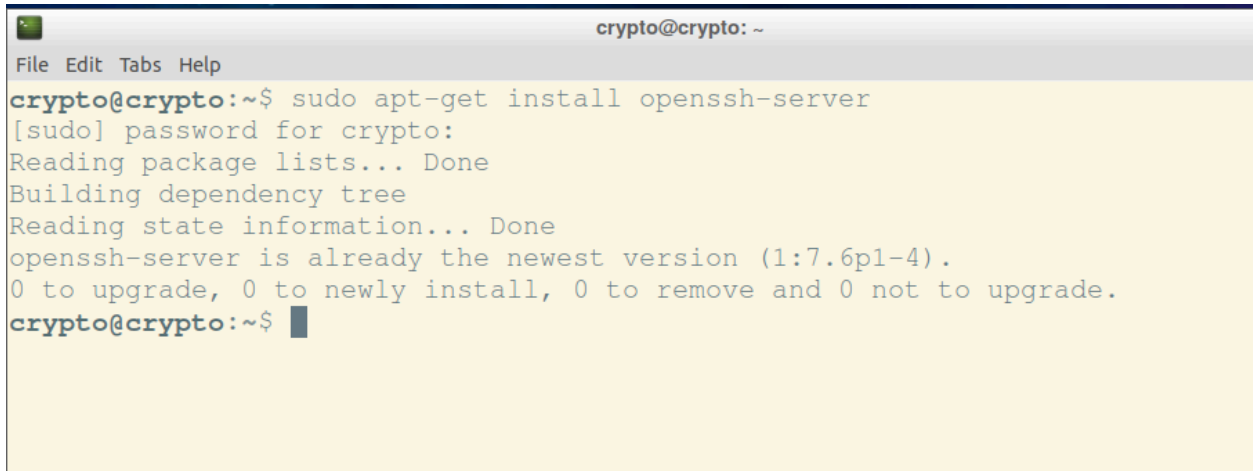


Project 1 Part 1

SSH to localhost

3.1.1

install and run the SSH server in the VM

A terminal window titled 'crypto@crypto: ~' with a menu bar 'File Edit Tabs Help'. The terminal shows the command 'sudo apt-get install openssh-server' being executed. The output indicates that the package is already installed and is the newest version (1:7.6p1-4). The terminal text is as follows:

```
crypto@crypto:~$ sudo apt-get install openssh-server
[sudo] password for crypto:
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-server is already the newest version (1:7.6p1-4).
0 to upgrade, 0 to newly install, 0 to remove and 0 not to upgrade.
crypto@crypto:~$
```

check the ssh configuration

```
crypto@crypto:~$ sudo service sshd start
crypto@crypto:~$ which sshd
/usr/sbin/sshd
crypto@crypto:~$
```

```
GNU nano 2.9.3 /etc/ssh/sshd_config Modified

#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will

^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos
^X Exit          ^R Read File    ^\ Replace      ^U Uncut Text   ^T To Spell     ^_ Go To Line
```

