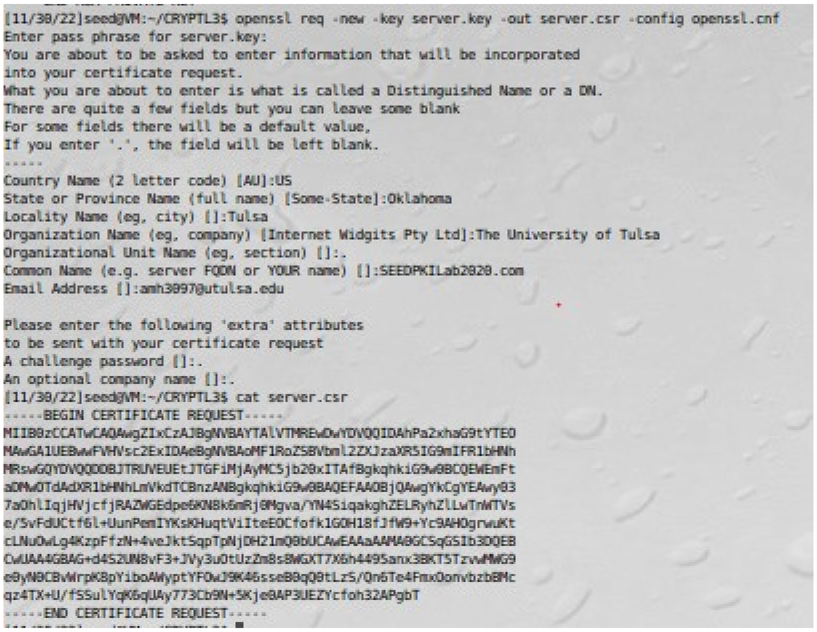
    a. Generate Public/Private Key Pair



i.

```
rivate-Key: (1024 bit)
odulus:
    00:c3:2d:37:ed:a3:a1:94:8a:a3:1d:58:dc:7e:34:
    40:65:61:84:76:97:ba:28:df:24:ea:64:63:d0:c8:
    2f:6b:f6:0d:e1:28:aa:6a:48:21:64:42:d1:ca:16:
    65:2f:04:e7:59:35:6c:7b:fe:6f:15:d5:02:b5:fe:
    a5:f9:4b:a7:3d:e9:88:60:ab:0a:1e:ea:ad:56:22:
    2d:78:43:82:7e:87:e4:d4:63:87:d7:c7:c9:7d:6f:
    7e:61:cf:40:1c:e8:2b:c2:e2:ad:70:b3:6e:3b:02:
    e0:e0:ac:e9:15:fc:cd:fb:8b:de:26:4b:52:aa:94:
    e9:36:30:c7:db:59:90:d1:b5
ublicExponent: 65537 (0x10001)
rivateExponent:
    30:77:40:16:20:b5:f4:fe:e0:36:5f:64:91:6a:44:
    3b:68:95:ce:25:2b:33:0f:06:49:b6:18:1b:36:3a:
    a0:62:7f:5b:d4:0f:4d:49:10:11:a7:8e:14:d2:ae:
    d9:98:2c:22:b8:e3:71:7e:e2:f2:d6:ec:4f:69:26:
    a9:db:21:72:0d:27:76:98:50:0b:a8:47:e7:63:ff:
    87:f7:5c:1a:fa:03:d4:7a:4b:9b:ac:e7:84:24:f0:
    c2:29:cc:8a:c8:2b:40:32:90:fd:1f:10:c3:c6:71:
    ac:72:c3:9f:18:84:f9:28:e6:fb:a4:37:fb:95:9e:
    3c:93:70:55:8b:bf:ac:c1
rime1:
    00:ec:1c:27:d7:f6:59:e9:c5:a7:7e:8c:cc:42:63:
    15:fa:dc:00:73:a3:2c:aa:ef:d0:17:0e:09:0d:df:
    15:ab:8a:19:7f:df:ba:e5:38:e8:e7:08:96:5f:07:
    f0:9a:be:25:80:a6:2d:99:31:77:d0:e4:a4:6b:25:
    4e:2d:1a:f6:0d
rime2:
    00:d3:9e:4f:eb:ab:79:de:76:3c:f8:a7:1f:3b:9b:
    a4:bb:fe:4f:e4:70:a3:ce:3d:cd:3d:6e:50:d9:8f:
    c5:40:5f:f7:00:f0:c3:4d:30:05:a3:93:c8:fd:df:
    5a:dd:6b:95:03:f2:e7:d0:4e:91:88:7e:fb:64:77:
    e7:f0:21:48:49
xponent1:
    1b:78:77:26:48:52:53:c1:9c:68:3b:e7:73:fd:e5:
