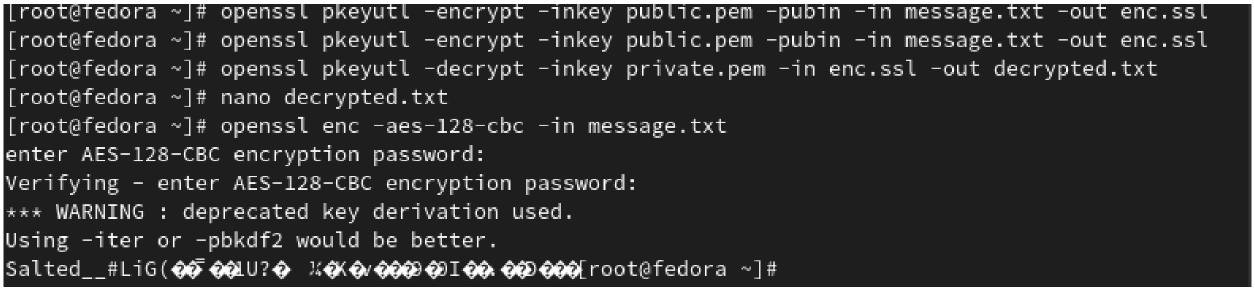
Project Group 5

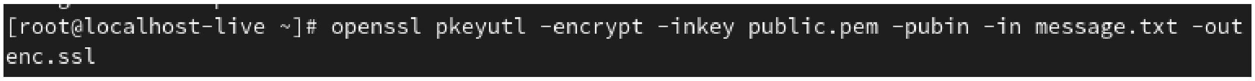
Question 1:



```
[root@fedora ~]# openssl pkeyutl -encrypt -inkey public.pem -pubin -in message.txt -out enc.ssl
[root@fedora ~]# openssl pkeyutl -encrypt -inkey public.pem -pubin -in message.txt -out enc.ssl
[root@fedora ~]# openssl pkeyutl -decrypt -inkey private.pem -in enc.ssl -out decrypted.txt
[root@fedora ~]# nano decrypted.txt
[root@fedora ~]# openssl enc -aes-128-cbc -in message.txt
enter AES-128-CBC encryption password:
Verifying - enter AES-128-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
Salted__#LiG(��̄��1U?� ¼�K�v���8�0I��.��D���[root@fedora ~]#
```

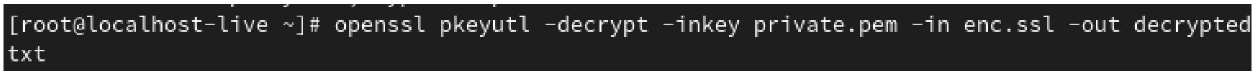
Question 2:

1.



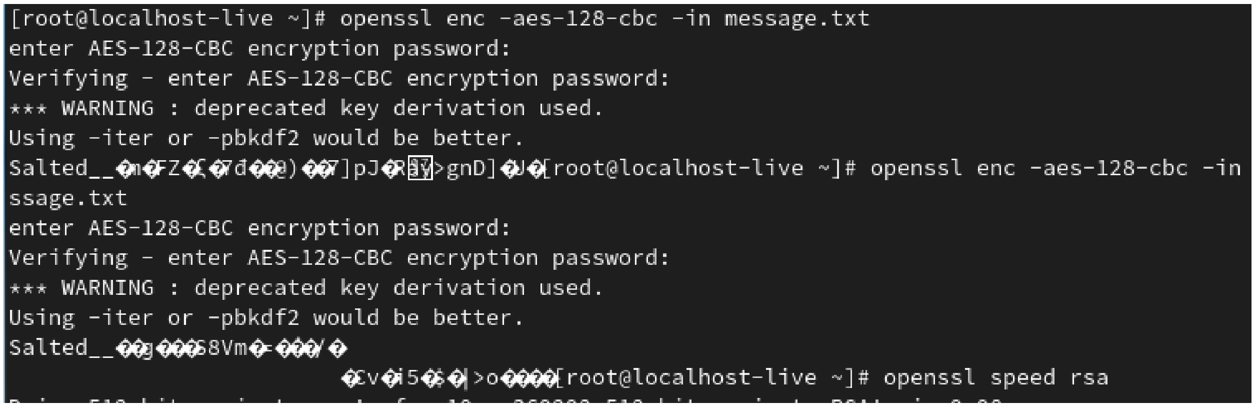
```
[root@localhost-live ~]# openssl pkeyutl -encrypt -inkey public.pem -pubin -in message.txt -out
enc.ssl
```

2.



```
[root@localhost-live ~]# openssl pkeyutl -decrypt -inkey private.pem -in enc.ssl -out decrypted
txt
```

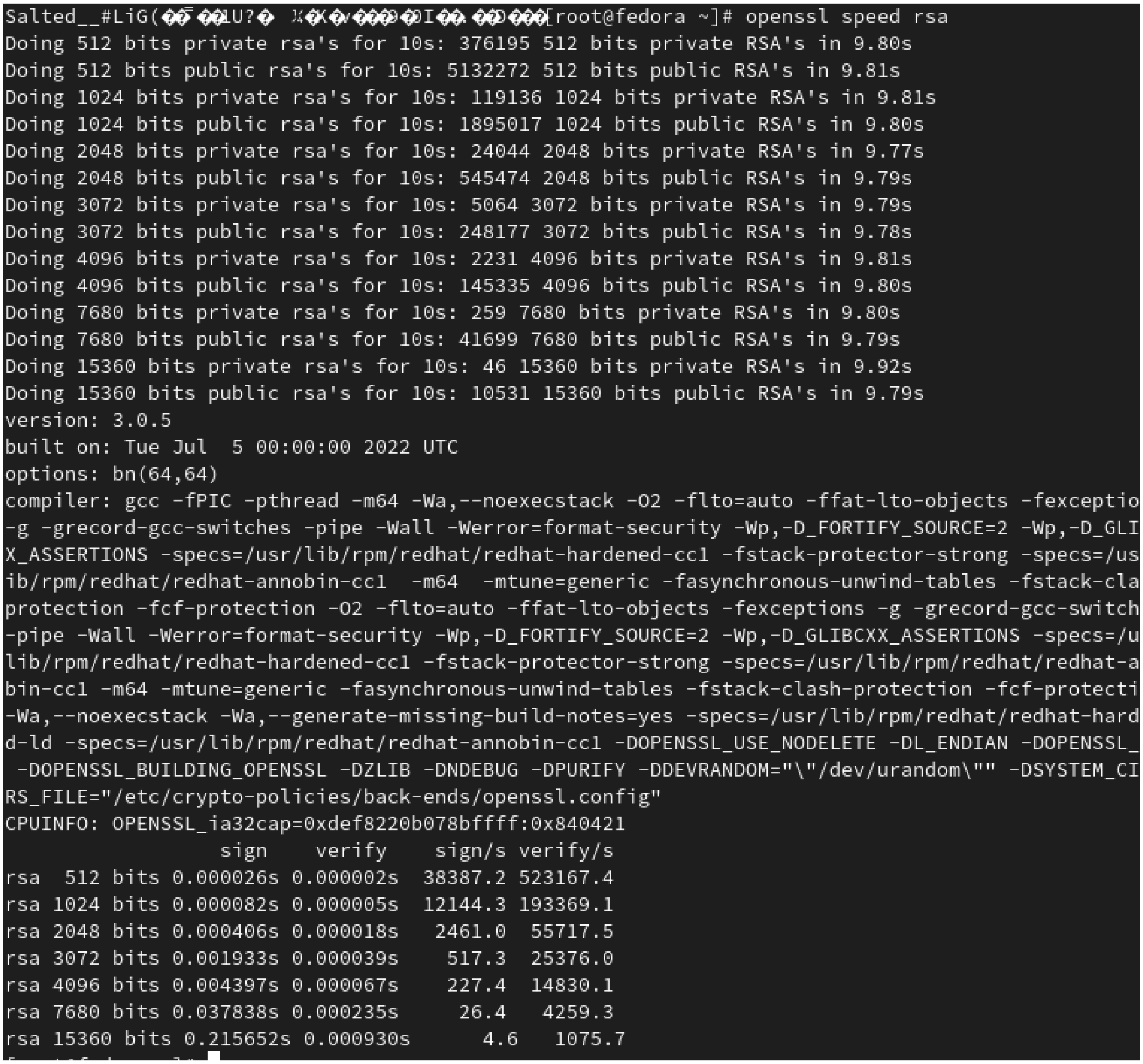
3.



```
[root@localhost-live ~]# openssl enc -aes-128-cbc -in message.txt
enter AES-128-CBC encryption password:
Verifying - enter AES-128-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
Salted__�m�FZ�(�7d��2)��7]pJ�R3Y>gnD]�U�[root@localhost-live ~]# openssl enc -aes-128-cbc -in
ssage.txt
enter AES-128-CBC encryption password:
Verifying - enter AES-128-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
Salted__��g���68Vm�-���/�
                          �Cv�i5�$�|>o����[root@localhost-live ~]# openssl speed rsa
```