ssh to localhost with your user name and password

```
crypto@crypto:~$ ssh localhost
The authenticity of host 'localhost (:::1)' can't be established.
ECDSA key fingerprint is SHA256:/lgGLctckZ35iQY16Whblg0G04YP4QfHxZD1/iB1m6w.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
crypto@localhost's password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

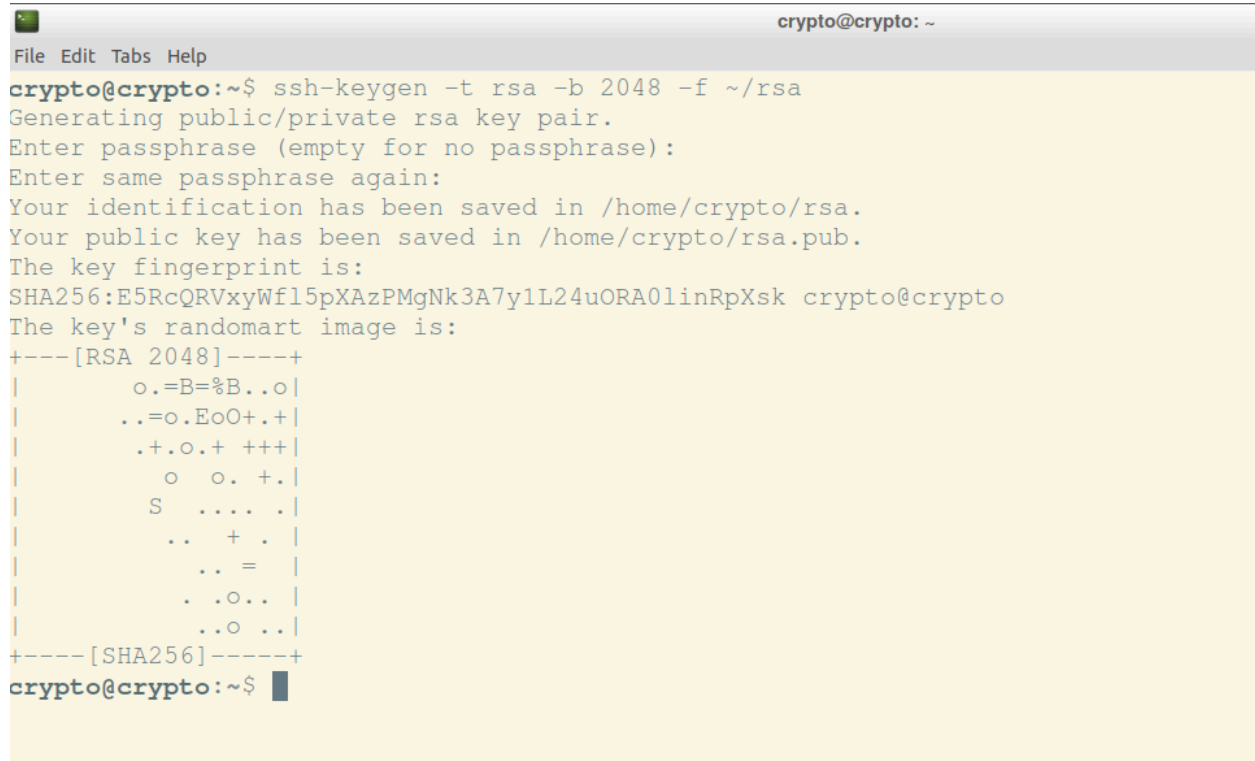
0 packages can be updated.
0 updates are security updates.

Last login: Tue Apr  1 22:09:38 2025 from 127.0.0.1
crypto@crypto:~$ exit
logout
Connection to localhost closed.
crypto@crypto:~$
```

3.2 ssh to localhost with public-key authentication

3.2.1

generate an RSA key pair and set a passphrase to protect it



```
crypto@crypto: ~  
File Edit Tabs Help  
crypto@crypto:~$ ssh-keygen -t rsa -b 2048 -f ~/rsa  
Generating public/private rsa key pair.  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/crypto/rsa.  
Your public key has been saved in /home/crypto/rsa.pub.  
The key fingerprint is:  
SHA256:E5RcQRVxyWf15pXAzPMgNk3A7y1L24uORA0linRpXsk crypto@crypto  
The key's randomart image is:  
+---[RSA 2048]-----+  
|      o.=B=%B..o|  
|      ..=o.EoO+.+|  
|      .+.o.+ +++|  
|      o  o. +. |  
|      S  .... .|  
|      ..  + .  |  
|      .. =    |  
|      . .o..  |  
|      ..o ..  |  
+-----[SHA256]-----+  
crypto@crypto:~$
```

check the generated private key

configure the ssh server accept the RSA key in authentication

```
crypto@crypto: ~
File Edit Tabs Help
GNU nano 2.9.3 /etc/ssh/sshd_config

#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos  M-U Undo
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line M-E Redo
```

```
crypto@crypto: ~
File Edit Tabs Help
GNU nano 2.9.3 /etc/ssh/sshd_config

#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication no
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
#ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos  M-U Undo
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line M-E Redo
```

```

crypto@crypto:~$ sudo nano /etc/ssh/sshd_config
[sudo] password for crypto:
crypto@crypto:~$ sudo service ssh restart
crypto@crypto:~$ ssh -i ~/rsa localhost
crypto@localhost's password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

0 packages can be updated.
0 updates are security updates.

Last login: Tue Apr  1 22:10:31 2025 from ::1
crypto@crypto:~$ █