    4b:c7:97:01:dd:45:50:2a:10:b2:ed:fe:1d:b0:0b:
    ec:66:67:eb:19:d3:bb:e1:b0:2f:59:2f:6d:a5:15:
    d8:5b:31:2f:d3:a5:d0:82:11:e7:ab:02:7a:38:df:
    ec:9d:8b:6d
xponent2:
    75:4e:57:cd:33:23:fe:4e:9a:e3:d7:78:77:c9:82:
    9a:f7:91:7f:f7:74:c6:39:fa:10:a8:9b:46:ce:ec:
    b0:0f:c2:53:92:23:21:21:92:ae:a7:98:8e:2a:87:
    2b:20:9c:dd:30:84:92:33:4b:77:57:b4:b1:6f:ca:
    71:91:71:89
oefficient:
    00:e7:64:95:d5:23:87:f5:bf:04:bd:9c:87:37:80:
    db:ba:7a:10:07:91:88:d5:5f:00:21:b2:4a:8f:bd:
    7e:91:18:d6:19:0f:16:ba:44:68:0c:0c:1d:f5:80:
    65:5f:ab:5b:9a:21:fd:33:e1:38:4c:11:c4:22:e9:
    91:09:aa:93:c1
riting RSA key
----BEGIN RSA PRIVATE KEY-----
IICXAIBAAKBgQDDLTfto6GUiqMdWNx+NEBlYYR2l7oo3yTqZGPQyC9r9g3hKKpq
CFkQtHKFmUvBOdZNWx7/m8V1QK1/qXS56c96Yhgqwoe6q1WIi14Q4J+h+TUY4fX
8l9b35hz0Ac6CvC4q1ws247AuDgrOkV/M37i94mS1KqlOk2MMfbWZDRtQIDAQAB
oGAMHdAFiC19P7gNl9kkWpEO2iVziUrMw8GSbYYGzY6oGJ/W9QPTUkQEaeOFNKu
ZgsIrjjcX7i8tbsT2kmqdshcg0ndphQC6hH52P/h/dcGvoD1HpLm6znhCTwwinM
sgrQDKQ/R8Qw8ZxrHLDnxiE+Sjm+6Q3+5WePJNwVYu/rMECQQDsHCfX9lnpxad+
MxCYxX63ABzoyyq79AXDgkN3xWrihl/37rlOOjnCJZfB/CaviWApi2ZMXfQ5KRr
U4tGvYNAkEA0S5P66t53nY8+KcfO5uku/5P5HCjzj3NPW5Q2Y/FQF/3APDOTTAF
5PI/d9a3WuVA/Ln0E6RiH77ZHfn8CFISQJAG3h3JkhSU8GcaDvnc/3lS8eXAd1F
CoQsu3+HbAL7GZn6xnTu+GwL1kvbaUV2FsxL90l0IIR56sCejjf7J2LbQJAdU5X
TMj/k6a49d4d8mCmveRf/d0xjn6EKibRs7ssA/CU5IjISGSrqeYjiqHKyCc3TCE
jNLd1e0sW/KcZFxiQJBAOdkldUjh/W/BL2chzeA27p6EAeRiNVfACGySo+9fpEY
hkPFrpEaAwMHfWAZV+rW5oh/TPhOEwRxCLpkQmqk8E=
----END RSA PRIVATE KEY-----
[11/30/22]seed@VM:~/CRYPTL3$ █
```