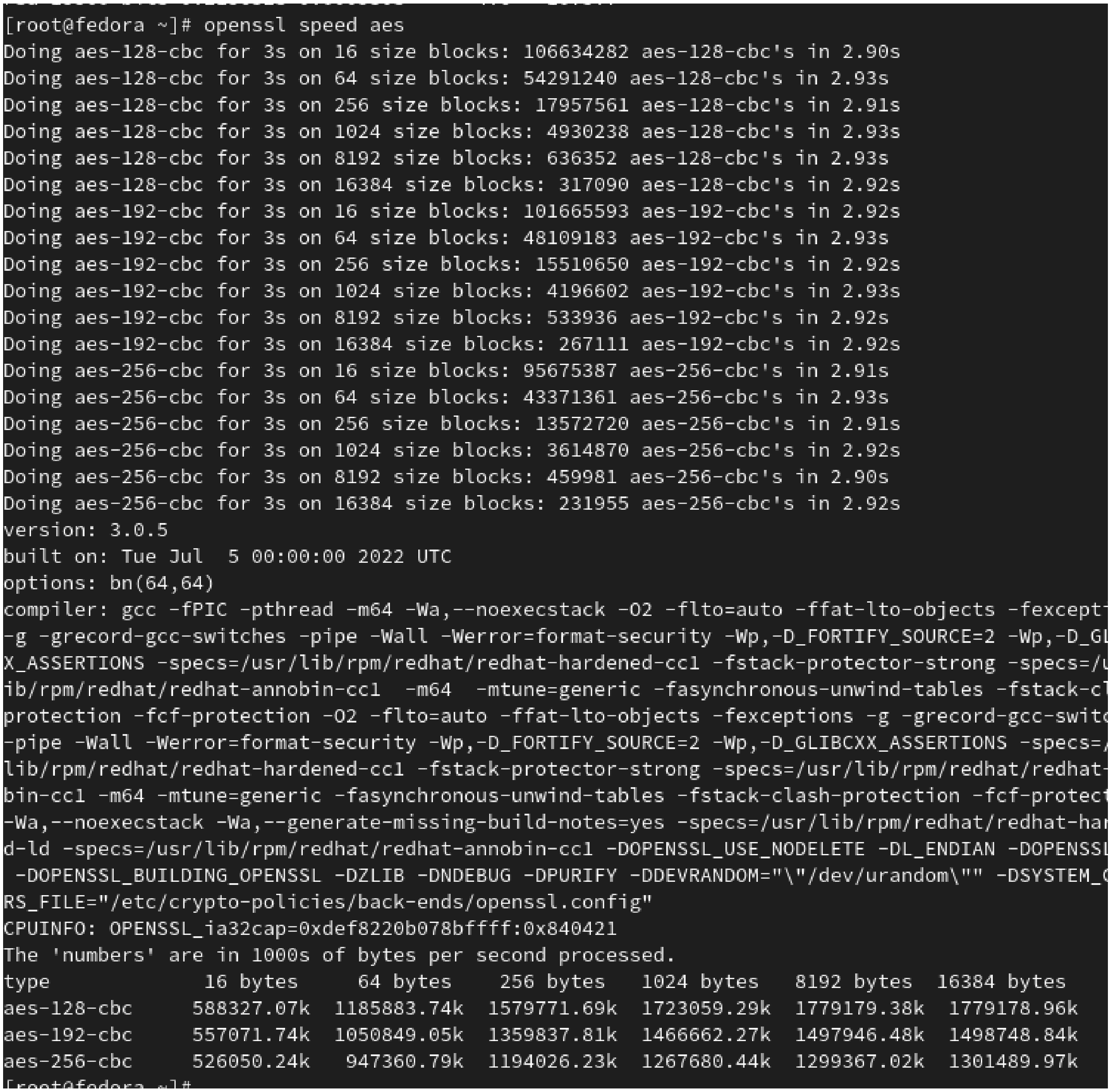
Question 2.1.1:

RSA encryption:



```
Salted__#LiG(��̅ ��1U?�  ¼�X�v���9�DI��.��D���[root@fedora ~]# openssl speed rsa
Doing 512 bits private rsa's for 10s: 376195 512 bits private RSA's in 9.80s
Doing 512 bits public rsa's for 10s: 5132272 512 bits public RSA's in 9.81s
Doing 1024 bits private rsa's for 10s: 119136 1024 bits private RSA's in 9.81s
Doing 1024 bits public rsa's for 10s: 1895017 1024 bits public RSA's in 9.80s
Doing 2048 bits private rsa's for 10s: 24044 2048 bits private RSA's in 9.77s
Doing 2048 bits public rsa's for 10s: 545474 2048 bits public RSA's in 9.79s
Doing 3072 bits private rsa's for 10s: 5064 3072 bits private RSA's in 9.79s
Doing 3072 bits public rsa's for 10s: 248177 3072 bits public RSA's in 9.78s
Doing 4096 bits private rsa's for 10s: 2231 4096 bits private RSA's in 9.81s
Doing 4096 bits public rsa's for 10s: 145335 4096 bits public RSA's in 9.80s
Doing 7680 bits private rsa's for 10s: 259 7680 bits private RSA's in 9.80s
Doing 7680 bits public rsa's for 10s: 41699 7680 bits public RSA's in 9.79s
Doing 15360 bits private rsa's for 10s: 46 15360 bits private RSA's in 9.92s
Doing 15360 bits public rsa's for 10s: 10531 15360 bits public RSA's in 9.79s
version: 3.0.5
built on: Tue Jul  5 00:00:00 2022 UTC
options: bn(64,64)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -O2 -flto=auto -ffat-lto-objects -fexceptio
-g -grecord-gcc-switches -pipe -Wall -Werror=format-security -Wp,-D_FORTIFY_SOURCE=2 -Wp,-D_GLI
X_ASSERTIONS -specs=/usr/lib/rpm/redhat/redhat-hardened-cc1 -fstack-protector-strong -specs=/us
ib/rpm/redhat/redhat-annobin-cc1  -m64  -mtune=generic -fasynchronous-unwind-tables -fstack-cla
protection -fcf-protection -O2 -flto=auto -ffat-lto-objects -fexceptions -g -grecord-gcc-switch
-pipe -Wall -Werror=format-security -Wp,-D_FORTIFY_SOURCE=2 -Wp,-D_GLIBCXX_ASSERTIONS -specs=/u
lib/rpm/redhat/redhat-hardened-cc1 -fstack-protector-strong -specs=/usr/lib/rpm/redhat/redhat-a
bin-cc1 -m64 -mtune=generic -fasynchronous-unwind-tables -fstack-clash-protection -fcf-protecti
-Wa,--noexecstack -Wa,--generate-missing-build-notes=yes -specs=/usr/lib/rpm/redhat/redhat-hard
d-ld -specs=/usr/lib/rpm/redhat/redhat-annobin-cc1 -DOPENSSL_USE_NODELETE -DL_ENDIAN -DOPENSSL_
 -DOPENSSL_BUILDING_OPENSSL -DZLIB -DNDEBUG -DPURIFY -DDEVRANDOM="\"/dev/urandom\"" -DSYSTEM_CI
RS_FILE="/etc/crypto-policies/back-ends/openssl.config"
CPUINFO: OPENSSL_ia32cap=0xdef8220b078bffff:0x840421
                  sign    verify    sign/s verify/s
rsa  512 bits 0.000026s 0.000002s  38387.2 523167.4
rsa 1024 bits 0.000082s 0.000005s  12144.3 193369.1
rsa 2048 bits 0.000406s 0.000018s   2461.0  55717.5
rsa 3072 bits 0.001933s 0.000039s    517.3  25376.0
rsa 4096 bits 0.004397s 0.000067s    227.4  14830.1
rsa 7680 bits 0.037838s 0.000235s     26.4   4259.3
rsa 15360 bits 0.215652s 0.000930s      4.6   1075.7
```

AES encryption:

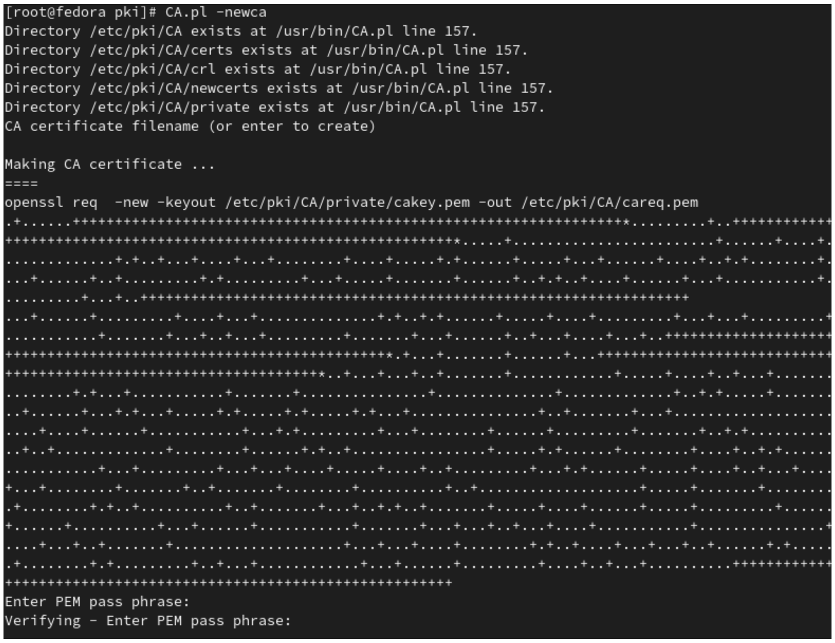


```
[root@fedora ~]# openssl speed aes
Doing aes-128-cbc for 3s on 16 size blocks: 106634282 aes-128-cbc's in 2.90s
Doing aes-128-cbc for 3s on 64 size blocks: 54291240 aes-128-cbc's in 2.93s
Doing aes-128-cbc for 3s on 256 size blocks: 17957561 aes-128-cbc's in 2.91s
Doing aes-128-cbc for 3s on 1024 size blocks: 4930238 aes-128-cbc's in 2.93s
Doing aes-128-cbc for 3s on 8192 size blocks: 636352 aes-128-cbc's in 2.93s
Doing aes-128-cbc for 3s on 16384 size blocks: 317090 aes-128-cbc's in 2.92s
Doing aes-192-cbc for 3s on 16 size blocks: 101665593 aes-192-cbc's in 2.92s
Doing aes-192-cbc for 3s on 64 size blocks: 48109183 aes-192-cbc's in 2.93s
Doing aes-192-cbc for 3s on 256 size blocks: 15510650 aes-192-cbc's in 2.92s
Doing aes-192-cbc for 3s on 1024 size blocks: 4196602 aes-192-cbc's in 2.93s
Doing aes-192-cbc for 3s on 8192 size blocks: 533936 aes-192-cbc's in 2.92s
Doing aes-192-cbc for 3s on 16384 size blocks: 267111 aes-192-cbc's in 2.92s
Doing aes-256-cbc for 3s on 16 size blocks: 95675387 aes-256-cbc's in 2.91s
Doing aes-256-cbc for 3s on 64 size blocks: 43371361 aes-256-cbc's in 2.93s
Doing aes-256-cbc for 3s on 256 size blocks: 13572720 aes-256-cbc's in 2.91s
Doing aes-256-cbc for 3s on 1024 size blocks: 3614870 aes-256-cbc's in 2.92s
Doing aes-256-cbc for 3s on 8192 size blocks: 459981 aes-256-cbc's in 2.90s
Doing aes-256-cbc for 3s on 16384 size blocks: 231955 aes-256-cbc's in 2.92s
version: 3.0.5
built on: Tue Jul  5 00:00:00 2022 UTC
options: bn(64,64)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -O2 -flto=auto -ffat-lto-objects -fexcept
-g -grecord-gcc-switches -pipe -Wall -Werror=format-security -Wp,-D_FORTIFY_SOURCE=2 -Wp,-D_GL
X_ASSERTIONS -specs=/usr/lib/rpm/redhat/redhat-hardened-cc1 -fstack-protector-strong -specs=/u
ib/rpm/redhat/redhat-annobin-cc1  -m64  -mtune=generic -fasynchronous-unwind-tables -fstack-cl
protection -fcf-protection -O2 -flto=auto -ffat-lto-objects -fexceptions -g -grecord-gcc-swit
-pipe -Wall -Werror=format-security -Wp,-D_FORTIFY_SOURCE=2 -Wp,-D_GLIBCXX_ASSERTIONS -specs=/
lib/rpm/redhat/redhat-hardened-cc1 -fstack-protector-strong -specs=/usr/lib/rpm/redhat/redhat-
bin-cc1 -m64 -mtune=generic -fasynchronous-unwind-tables -fstack-clash-protection -fcf-protect
-Wa,--noexecstack -Wa,--generate-missing-build-notes=yes -specs=/usr/lib/rpm/redhat/redhat-har
d-ld -specs=/usr/lib/rpm/redhat/redhat-annobin-cc1 -DOPENSSL_USE_NODELETE -DL_ENDIAN -DOPENSSL
 -DOPENSSL_BUILDING_OPENSSL -DZLIB -DNDEBUG -DPURIFY -DDEVRANDOM="\"/dev/urandom\"" -DSYSTEM_C
RS_FILE="/etc/crypto-policies/back-ends/openssl.config"
CPUINFO: OPENSSL_ia32cap=0xdef8220b078bffff:0x840421
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes  16384 bytes
aes-128-cbc     588327.07k  1185883.74k  1579771.69k  1723059.29k  1779179.38k  1779178.96k
aes-192-cbc     557071.74k  1050849.05k  1359837.81k  1466662.27k  1497946.48k  1498748.84k
aes-256-cbc     526050.24k   947360.79k  1194026.23k  1267680.44k  1299367.02k  1301489.97k
[root@fedora ~]#
```

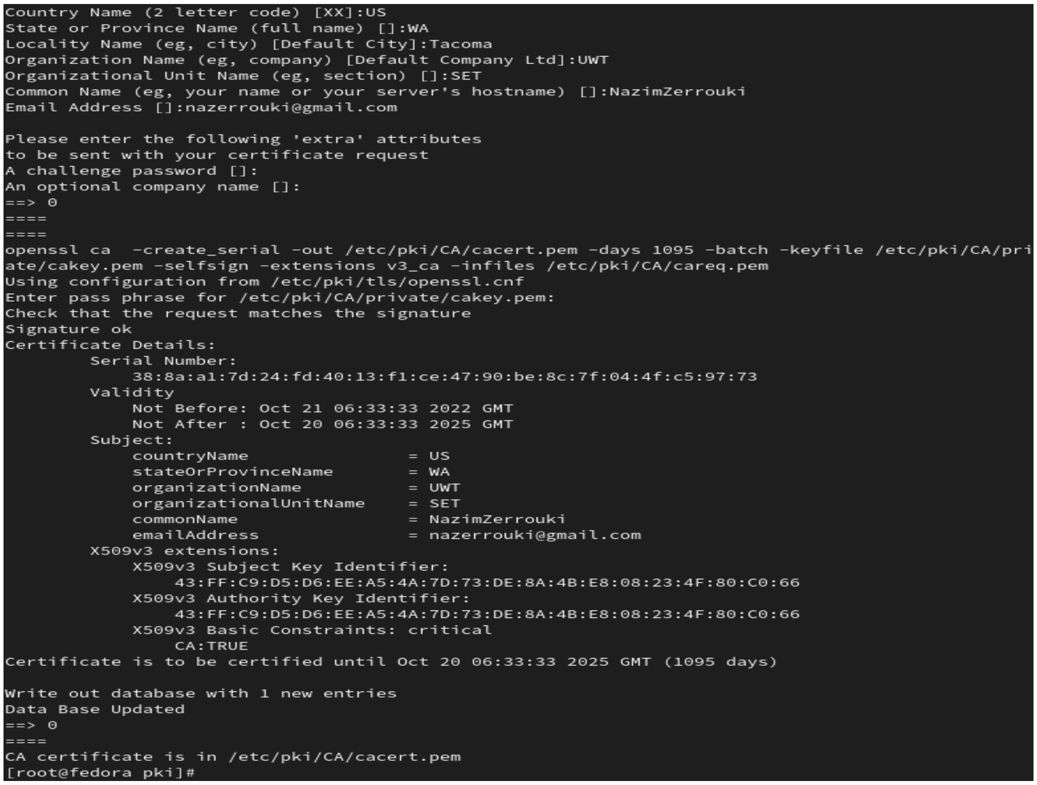
Question 2.1.2:

The results seemed to deviate a fair bit from the time that was projected upon first glance. However, in all actuality, the results were within a 1-3% margin of error where encrypting using both RSA and AES was actually faster than projected. Within statistics, predicting something accurately within a 98% confidence interval is very good so we can presume that these statistics are fairly precise based on that information.