```

4. Set up the Certificate Authority on the VM

CA key

```

crypto@crypto:~$ mkdir ~/myca/private
crypto@crypto:~$ touch ~/myca/mycaindex
crypto@crypto:~$ openssl genpkey -algorithm RSA -out ~/myca/private/ca.key -aes256
.....+++++
.....+++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
crypto@crypto:~$ openssl req -key ~/myca/private/ca.key -new -x509 -out ~/myca/ca.crt -days 3650
Enter pass phrase for /home/crypto/myca/private/ca.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]:AU
State or Province Name (full name) [Some-State]:NSW
Locality Name (eg, city) []:SYD
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UTS
Organizational Unit Name (eg, section) []:FEIT
Common Name (e.g. server FQDN or YOUR name) []:utscrypto.com.au
Email Address []:utscrypto@netsec.com.au

```

```
crypto@crypto:~$ cd ~/myca/private
crypto@crypto:~/myca/private$ openssl rsa -in ca.key -text
Enter pass phrase for ca.key:
RSA Private-Key: (1024 bit, 2 primes)
modulus:
 00:96:c5:7a:1b:fd:a2:f6:21:07:c4:b8:22:75:b7:
 81:9c:bb:00:6d:0e:23:83:2b:9a:73:13:cb:aa:b8:
 20:98:a4:5c:f5:65:c6:4d:87:34:87:47:9d:2b:38:
 15:4c:8b:26:ae:eb:8e:54:a1:44:a9:80:26:d0:57:
 52:f3:5e:b9:d5:34:3b:43:aa:65:dd:4e:5a:cc:d9:
 98:ed:b0:f8:74:2f:87:2f:02:ab:23:fd:0a:d5:d3:
 66:98:96:3c:8c:a6:88:ea:d7:35:ee:7d:fd:40:d4:
 b7:02:b7:9a:5c:9d:a7:df:13:4f:f8:76:ed:b8:2b:
 08:4e:48:32:a4:7c:a3:12:8b
publicExponent: 65537 (0x10001)
privateExponent:
 48:a9:23:10:1a:4c:4f:11:dc:0c:92:31:09:4a:46:
 cc:a1:d2:b2:bb:fd:a1:59:82:35:b3:74:93:f1:e8:
 c3:a7:72:a5:51:47:20:55:e8:9a:c9:88:95:2b:92:
 18:31:77:93:15:32:a2:d6:95:a0:9a:82:1a:25:fb:
 74:0e:52:c0:0f:ed:ee:5c:f3:98:67:25:2e:8b:e2:
 01:8d:45:4f:43:18:34:e9:e7:68:3f:e3:4a:ff:c9:
 a5:85:30:e6:c7:4b:bb:8b:17:10:23:82:ef:60:96:
 0d:76:44:86:c6:70:6e:0c:95:33:c3:47:c7:9a:79:
 c7:75:74:cd:0b:3e:bf:01
primel:
 00:c5:b5:74:f2:3e:e7:26:a5:94:3c:8e:31:01:89:
```

```

2d:de:1b:dd
exponent2:
29:cc:8b:52:51:08:d3:4f:f3:4c:6c:68:17:06:6e:
58:a0:e9:f0:6c:57:a8:0d:ba:08:c1:4a:18:64:7f:
47:fb:a3:3f:94:98:3f:7a:89:e5:57:fd:b2:cd:73:
e7:13:73:f5:5d:ab:d6:53:9f:eb:f9:50:d6:8d:8d:
75:6f:44:c1
coefficient:
00:bb:55:79:cd:5e:19:9d:61:d6:15:8e:f8:db:03:
a2:2f:f4:ef:c7:8f:8e:b2:1d:36:98:de:20:c3:0c:
b4:dc:23:4e:89:0d:60:b3:c2:19:c5:85:a8:34:19:
9b:df:49:fe:e6:57:43:6b:68:27:8e:ba:45:9c:44:
89:30:d1:cb:ef
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQCWxXob/aL2IQfEuCJ1t4GcuwBtDiODK5pzE8uquCCYpFz1ZcZN
azSHR50rOBVMiyau645UoUSpgCbQV1LzXrnVNDtDqmXdTlrM2ZjtsPh0L4cvAqsj
/QrV02aYlJyMpojqlzXufflA1LcCt5pcnaFFE0/4du24KwhOSDKkfKMSiwIDAQAB
AoGASKkjEBpMTxHcDJIXcUpGzKHSsrV9oVMcNbN0k/How6dypVFHIFXomsmIlSuS
GDF3kxUyotaVoJqCGiX7dA5SwA/t7lzzmGclLoviAY1FT0MYNOnnaD/jSv/JpYUw
5sdLu4sXECOC72CWDXZEhsZwbgyVM8NHx5p5x3V0zQs+vWECQQDFtXTyPucmpZQ8
jjEBichgcE+WmCF1CsJa+VuaVVVWi8eufHHmGzekyXRG+qlL0sJ5JOkC3qU8pRx2
01Z1HaEnAkEAwzlOgF8SeCH7Q2yrs8k4UgL3RGURctEKoHZF8RZTIOR5WExUb0Qv
SUlo/ZOIsZypdyBsXpEwvZ1HOORXoDIZ/QJAZsrzZMfjsqpAKkPbousaLVn3Z1rt
cfVoG5iuUc2wMvE1/rhhF7xq79h2BjlpMC0CQ643H/DWhHNSGzPCLd4b3QJAKcyL
JlEI00/zTGxoFwZuWKDp8GxXqA26CMFKGGR/R/ujP5SYP3qJ5Vf9ss1z5xNz9V2r
llof6/lQ1o2NdW9EwQJBALtVecleGZ1h1hWO+NsDoi/078ePjridNpjeIMMMtNwj
TokNYLPCCGWFqDQZm99J/uZXQ2toJ466RZxEiTDRy+8=
-----END RSA PRIVATE KEY-----
crypto@crypto:~/myca/private$