b. Generate a CSR

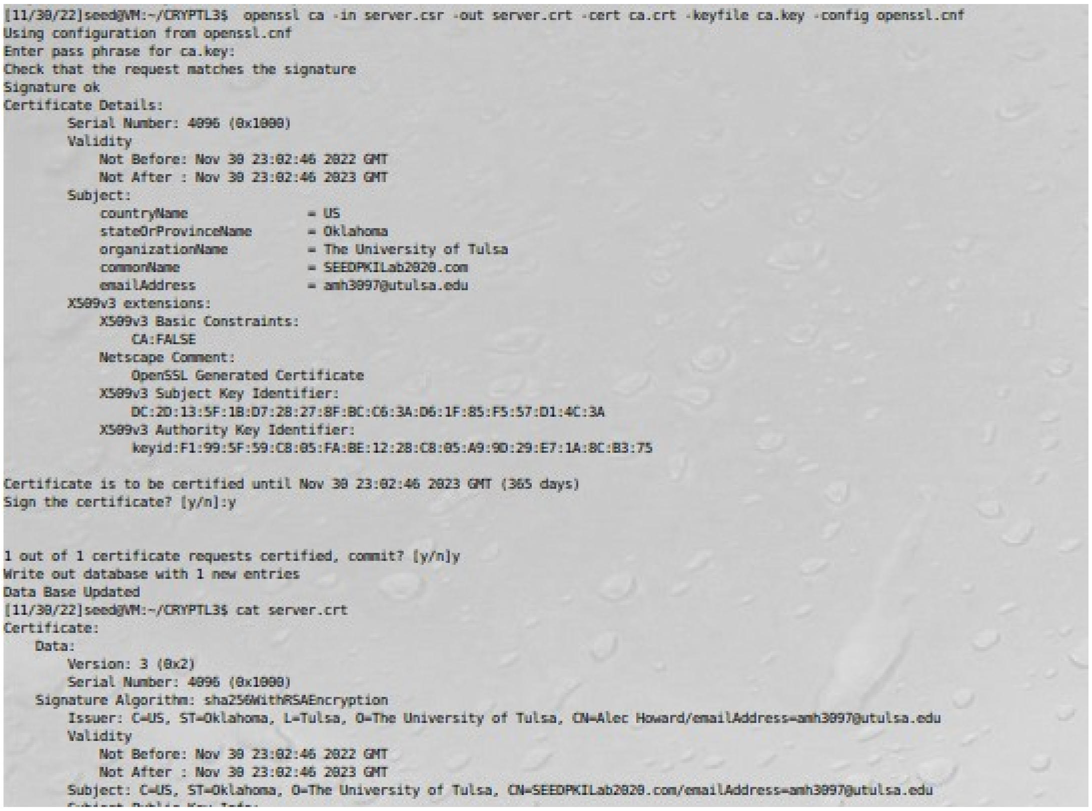
i. 

```
[11/30/22]seed@VM:~/CRYPTL3$ openssl req -new -key server.key -out server.csr -config openssl.cnf
Enter pass phrase for server.key:
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]:US
State or Province Name (full name) [Some-State]:Oklahoma
Locality Name (eg, city) []:Tulsa
Organization Name (eg, company) [Internet Widgits Pty Ltd]:The University of Tulsa
Organizational Unit Name (eg, section) []:.
Common Name (e.g. server FQDN or YOUR name) []:SEEDPKILab2020.com
Email Address []:amh3097@utulsa.edu

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:.
An optional company name []:.
[11/30/22]seed@VM:~/CRYPTL3$ cat server.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIB0zCCATwCAQAwgZIxCzAJBgNVBAYTAlVTMREwDwYDVQQIDAhPa2xhaG9tYTEO
MAwGA1UEBwwFVHVsc2ExIDAeBgNVBAoMF1RoZSBVbml2ZXJzaXR5IG9mIFR1bHNh
MRswGQYDVQQDDBJTRUVEUEtJTGFiMjAyMC5jb20xITAfBgkqhkiG9w0BCQEWEmFt
aDMwOTdAdXR1bHNhLmVkdTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAwy03
7aOhlIqjHVjcfjRAZWGEdpe6KN8k6mRj0Mgva/YN4SiqakghZELRyhZlLwTnWTVs
e/SvFdUCtf6l+UunPemIYKsKHuqtViIteEOCfofk1GOH18fJfW9+Yc9AHOgrwuKt
cLNuOwLg4KzpFfzN+4veJktSqpTpNjDH21mQ0bUCAwEAAaAAMA0GCSqGSIb3DQEB
CwUAA4GBAG+d4S2UN8vF3+JVy3uOtUzZm8s8WGXT7X6h4495anx3BKT5TzvwMWG9
e0yN0CBvWrpK8pYiboAWyptYFOwJ9K46sseB0qQ0tLzS/Qn6Te4FmxOonvbzbBMc
qz4TX+U/fSSulYqK6qUAy773Cb9N+5Kje0AP3UEZYcfoh32APgbT
-----END CERTIFICATE REQUEST-----
```