Question 3.1:

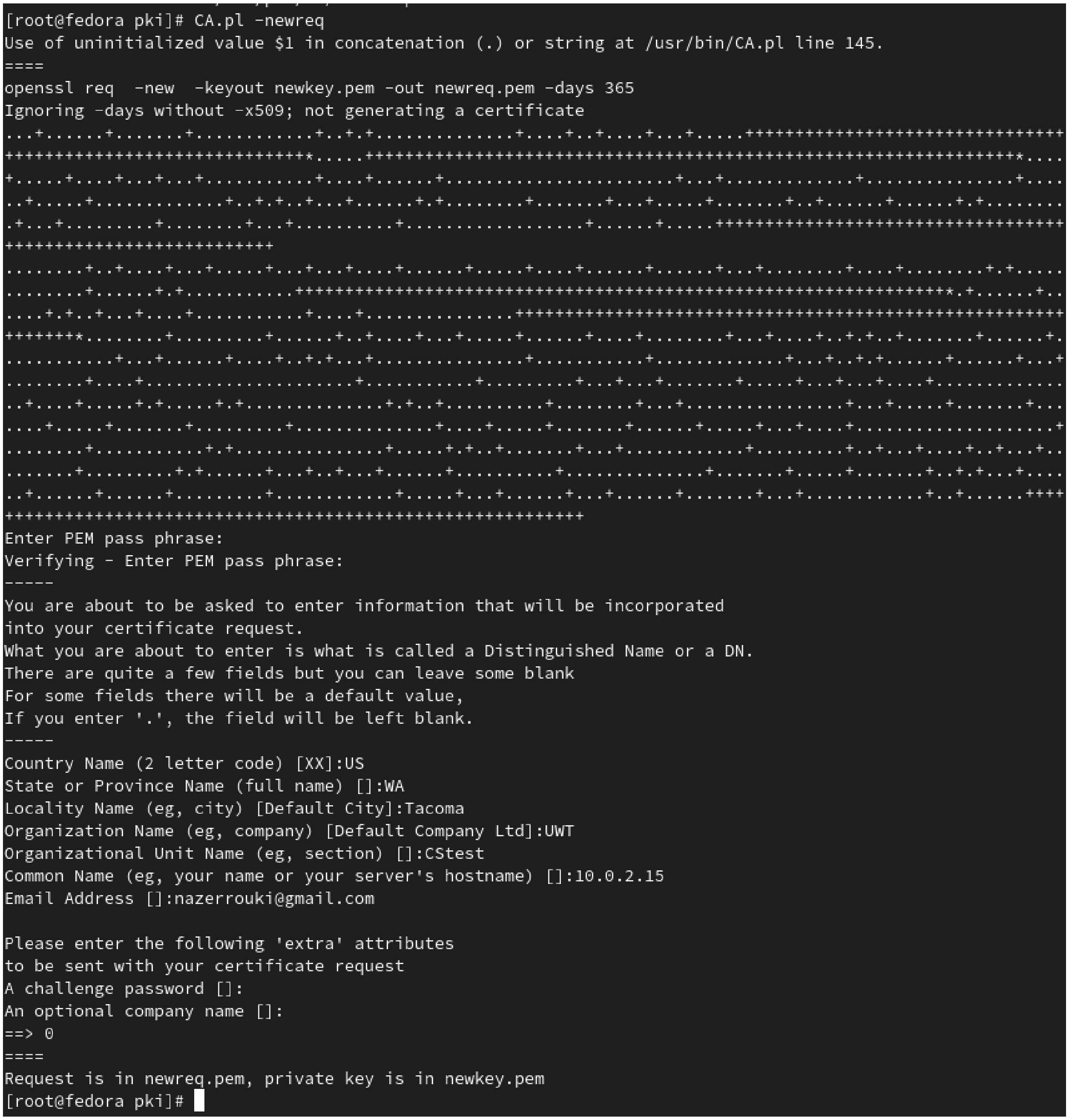


```
[root@fedora pki]# CA.pl -newca
Directory /etc/pki/CA exists at /usr/bin/CA.pl line 157.
Directory /etc/pki/CA/certs exists at /usr/bin/CA.pl line 157.
Directory /etc/pki/CA/crl exists at /usr/bin/CA.pl line 157.
Directory /etc/pki/CA/newcerts exists at /usr/bin/CA.pl line 157.
Directory /etc/pki/CA/private exists at /usr/bin/CA.pl line 157.
CA certificate filename (or enter to create)

Making CA certificate ...
====
openssl req  -new -keyout /etc/pki/CA/private/cakey.pem -out /etc/pki/CA/careq.pem
.+......+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*........+..+++++++++++
+++++++++++++++++++++++++++++++++++++++++++++++++++++*.....+.......................+......+....+.
............+.+..+...+....+...+........+....+.....+.+......+.....+...+......+....+..+.+.......+.
...+......+..+.........+.+.........+...+.....+.......+......+..+.+..+....+......+...+..........+.
.........+...+..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
...+......+.........+....+...+.............+.+..+.+......+.....+....+.........+...+...+.........+
..........+.......+...+..+...+.........+.......+...+......+..+...+....+...+..++++++++++++++++++++
+++++++++++++++++++++++++++++++++++++++++++++++*.+...+......+......+...++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++++++*..+...+...+..+.......+............+.....+....+..+...+.....
.......+.+...+..........+.......+...............+..............+.............+..+.+.....+.......
..+......+...+.+...+.....+.+.....+.+.....+.+...+...............+..+.......+...+..................
....+....+......+...........+...+.+.........+...+........+......+.........+.......+..+.+.........
..+..+............+........+......+.+..+...............+.....+.+......+........+....+..+.+.....
..........+...+.........+...+...+....+.....+....+..+.........+...+.+......+.....+....+..+...+....
+...+........+.......+..+.......+........+..........+..+..................+.....+.......+.......
.+........+.+..+..........+..+.......+...+..+.+..+.......+.....+....+......+.....+.........+.....
+......+..........+...+......+...........+.......+...+...+..+...+....+...........+..............+
....+...+..+.......+..................+...+...+....+........+.+..+....+...+...+..+.....+.+.....
.+........+.+.........+..+...+...........+...+......+.........+....+..+...+..........++++++++++++
+++++++++++++++++++++++++++++++++++++++++++++++++++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```



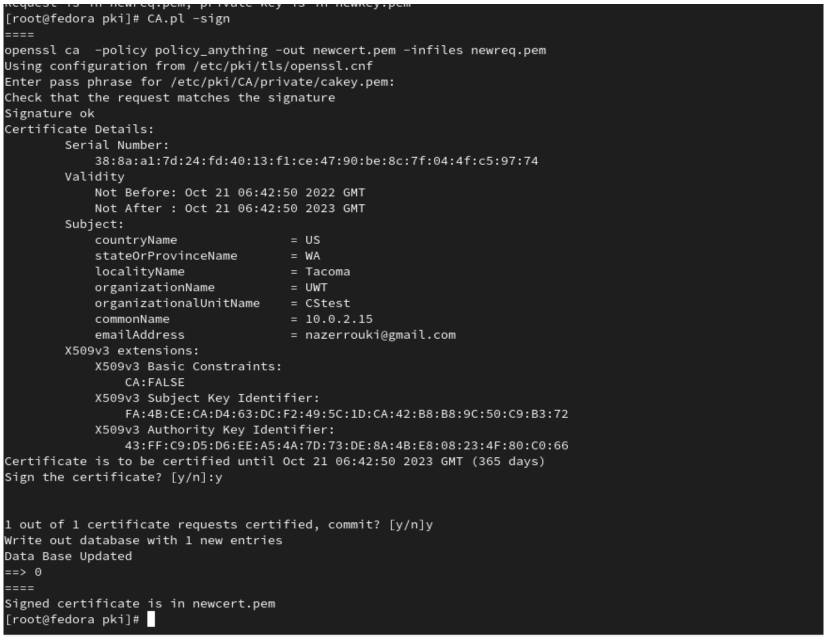
```
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:WA
Locality Name (eg, city) [Default City]:Tacoma
Organization Name (eg, company) [Default Company Ltd]:UWT
Organizational Unit Name (eg, section) []:SET
Common Name (eg, your name or your server's hostname) []:NazimZerrouki
Email Address []:nazerrouki@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
==> 0
====
====
openssl ca  -create_serial -out /etc/pki/CA/cacert.pem -days 1095 -batch -keyfile /etc/pki/CA/pri
ate/cakey.pem -selfsign -extensions v3_ca -infiles /etc/pki/CA/careq.pem
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for /etc/pki/CA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            38:8a:a1:7d:24:fd:40:13:f1:ce:47:90:be:8c:7f:04:4f:c5:97:73
        Validity
            Not Before: Oct 21 06:33:33 2022 GMT
            Not After : Oct 20 06:33:33 2025 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = WA
            organizationName          = UWT
            organizationalUnitName    = SET
            commonName                = NazimZerrouki
            emailAddress              = nazerrouki@gmail.com
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                43:FF:C9:D5:D6:EE:A5:4A:7D:73:DE:8A:4B:E8:08:23:4F:80:C0:66
            X509v3 Authority Key Identifier:
                43:FF:C9:D5:D6:EE:A5:4A:7D:73:DE:8A:4B:E8:08:23:4F:80:C0:66
            X509v3 Basic Constraints: critical
                CA:TRUE
Certificate is to be certified until Oct 20 06:33:33 2025 GMT (1095 days)