```

CA Certificate

```

crypto@crypto: ~/myca
File Edit Tabs Help
crypto@crypto:~/myca/private$ openssl req -key ~/myca/private/ca.key -new -x509 -out ~/myca/ca.crt -days 365
0
Enter pass phrase for /home/crypto/myca/private/ca.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]:AU
State or Province Name (full name) [Some-State]:NSW
Locality Name (eg, city) []:SYD
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UTS
Organizational Unit Name (eg, section) []:FEIT
Common Name (e.g. server FQDN or YOUR name) []:utscrypto.com.au
Email Address []:utscrypto@netsec.com.au
crypto@crypto:~/myca/private$ openssl x509 -in ca.crt -text
x509: Cannot open input file ca.crt, No such file or directory
x509: Use -help for summary.
crypto@crypto:~/myca/private$ cd /myca/
-bash: cd: /myca/: No such file or directory
crypto@crypto:~/myca/private$ cd ~/myca/
crypto@crypto:~/myca$ openssl x509 -in ca.crt -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            fd:a5:f1:2e:bc:11:cf:12
        Signature Algorithm: sha256WithRSAEncryption

```

```

X509v3 Basic Constraints: critical
CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
66:ca:0b:a1:44:8d:b5:ac:b4:c7:25:a6:2d:be:ac:79:02:0d:
2e:19:00:7c:0a:52:d3:de:2e:8b:85:60:ca:d0:7a:b2:b0:9d:
59:2b:3a:89:0e:71:2b:f0:93:f7:cf:ec:df:cc:4e:cc:e5:9f:
cd:35:b9:ea:8c:b6:b2:03:96:fc:c7:55:1c:c8:b5:c8:69:96:
82:d7:c0:17:bb:15:8e:88:61:26:e4:52:a0:50:55:54:ce:d8:
29:3f:b6:5d:ba:a1:df:a7:32:f1:e5:ae:b5:b8:ae:4e:9a:be:
fe:ae:11:dc:cb:57:ac:95:76:59:80:fc:f0:3a:f1:12:d4:8d:
3e:32
-----BEGIN CERTIFICATE-----
MIIC5zCCAlCgAwIBAgIJAP218S68Ec8SMA0GCSqGSIb3DQEBCwUAMIGKMqswCQYD
VQQGEwJBVTEMMMAoGA1UECAwDTlNXMQwwCgYDVQQHDANTWUQxDDAKBgNVBAoMA1VU
UzENMAAsGA1UECwwERkVJVDZMBcGA1UEAwwQdXRzY3J5cHRvLmNvbS5hdTENMCUG
CSqGSIb3DQEJARYYdXRzY3J5cHRvIEBuZXRzZWMuY29tLmF1MB4XDTE1MDQwMTEy
NDg0MFoXDTM1MDMzMDEyNDg0MFowYoxCzAJBgNVBAYTAkFVMQwwCgYDVQQIDANQ