c. Generating Certificates

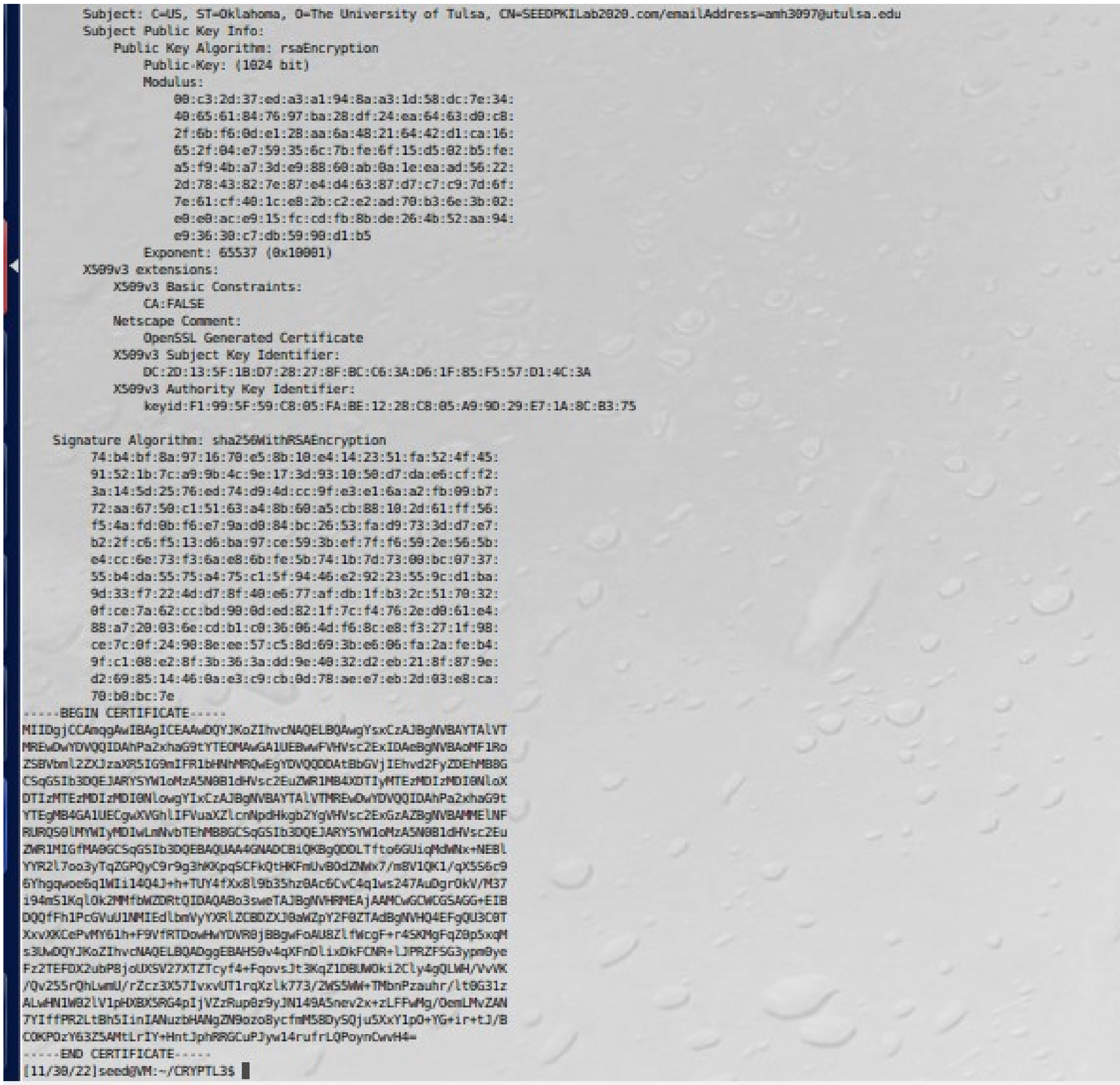
i.



```
[11/30/22]seed@VM:~/CRYPTL3$  openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Nov 30 23:02:46 2022 GMT
            Not After : Nov 30 23:02:46 2023 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = Oklahoma
            organizationName          = The University of Tulsa
            commonName                = SEEDPKILab2020.com
            emailAddress              = amh3097@utulsa.edu
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                DC:2D:13:5F:1B:D7:28:27:8F:BC:C6:3A:D6:1F:85:F5:57:D1:4C:3A
            X509v3 Authority Key Identifier:
                keyid:F1:99:5F:59:C8:05:FA:BE:12:28:C8:05:A9:9D:29:E7:1A:8C:B3:75

Certificate is to be certified until Nov 30 23:02:46 2023 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
[11/30/22]seed@VM:~/CRYPTL3$ cat server.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Oklahoma, L=Tulsa, O=The University of Tulsa, CN=Alec Howard/emailAddress=amh3097@utulsa.edu
        Validity
            Not Before: Nov 30 23:02:46 2022 GMT
            Not After : Nov 30 23:02:46 2023 GMT
        Subject: C=US, ST=Oklahoma, O=The University of Tulsa, CN=SEEDPKILab2020.com/emailAddress=amh3097@utulsa.edu
        Subject Public Key Info:
```