Write out database with 1 new entries
Data Base Updated
==> 0
====
CA certificate is in /etc/pki/CA/cacert.pem
[root@fedora pki]#
```

Question 3.2:



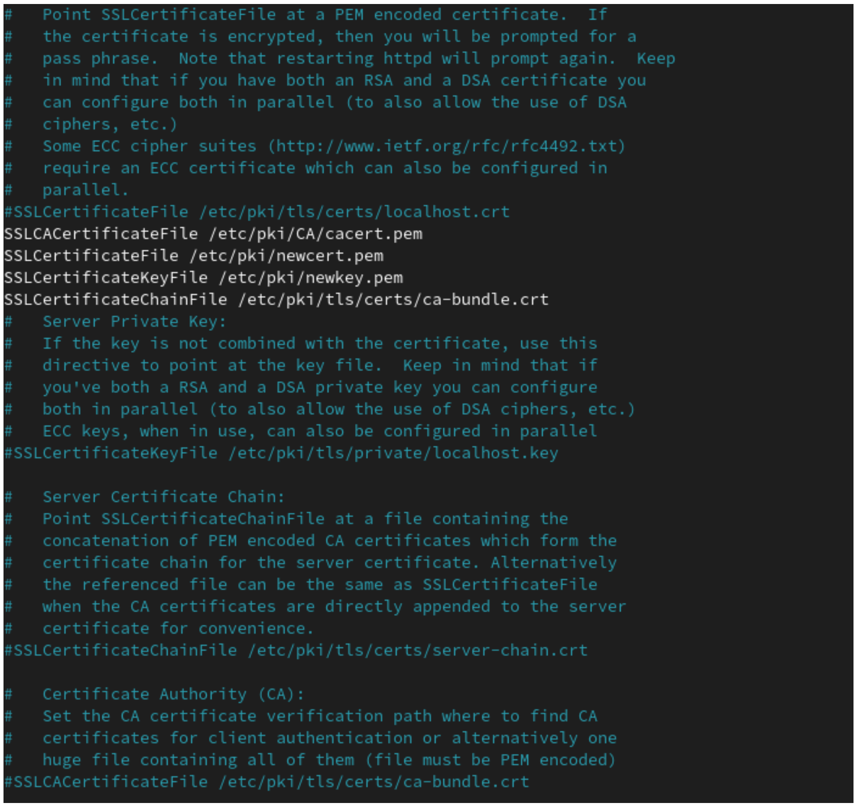
```
[root@fedora pki]# CA.pl -newreq
Use of uninitialized value $1 in concatenation (.) or string at /usr/bin/CA.pl line 145.
====
openssl req  -new  -keyout newkey.pem -out newreq.pem -days 365
Ignoring -days without -x509; not generating a certificate
...+......+......+..........+..+.+............+....+..+....+...+.....+++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++*.....++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*....
+.....+....+...+...+..........+....+......+......................+...+............+..............+....
..+.....+............+..+.+..+...+......+.+........+.......+...+.....+.......+..+......+......+.+.......
.+...+.........+........+...+..........+.................+......+.....++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++
........+..+....+...+.....+...+...+....+......+.....+....+......+......+...+........+....+........+.+.....
........+......+.+..........+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+......+..
....+.+..+...+....+..........+....+..............++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++*........+.........+......+..+....+...+.....+......+....+........+...+....+..+.+..+.......+......+.
...........+...+......+....+..+.+...+...............+..........+.............+...+..+.+......+......+...+
........+....+.....................+..........+.........+...+...+.......+.....+...+...+....+...........
..+....+.....+.+.....+.+.............+.+..+.........+........+...+...............+...+.....+.......+...
....+.....+.......+.........+.............+....+.....+.......+......+.....+...+....+...................+
........+..........+.+..............+.....+.+..+.......+...+............+.........+..+...+....+..+...+..
.......+.........+.+......+...+..+...+......+..........+.............+.......+.....+.......+..+.+...+....
..+......+......+........+...........+.....+...+......+...+......+.......+...+...........+..+......++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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) [XX]:US
State or Province Name (full name) []:WA
Locality Name (eg, city) [Default City]:Tacoma
Organization Name (eg, company) [Default Company Ltd]:UWT
Organizational Unit Name (eg, section) []:CStest
Common Name (eg, your name or your server's hostname) []:10.0.2.15
Email Address []:nazerrouki@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
==> 0
====
Request is in newreq.pem, private key is in newkey.pem
[root@fedora pki]#
```

Question 3.3:

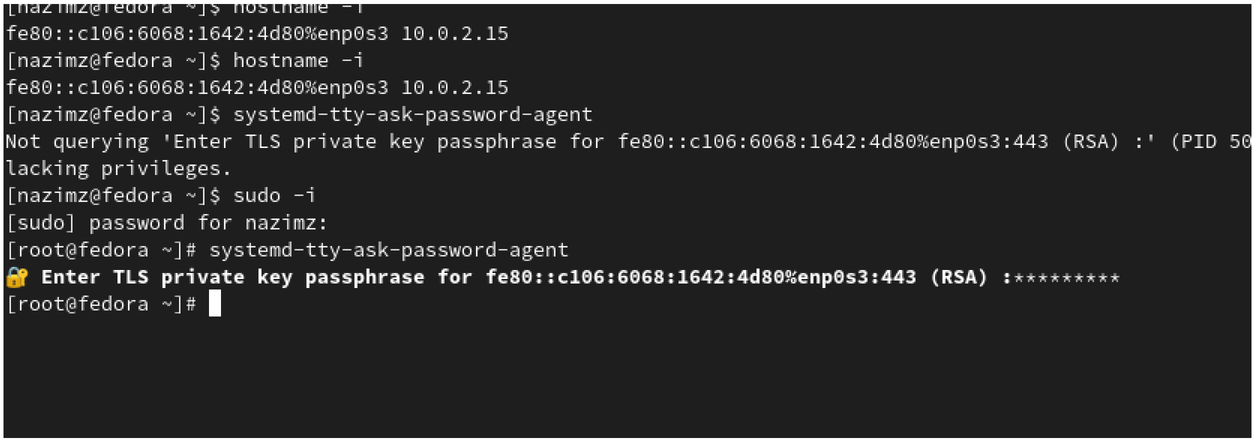


```
Request is in newreq.pem, private key is in newkey.pem
[root@fedora pki]# CA.pl -sign
====
openssl ca  -policy policy_anything -out newcert.pem -infiles newreq.pem
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for /etc/pki/CA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            38:8a:a1:7d:24:fd:40:13:f1:ce:47:90:be:8c:7f:04:4f:c5:97:74
        Validity
            Not Before: Oct 21 06:42:50 2022 GMT
            Not After : Oct 21 06:42:50 2023 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = WA
            localityName              = Tacoma
            organizationName          = UWT
            organizationalUnitName    = CStest
            commonName                = 10.0.2.15
            emailAddress              = nazerrouki@gmail.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                FA:4B:CE:CA:D4:63:DC:F2:49:5C:1D:CA:42:B8:B8:9C:50:C9:B3:72
            X509v3 Authority Key Identifier:
                43:FF:C9:D5:D6:EE:A5:4A:7D:73:DE:8A:4B:E8:08:23:4F:80:C0:66
Certificate is to be certified until Oct 21 06:42:50 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
==> 0
====
Signed certificate is in newcert.pem
[root@fedora pki]# 
```

Question 4.1:



```
#   Point SSLCertificateFile at a PEM encoded certificate.  If
#   the certificate is encrypted, then you will be prompted for a
#   pass phrase.  Note that restarting httpd will prompt again.  Keep
#   in mind that if you have both an RSA and a DSA certificate you
#   can configure both in parallel (to also allow the use of DSA
#   ciphers, etc.)
#   Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)
#   require an ECC certificate which can also be configured in
#   parallel.
#SSLCertificateFile /etc/pki/tls/certs/localhost.crt
SSLCACertificateFile /etc/pki/CA/cacert.pem
SSLCertificateFile /etc/pki/newcert.pem
SSLCertificateKeyFile /etc/pki/newkey.pem
SSLCertificateChainFile /etc/pki/tls/certs/ca-bundle.crt
#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
#   ECC keys, when in use, can also be configured in parallel
#SSLCertificateKeyFile /etc/pki/tls/private/localhost.key

#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
#   concatenation of PEM encoded CA certificates which form the
#   certificate chain for the server certificate. Alternatively
#   the referenced file can be the same as SSLCertificateFile
#   when the CA certificates are directly appended to the server
#   certificate for convenience.
#SSLCertificateChainFile /etc/pki/tls/certs/server-chain.crt