U1cxDDAKBgNVBAcMA1NlZDEMMMAoGA1UECgwDVVVTMQ0wCwYDVQQLDARGRU1UMRkw
FwYDVQQDDDB1dHNjcnlwdG8uY29tLmF1MScwJQYJKoZIhvcNAQkBFhh1dHNjcnlw
dG8gQG51dHN1Yy5jb20uYXUwZz8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJbF
ehv9ovYhB8S4InW3gZy7AG0OI4MrnmMTy6q4IJikXPVlxk2HNIIdHnSs4FUyLJq7r
j1ShrKmAjtbXUvNeudU000OqZd1OWszZm02w+HQvhy8CqyP9CtXTZpiWPIymiOrX
Ne59/UDUtWk3mlydp98TT/h27bgrCE5IMqR8oxKLAGMBAAGjUzBRMB0GA1UdDgQW
BBRiNZwWaTkEpQKTtqg5U4X3dX7y7TAFBgNVHSMGDAWgBRiNZwWaTkEpQKTtqg5
U4X3dX7y7TAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4GBAGbKC6FE
jbWstMc1pi2+rHkCDS4ZAHwKUtPeLouFYMrQerKwnVkrOokOcSvwk/fP7N/MTsz1
n801ueqMtrIDlvzHVRzItchp1oLXwBe7FY6IYSbkUgBQVVT02Ck/tl26od+nMvHl
rrW4rk6avv6uEdzLV6yVdlmA/PA68RLUjT4y
-----END CERTIFICATE-----
crypto@crypto:~/myca$

```

5.1 Generate public/private key pair for the HTTPS server

5.1.2

```

crypto@crypto:~/myca$ openssl genpkey -algorithm RSA -out server.key -aes256
.....+++++
.....+++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
crypto@crypto:~/myca$ ls server.key
server.key
crypto@crypto:~/myca$ openssl rsa -in server.key -text
Enter pass phrase for server.key:
RSA Private-Key: (1024 bit, 2 primes)
modulus:
 00:d5:57:42:08:1f:6e:b6:dd:f1:62:54:e5:fc:e5:
 a9:56:b8:99:55:d3:09:5d:ba:43:c2:4d:4e:f7:ae:
 5d:16:6b:dd:c3:ce:91:74:82:ed:fc:4f:ff:b5:4f:
 c8:67:49:ae:b0:75:cc:ae:04:0d:9c:93:28:2f:cb:
 12:35:ad:b0:ab:f6:dc:4c:8a:27:95:d2:88:8c:99:
 72:3f:dd:18:97:9a:e6:a7:8a:77:48:bf:94:b8:c0:
 39:75:0b:cc:b0:d6:45:e6:c9:e8:e0:ad:0e:04:74:
 87:b7:e7:9a:a8:69:06:a2:20:55:d9:3b:1c:50:b0:
 92:70:d1:37:5d:4b:34:e1:c5
publicExponent: 65537 (0x10001)
privateExponent:
 5d:73:cf:b5:07:2f:d4:62:fc:6d:fa:8a:94:71:75:
 f0:4b:04:c0:17:a5:ae:ac:fd:29:8b:fb:df:7b:3d:
 c3:a8:94:88:45:60:6a:0d:40:7a:9a:00:85:47:e1:
 9d:7d:25:4c:9f:0d:7d:dc:c0:a9:a9:bc:9c:d2:f3:
 b3:17:d6:9f:70:b6:d5:98:fa:64:3d:86:39:0b:25:

```



```

5c:8e:d9:41
exponent2:
  71:8e:8f:3f:56:7d:49:4d:11:7e:0a:df:aa:b5:31:
  9d:28:55:c9:5b:91:04:17:1e:24:05:39:15:18:72:
  52:13:c0:63:97:de:ad:1b:e4:a0:26:79:f0:84:80:
  d5:27:9d:2d:f3:53:96:34:1a:86:87:de:58:f8:77:
  5a:f2:cc:c9
coefficient:
  00:d0:ac:fa:56:8c:56:10:36:cb:c4:29:13:1c:cf:
  49:a1:c3:3c:45:3e:29:84:84:cb:24:97:70:77:a2:
  e3:89:81:dd:32:77:f1:d2:17:e6:a7:d8:2e:13:ce:
  cc:67:c0:c5:ad:e9:33:56:12:61:1c:c7:8c:a7:b6:
  74:69:f5:39:b7
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIICXAIIBAAKBgQDVV0IIH2623fFiVOX85alWuJlV0wldukPCTU73rl0Wa93DzpF0
gu38T/+1T8hnSa6wdcyuBA2ckygvvyxI1rbCr9txMiieV0oiMmXI/3RiXmuanindI
v5S4wDl1C8ywlkXmyejgrQ4EdIe355qoaQaiIFXZOxxQsJJw0TddSzThxQIDAQAB
AoGAXXPtQcv1GL8bfgKlHF18EsEwBelrqz9KYv733s9w6iUiEVgag1AepoAhUfh
nX01TJ8NfdzAqam8nNLzsfWn3C21Zj6ZD2GOQslIK+S1Ga2tcIW7NPN6tRK93p
9R4ePVvF6oJ5+QSQK9UFzstIVaI62JC6LfzgO0lag1rEPwECQQDxP+QhliAaceMF
IQgv40fqT0hOGHMdYkPnS5Vt5SzPg/GO2DuNz2q2vlkCe+nI3ynfJB7EeexJNs7H
wzUlrH6xAkEA4mKIAYjbaeEHPDrarhGSF7hBTU6vleggQ5VifxHUEW22E+gIYwMk
3Y65+/g5I/8VbWJtKfPcAxi+pcxTcbohVQJAQ5mfl0uk20QmVP2YibKqKCHnJNr9
BrLOTDFvbGGCO/z9A7rQSVpxaM4ldVbAQpndTtt06hGaY2OC7PLXI7ZQQJAcY6P
PlZ9SU0RfgrfqrUxnShVfVuRBbceJAu5FRhyUhPAY5ferRvkoCZ58ISa1SedLfNT
ljQahofeWPh3WvLMYQJBANCs+laMVhA2y8QpExzPSaHDEPU+KYSEyySxcHei44mB
3TJ38dIX5qfYlhpOzGfAxa3pM1YSYRzHjKe2dGn10bc=
-----END RSA PRIVATE KEY-----
crypto@crypto:~/myca$ █

```

5.2 Generate a Certificate Signing Request

5.2.1

```

crypto@crypto:~/myca$ cd ~/myca
crypto@crypto:~/myca$ openssl req -new -key server.key -out server.csr
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]:AU
State or Province Name (full name) [Some-State]:NSW
Locality Name (eg, city) []:SYD
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UTS
Organizational Unit Name (eg, section) []:FEIT
Common Name (e.g. server FQDN or YOUR name) []:utscrypto.com.au
Email Address []:root@utscrypto.com.au

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
crypto@crypto:~/myca$ ls
ca.crt  mycaindex  newcerts  private  server.csr  server.key
crypto@crypto:~/myca$ openssl req -in server.csr -noout -text
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: C = AU, ST = NSW, L = SYD, O = UTS, OU = FEIT, CN = utscrypto.com.au, emailAddress = root@u