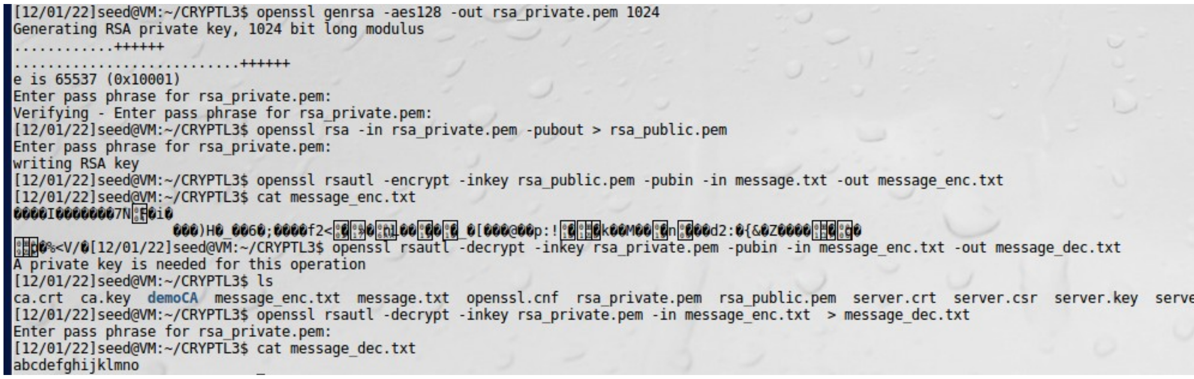


```
        Subject: C=US, ST=Oklahoma, O=The University of Tulsa, CN=SEEDPKILab2020.com/emailAddress=amh3097@utulsa.edu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:c3:2d:37:ed:a3:a1:94:8a:a3:1d:58:dc:7e:34:
                    40:65:61:84:76:97:ba:28:df:24:ea:64:63:d0:c8:
                    2f:6b:f6:0d:e1:28:aa:6a:48:21:64:42:d1:ca:16:
                    65:2f:04:e7:59:35:6c:7b:fe:6f:15:d5:02:b5:fe:
                    a5:f9:4b:a7:3d:e9:88:60:ab:0a:1e:ea:ad:56:22:
                    2d:78:43:82:7e:87:e4:d4:63:87:d7:c7:c9:7d:6f:
                    7e:61:cf:40:1c:e8:2b:c2:e2:ad:70:b3:6e:3b:02:
                    e0:e0:ac:e9:15:fc:cd:fb:8b:de:26:4b:52:aa:94:
                    e9:36:30:c7:db:59:90:d1:b5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                DC:2D:13:5F:1B:D7:28:27:8F:BC:C6:3A:D6:1F:85:F5:57:D1:4C:3A
            X509v3 Authority Key Identifier:
                keyid:F1:99:5F:59:C8:05:FA:BE:12:28:C8:05:A9:9D:29:E7:1A:8C:B3:75

    Signature Algorithm: sha256WithRSAEncryption
         74:b4:bf:8a:97:16:70:e5:8b:10:e4:14:23:51:fa:52:4f:45:
         91:52:1b:7c:a9:9b:4c:9e:17:3d:93:10:50:d7:da:e6:cf:f2:
         3a:14:5d:25:76:ed:74:d9:4d:cc:9f:e3:e1:6a:a2:fb:09:b7:
         72:aa:67:50:c1:51:63:a4:8b:60:a5:cb:88:10:2d:61:ff:56:
         f5:4a:fd:0b:f6:e7:9a:d0:84:bc:26:53:fa:d9:73:3d:d7:e7:
         b2:2f:c6:f5:13:d6:ba:97:ce:59:3b:ef:7f:f6:59:2e:56:5b:
         e4:cc:6e:73:f3:6a:e8:6b:fe:5b:74:1b:7d:73:00:bc:07:37:
         55:b4:da:55:75:a4:75:c1:5f:94:46:e2:92:23:55:9c:d1:ba:
         9d:33:f7:22:4d:d7:8f:40:e6:77:af:db:1f:b3:2c:51:70:32:
         0f:ce:7a:62:cc:bd:90:0d:ed:82:1f:7c:f4:76:2e:d0:61:e4:
         88:a7:20:03:6e:cd:b1:c0:36:06:4d:f6:8c:e8:f3:27:1f:98:
         ce:7c:0f:24:90:8e:ee:57:c5:8d:69:3b:e6:06:fa:2a:fe:b4:
         9f:c1:08:e2:8f:3b:36:3a:dd:9e:40:32:d2:eb:21:8f:87:9e:
         d2:69:85:14:46:0a:e3:c9:cb:0d:78:ae:e7:eb:2d:03:e8:ca:
         70:b0:bc:7e
-----BEGIN CERTIFICATE-----
MIIDgjCCAmqgAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwgYsxCzAJBgNVBAYTAlVT
MREwDwYDVQQIDAhPa2xhaG9tYTEOMAwGA1UEBwwFVHVsc2ExIDAeBgNVBAoMF1Ro
ZSBVbml2ZXJzaXR5IG9mIFR1bHNhMRQwEgYDVQQDDAtBbGVjIEhvd2FyZDEhMB8G
CSqGSIb3DQEJARYSYW1oMzA5N0B1dHVsc2EuZWR1MB4XDTIyMTEzMDIzMDI0NloX
DTIzMTEzMDIzMDI0NlowgYIxCzAJBgNVBAYTAlVTMREwDwYDVQQIDAhPa2xhaG9t
YTEgMB4GA1UECgwXVGhlIFVuaXZlcnNpdHkgb2YgVHVsc2ExGzAZBgNVBAMMElNF
RURQS0lMYWIyMDIwLmNvbTEhMB8GCSqGSIb3DQEJARYSYW1oMzA5N0B1dHVsc2Eu
ZWR1MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDDLTfto6GUiqMdWNx+NEBl
YYR2l7oo3yTqZGPQyC9r9g3hKKpqSCFkQtHKFmUvBOdZNWx7/m8V1QK1/qX556c9
6Yhgqwoe6q1WIi14Q4J+h+TUY4fXx8l9b35hz0Ac6CvC4q1ws247AuDgrOkV/M37
i94mS1Kql0k2MMfbWZDRtQIDAQABo3sweTAJBgNVHRMEAjAAMCwGCWCGSAGG+EIB
DQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQU3C0T
XxvXKCePvMY61h+F9VfRTDowHwYDVR0jBBgwFoAU8ZlfWcgF+r4SKMgFqZ0p5xqM
s3UwDQYJKoZIhvcNAQELBQADggEBAHS0v4qXFnDlixDkFCNR+lJPRZFSG3ypm0ye
Fz2TEFDX2ubP8joUXSV27XTZTcyf4+FqovsJt3KqZ1DBUWOki2Cly4gQLWH/VvVK
/Qv255rQhLwmU/rZcz3X57IvxvUT1rqXzlk773/2WS5WW+TMbnPzauhr/lt0G31z
ALwHN1W02lV1pHXBX5RG4pIjVZzRup0z9yJN149A5nev2x+zLFFwMg/OemLMvZAN
7YIffPR2LtBh5IinIANuzbHANgZN9ozo8ycfmM58DySQju5XxY1pO+YG+ir+tJ/B
COKPOzY63Z5AMtLrIY+HntJphRRGCuPJyw14rufrLQPoynCwvH4=
-----END CERTIFICATE-----
[11/30/22]seed@VM:~/CRYPTL3$
```