#   Certificate Authority (CA):
#   Set the CA certificate verification path where to find CA
#   certificates for client authentication or alternatively one
#   huge file containing all of them (file must be PEM encoded)
#SSLCACertificateFile /etc/pki/tls/certs/ca-bundle.crt
```

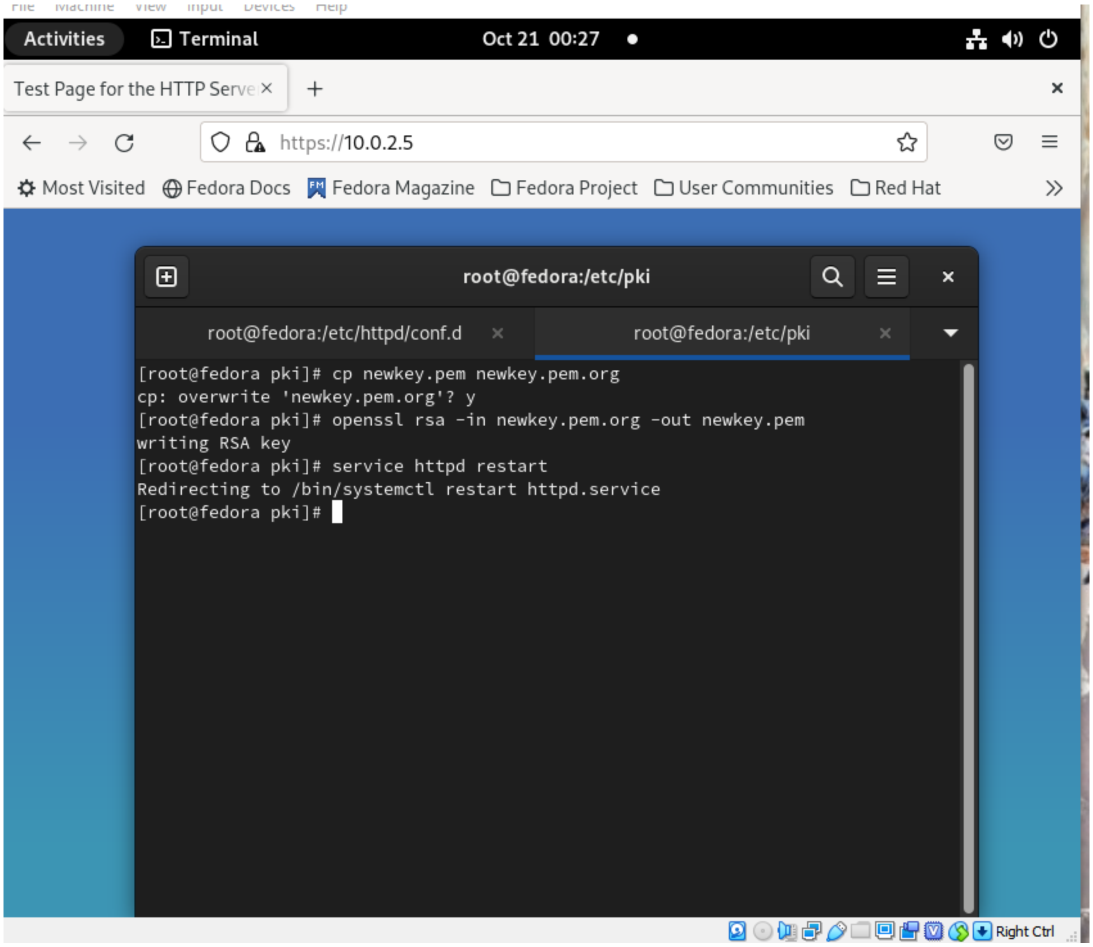


```
[nazimz@fedora ~]$ hostname -i
fe80::c106:6068:1642:4d80%enp0s3 10.0.2.15
[nazimz@fedora ~]$ hostname -i
fe80::c106:6068:1642:4d80%enp0s3 10.0.2.15
[nazimz@fedora ~]$ systemd-tty-ask-password-agent
Not querying 'Enter TLS private key passphrase for fe80::c106:6068:1642:4d80%enp0s3:443 (RSA) :' (PID 50
lacking privileges.
[nazimz@fedora ~]$ sudo -i
[sudo] password for nazimz:
[root@fedora ~]# systemd-tty-ask-password-agent
🔐 Enter TLS private key passphrase for fe80::c106:6068:1642:4d80%enp0s3:443 (RSA) :*********
[root@fedora ~]# █
```

I was asked to provide the password key phrase for the private key.

Question 4.2:

Connection to server:



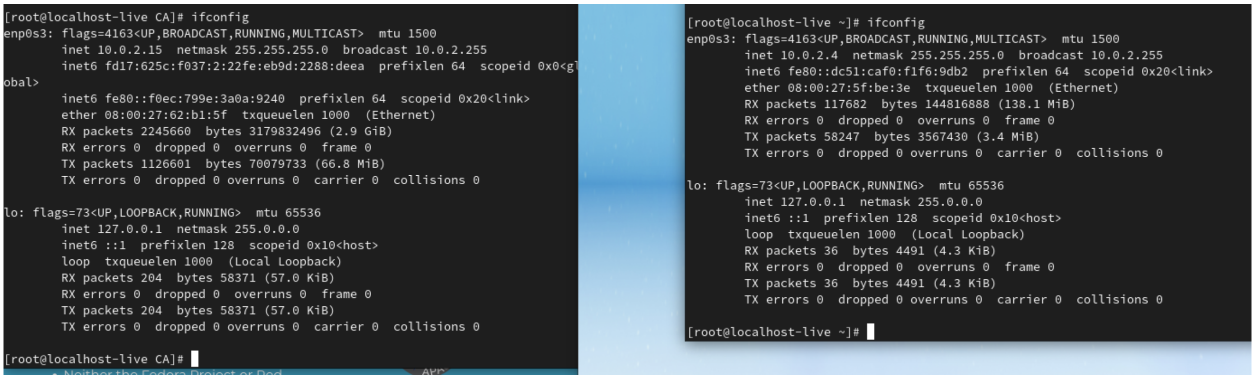
```
[root@fedora pki]# cp newkey.pem newkey.pem.org
cp: overwrite 'newkey.pem.org'? y
[root@fedora pki]# openssl rsa -in newkey.pem.org -out newkey.pem
writing RSA key
[root@fedora pki]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@fedora pki]# █
```

Inputting the aforementioned command complety bypassed the passkeyphrase prompt altogether.

Question 5:

Client-Server setup:

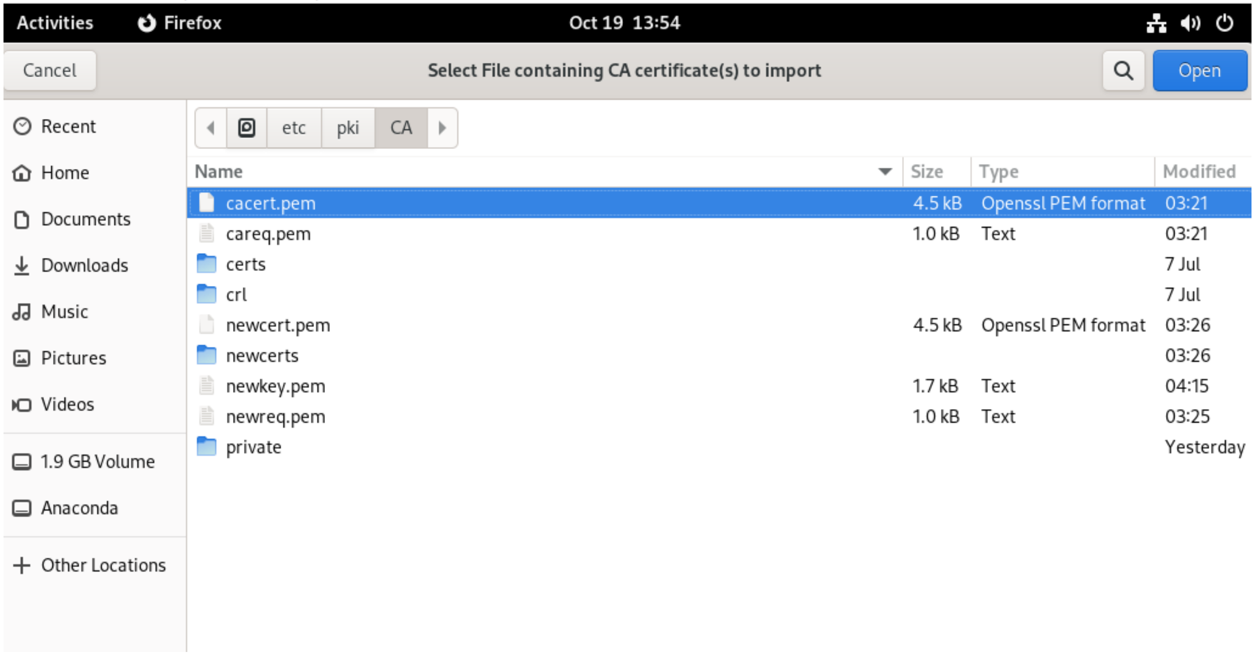
To set-up a connection between the server VM used for this project thus far and a client VM, I established an NAT Network within the Host VM i.e Oracle Virtualbox. From there, I had both VMs connect to the NAT Network and granted them access to all VMs. The end-result led to 2 VMs which had two separate IP addresses. The VM on the left is the server with an IP address of 10.0.2.15. The VM on the right is the client with an IP address of 10.0.2.4. As you can see, a client and server connection was successfully established. Now both need to install the certificate authority that we created thus far.