```

```

Data:
  Version: 1 (0x0)
  Subject: C = AU, ST = NSW, L = SYD, O = UTS, OU = FEIT, CN = utscrypto.com.au, emailAddress = root@utscrypto.com.au
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
      RSA Public-Key: (1024 bit)
      Modulus:
        00:d5:57:42:08:1f:6e:b6:dd:f1:62:54:e5:fc:e5:
        a9:56:b8:99:55:d3:09:5d:ba:43:c2:4d:4e:f7:ae:
        5d:16:6b:dd:c3:ce:91:74:82:ed:fc:4f:ff:b5:4f:
        c8:67:49:ae:b0:75:cc:ae:04:0d:9c:93:28:2f:cb:
        12:35:ad:b0:ab:f6:dc:4c:8a:27:95:d2:88:8c:99:
        72:3f:dd:18:97:9a:e6:a7:8a:77:48:bf:94:b8:c0:
        39:75:0b:cc:b0:d6:45:e6:c9:e8:e0:ad:0e:04:74:
        87:b7:e7:9a:a8:69:06:a2:20:55:d9:3b:1c:50:b0:
        92:70:d1:37:5d:4b:34:e1:c5
      Exponent: 65537 (0x10001)
  Attributes:
    a0:00
  Signature Algorithm: sha256WithRSAEncryption
    d1:d8:d5:70:90:af:a2:4a:56:40:c4:08:06:19:e9:04:5e:c1:
    b6:dc:99:12:bc:90:98:1c:d5:50:fe:f3:22:f9:69:4d:98:45:
    63:5b:f6:02:23:99:7b:ef:3b:00:25:d8:b3:d0:b6:59:0f:b0:
    b6:f4:90:8f:55:a7:81:98:06:f8:77:fd:6a:bb:d2:37:ee:03:
    b1:1c:f7:13:fe:be:67:9f:84:df:ec:c2:59:82:27:31:55:2e:
    a9:c1:13:19:c1:d1:ea:73:aa:ae:d6:3f:ac:e6:db:c2:0d:f1:
    6d:e2:e0:5e:df:85:8f:8d:b4:ba:12:59:a7:5b:56:51:60:71:
    d6:52
crypto@crypto:~/myca$

```

5.3 Sign the certificate

5.3.1

```

crypto@crypto:~/myca$ openssl x509 -req -in server.csr -CA ~/myca/ca.crt -CAkey ~/myca/private/ca.key -CAcreateserial -out server.crt -days
365
Signature ok
subject=C = AU, ST = NSW, L = SYD, O = UTS, OU = FEIT, CN = utscrypto.com.au, emailAddress = root@utscrypto.com.au
Getting CA Private Key
Enter pass phrase for /home/crypto/myca/private/ca.key:

```

```

crypto@crypto:~/myca$ openssl x509 -in server.crt -text -noout
Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number:
      8e:63:78:6b:d4:5e:6d:09
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C = AU, ST = NSW, L = SYD, O = UTS, OU = FEIT, CN = utscrypto.com.au, emailAddress = utscrypto@netsec.com.au
    Validity
      Not Before: Apr  2 06:20:05 2025 GMT
      Not After : Apr  2 06:20:05 2026 GMT
    Subject: C = AU, ST = NSW, L = SYD, O = UTS, OU = FEIT, CN = utscrypto.com.au, emailAddress = root@utscrypto.com.au
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (1024 bit)
      Modulus:
        00:d5:57:42:08:1f:6e:b6:dd:f1:62:54:e5:fc:e5:
        a9:56:b8:99:55:d3:09:5d:ba:43:c2:4d:4e:f7:ae:
        5d:16:6b:dd:c3:ce:91:74:82:ed:fc:4f:ff:b5:4f:
        c8:67:49:ae:b0:75:cc:ae:04:0d:9c:93:28:2f:cb:
        12:35:ad:b0:ab:f6:dc:4c:8a:27:95:d2:88:8c:99:
        72:3f:dd:18:97:9a:e6:a7:8a:77:48:bf:94:b8:c0:
        39:75:0b:cc:b0:d6:45:e6:c9:e8:e0:ad:0e:04:74:
        87:b7:e7:9a:a8:69:06:a2:20:55:d9:3b:1c:50:b0:
        92:70:d1:37:5d:4b:34:e1:c5
      Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
      3a:fa:5d:cl:4b:fc:91:82:7f:1e:f8:e1:79:9f:29:64:80:45:
      ca:ed:3b:4f:59:bb:47:b1:45:ab:ea:d7:8f:be:cb:c6:22:18:
      18:97:f4:16:fd:62:1e:e3:3d:f0:a1:57:63:c9:de:d2:b1:65:
      55:40:9f:d3:e2:3c:b9:ce:9e:c6:63:9c:5b:5b:e8:52:20:14:
      ba:2e:7c:ac:29:15:3d:09:0b:a1:98:2b:c5:56:aa:43:0b:f6:
      8a:aa:3e:a4:60:22:38:39:ff:a3:bb:38:aa:3b:4f:0a:2d:70:

```

6.Start test configurations

6.1

```
crypto@crypto:~/myca$ cat server.key server.crt > server.pem
crypto@crypto:~/myca$ sudo nano /etc/hosts
[sudo] password for crypto:
```

```
File Edit Tabs Help
GNU nano 2.9.3 /etc/hosts Modified

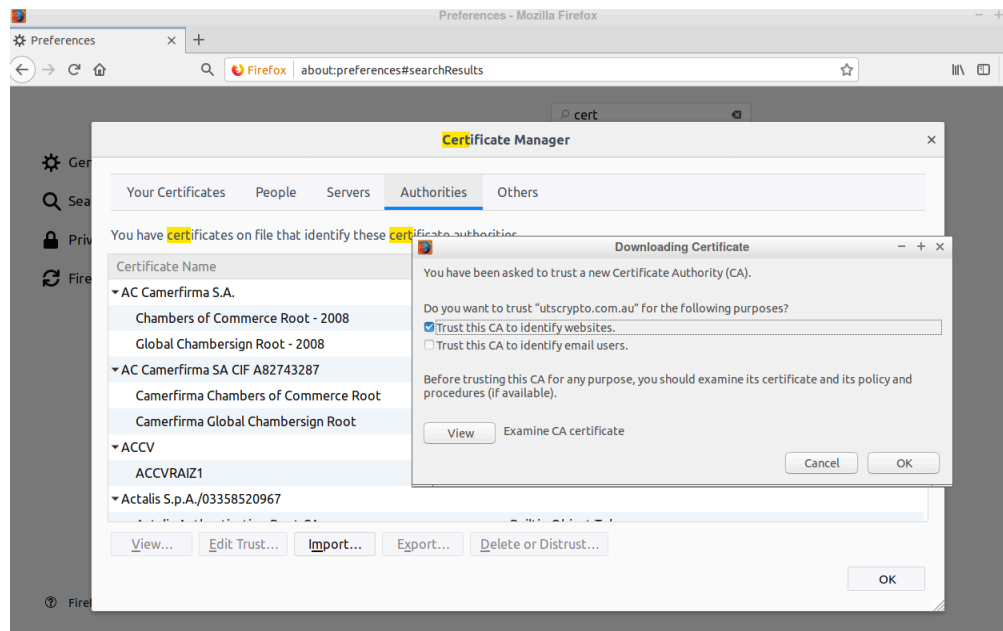
127.0.0.1    localhost
127.0.1.1    crypto
127.0.0.1    utscrypto.com.au

# The following lines are desirable for IPv6 capable hosts
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters

^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos      M-U Undo        M-A Mark Text
^X Exit          ^R Read File    ^_ Replace      ^U Uncut Text   ^T To Spell     ^_ Go To Line   M-E Redo       M-C Copy Text
```

```
crypto@crypto:~/myca$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
█
```

6.2 Configure the browser



```
crypto@crypto:~/myca$ openssl s_server -key server.key -cert server.crt -accept 4433 -www
Enter pass phrase for server.key:
Using default temp DH parameters
ACCEPT
ACCEPT
ACCEPT
```