3. Use PKI for Websites
    a. It is a list of ciphers supported in server binary.
    b. I edited a bit in the middle of the file, but could not observe any visible change\
    c. It brought me to the server page because we added the domain to /etc/hosts under 127.0.0.1
4. RSA vs AES
    a. Message: abcdefghijklmno
    b. Encrypt:

i.



```
[12/01/22]seed@VM:~/CRYPTL3$ openssl genrsa -aes128 -out rsa_private.pem 1024
Generating RSA private key, 1024 bit long modulus
...........++++++
...........................++++++
e is 65537 (0x10001)
Enter pass phrase for rsa_private.pem:
Verifying - Enter pass phrase for rsa_private.pem:
[12/01/22]seed@VM:~/CRYPTL3$ openssl rsa -in rsa_private.pem -pubout > rsa_public.pem
Enter pass phrase for rsa_private.pem:
writing RSA key
[12/01/22]seed@VM:~/CRYPTL3$ openssl rsautl -encrypt -inkey rsa_public.pem -pubin -in message.txt -out message_enc.txt
[12/01/22]seed@VM:~/CRYPTL3$ cat message_enc.txt
����I�������7N�F�i�
                   ���)H�_��6�;����f2<������n���������_�[���@��p:!�����k��M���n����d2:�{&�Z����������
���%<V/�[12/01/22]seed@VM:~/CRYPTL3$ openssl rsautl -decrypt -inkey rsa_private.pem -pubin -in message_enc.txt -out message_dec.txt
A private key is needed for this operation
[12/01/22]seed@VM:~/CRYPTL3$ ls
ca.crt  ca.key  democA  message_enc.txt  message.txt  openssl.cnf  rsa_private.pem  rsa_public.pem  server.crt  server.csr  server.key  serve
[12/01/22]seed@VM:~/CRYPTL3$ openssl rsautl -decrypt -inkey rsa_private.pem -in message_enc.txt  > message_dec.txt
Enter pass phrase for rsa_private.pem:
[12/01/22]seed@VM:~/CRYPTL3$ cat message_dec.txt
abcdefghijklmno
```

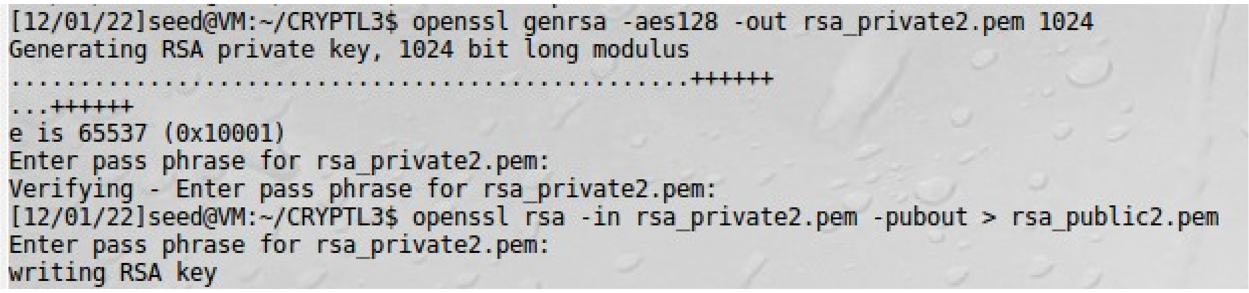
ii. openssl enc -aes-128-cbc -in message.txt -out message_enc2.txt

iii. I created a script for each method that ran the operation 1000 times. Then I divided the overall runtime by 1000 for the averages:

1. AES: 0.007248 s MOST TIME
2. RSA ENC: 0.005828 s LEAST TIME
3. RSA DEC: 0.006969 s

5. Create Digital Signature

a.



```
[12/01/22]seed@VM:~/CRYPTL3$ openssl genrsa -aes128 -out rsa_private2.pem 1024
Generating RSA private key, 1024 bit long modulus
................................................++++++
...++++++
e is 65537 (0x10001)
Enter pass phrase for rsa_private2.pem:
Verifying - Enter pass phrase for rsa_private2.pem:
[12/01/22]seed@VM:~/CRYPTL3$ openssl rsa -in rsa_private2.pem -pubout > rsa_public2.pem
Enter pass phrase for rsa_private2.pem:
writing RSA key
```

openssl dgst -sha256 -sign rsa_private.pem -out example.sha256.signature example.sha256

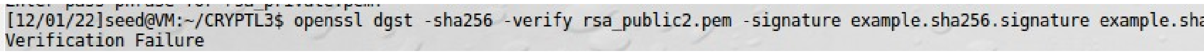
b. openssl dgst -sha256 -verify rsa_public2.pem -signature example.sha256.signature example.sha256

c. .

i. Original: alldogsgotoheaven

ii. Modified: allcatsgotoheaven

iii.



```
Enter pass phrase for rsa_private.pem:
[12/01/22]seed@VM:~/CRYPTL3$ openssl dgst -sha256 -verify rsa_public2.pem -signature example.sha256.signature example.sha
Verification Failure
```