```
[root@localhost-live CA]# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fd17:625c:f037:2:22fe:eb9d:2288:deea  prefixlen 64  scopeid 0x0<gl
obal>
        inet6 fe80::f0ec:799e:3a0a:9240  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:62:b1:5f  txqueuelen 1000  (Ethernet)
        RX packets 2245660  bytes 3179832496 (2.9 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1126601  bytes 70079733 (66.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 204  bytes 58371 (57.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 204  bytes 58371 (57.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost-live CA]# 
```

```
[root@localhost-live ~]# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::dc51:caf0:f1f6:9db2  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5f:be:3e  txqueuelen 1000  (Ethernet)
        RX packets 117682  bytes 144816888 (138.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 58247  bytes 3567430 (3.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 36  bytes 4491 (4.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 36  bytes 4491 (4.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost-live ~]# 
```

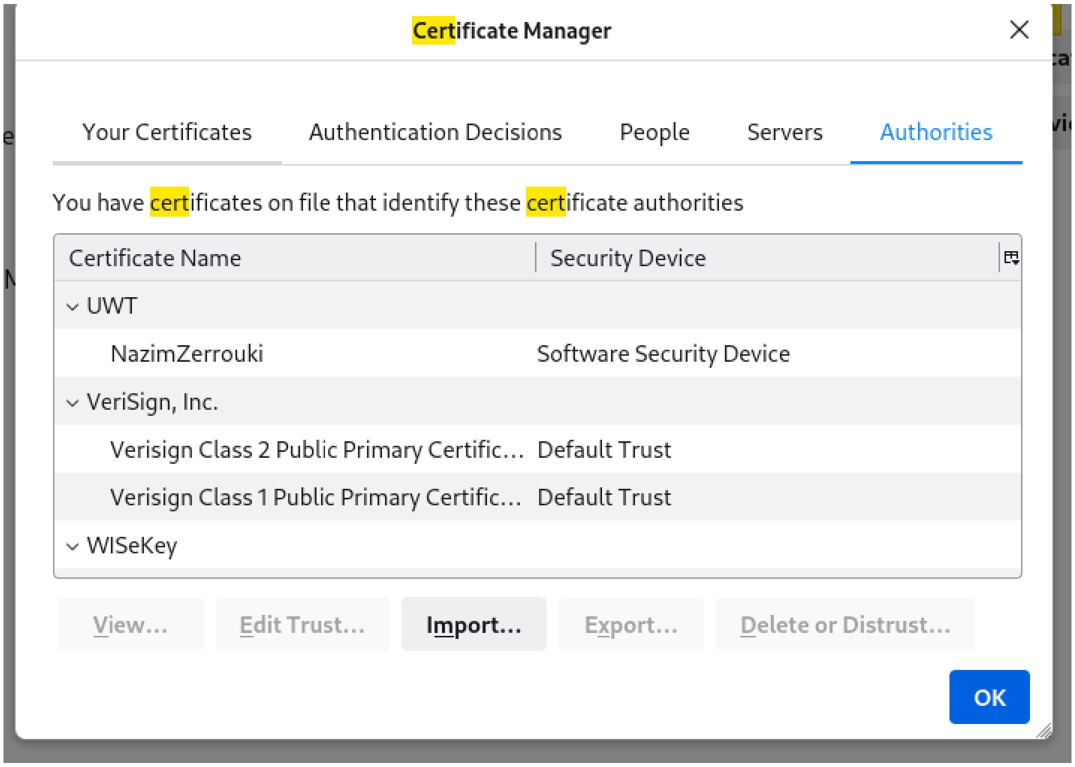
Question 5.1:



Select File containing CA certificate(s) to import

Name	Size	Type	Modified
cacert.pem	4.5 kB	Openssl PEM format	03:21
careq.pem	1.0 kB	Text	03:21
certs			7 Jul
crl			7 Jul
newcert.pem	4.5 kB	Openssl PEM format	03:26
newcerts			03:26
newkey.pem	1.7 kB	Text	04:15
newreq.pem	1.0 kB	Text	03:25
private			Yesterday

I didn’t receive a warning message because the installation of the root certificate authority was successful for the server VM as you can see here:

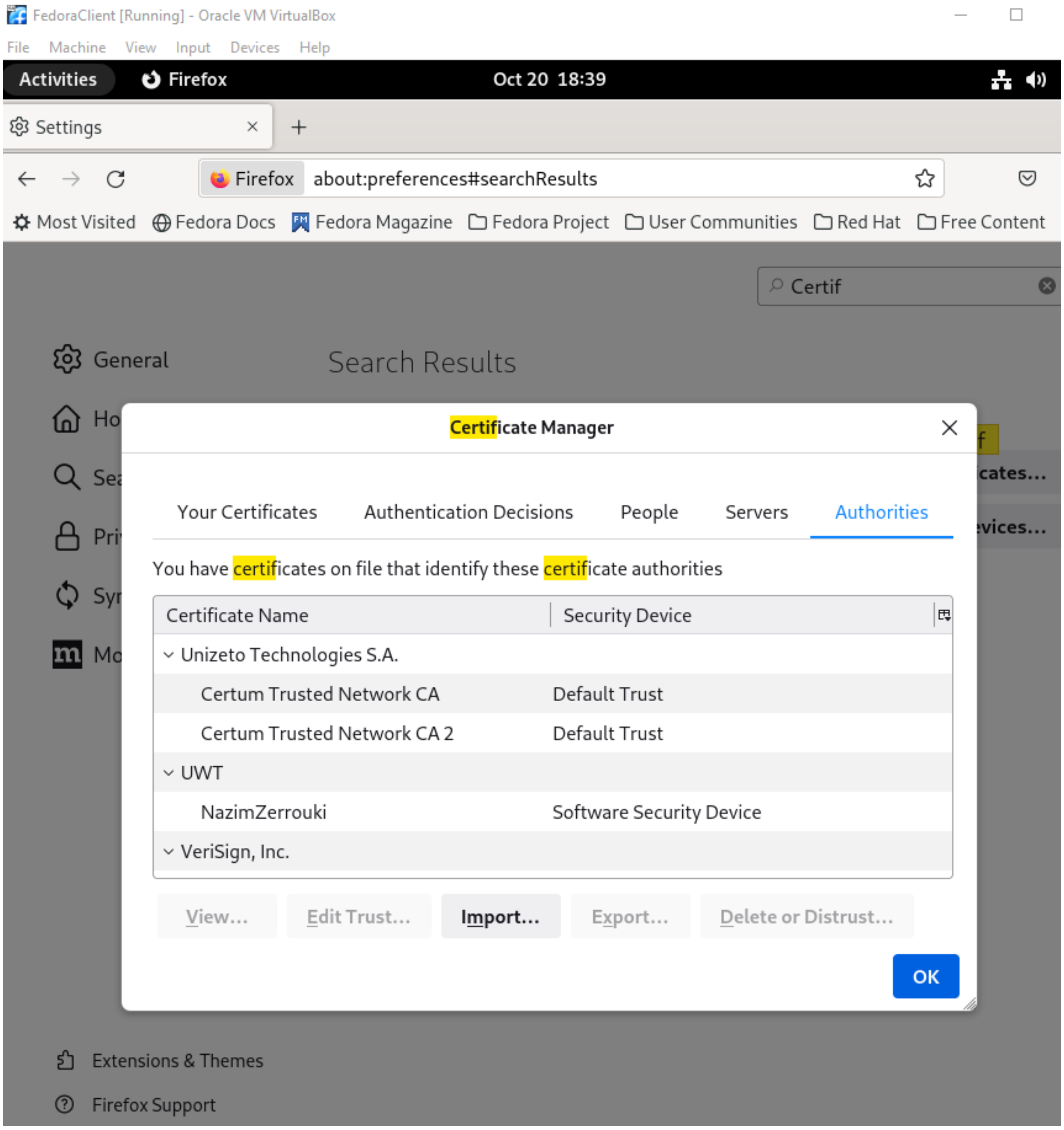


You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
UWT	
NazimZerrouki	Software Security Device
VeriSign, Inc.	
Verisign Class 2 Public Primary Certific…	Default Trust
Verisign Class 1 Public Primary Certific…	Default Trust
WISeKey	

Question 5.2:

The same process was repeated for the Client VM.

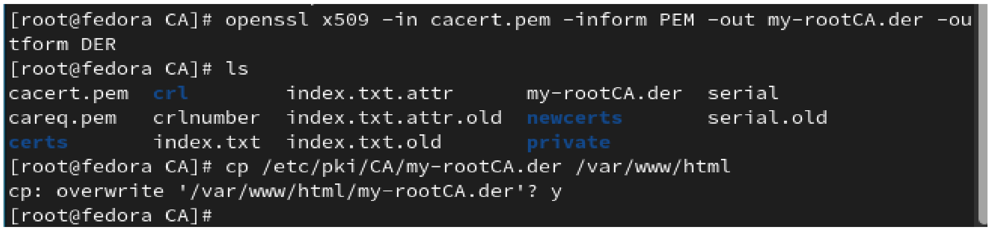


You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
Unizeto Technologies S.A.	
Certum Trusted Network CA	Default Trust
Certum Trusted Network CA 2	Default Trust
UWT	
NazimZerrouki	Software Security Device
VeriSign, Inc.	

Question 5.3:

To access the file, it must be copied in the /var/www/html directory so it can be viewed on the apache server.



```
[root@fedora CA]# openssl x509 -in cacert.pem -inform PEM -out my-rootCA.der -ou
tform DER
[root@fedora CA]# ls
cacert.pem  crl         index.txt.attr      my-rootCA.der  serial
careq.pem   crlnumber   index.txt.attr.old  newcerts       serial.old
certs       index.txt   index.txt.old       private
[root@fedora CA]# cp /etc/pki/CA/my-rootCA.der /var/www/html
cp: overwrite '/var/www/html/my-rootCA.der'? y
[root@fedora CA]#
```

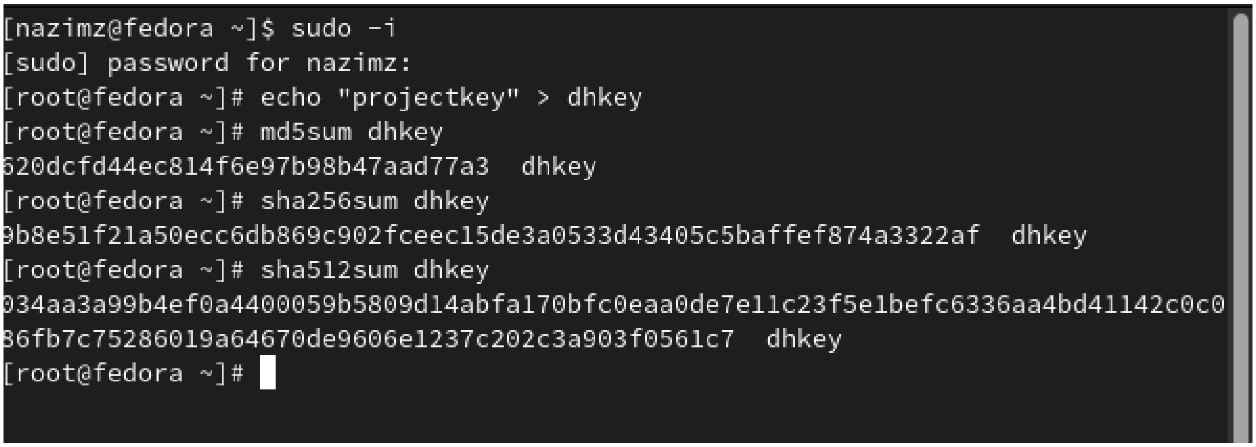
Or you can ssh from your Windows machine into your Linux machine to download the files via PuTTy which is an SSH client.

Question 5.4:

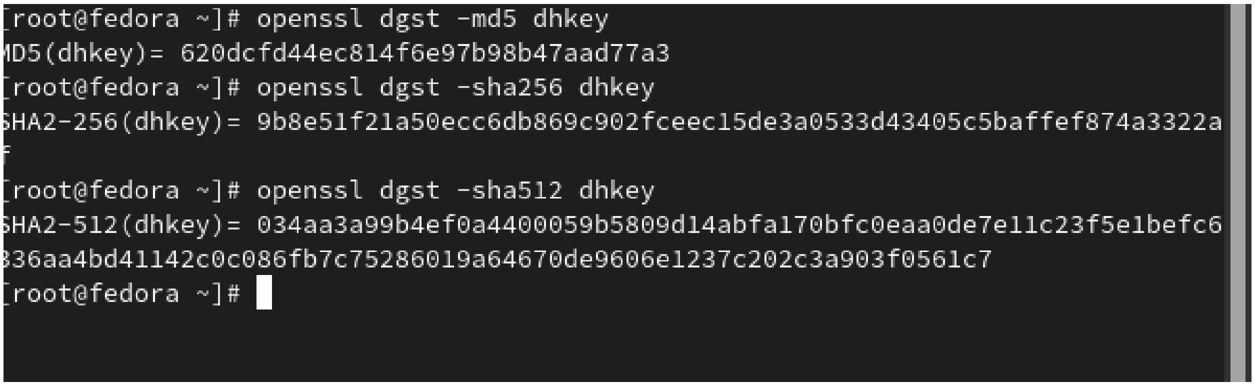
Unfortunately, I have not resolved the issue yet but plan on discussing with my group member on how to address it.

Question 6.1.1:

One-Way Hash Functions (Original):

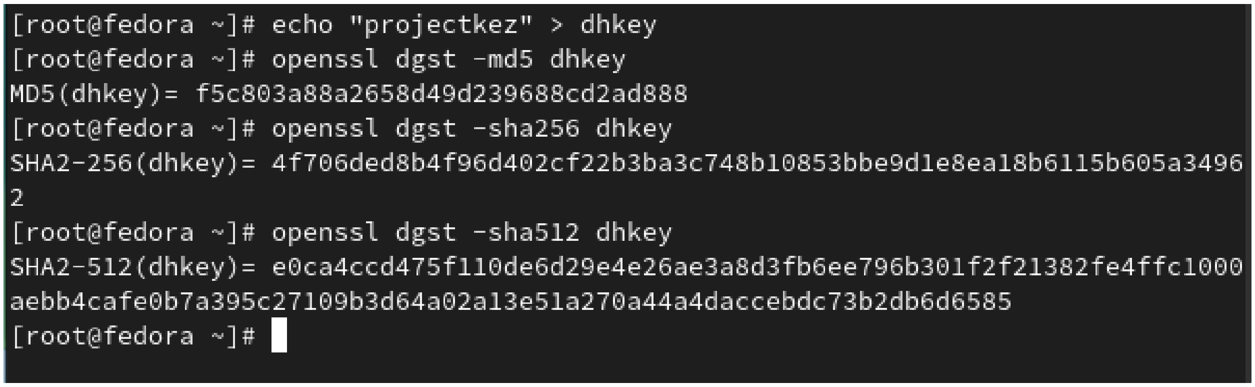


```
[nazimz@fedora ~]$ sudo -i
[sudo] password for nazimz:
[root@fedora ~]# echo "projectkey" > dhkey
[root@fedora ~]# md5sum dhkey
620dcfd44ec814f6e97b98b47aad77a3  dhkey
[root@fedora ~]# sha256sum dhkey
9b8e51f21a50ecc6db869c902fceec15de3a0533d43405c5baffef874a3322af  dhkey
[root@fedora ~]# sha512sum dhkey
034aa3a99b4ef0a4400059b5809d14abfa170bfc0eaa0de7e11c23f5e1befc6336aa4bd41142c0c0
86fb7c75286019a64670de9606e1237c202c3a903f0561c7  dhkey
[root@fedora ~]# 
```



```
[root@fedora ~]# openssl dgst -md5 dhkey
MD5(dhkey)= 620dcfd44ec814f6e97b98b47aad77a3
[root@fedora ~]# openssl dgst -sha256 dhkey
SHA2-256(dhkey)= 9b8e51f21a50ecc6db869c902fceec15de3a0533d43405c5baffef874a3322a
f
[root@fedora ~]# openssl dgst -sha512 dhkey
SHA2-512(dhkey)= 034aa3a99b4ef0a4400059b5809d14abfa170bfc0eaa0de7e11c23f5e1befc6
836aa4bd41142c0c086fb7c75286019a64670de9606e1237c202c3a903f0561c7
[root@fedora ~]#
```

One-Way Hash Functions (Altered):

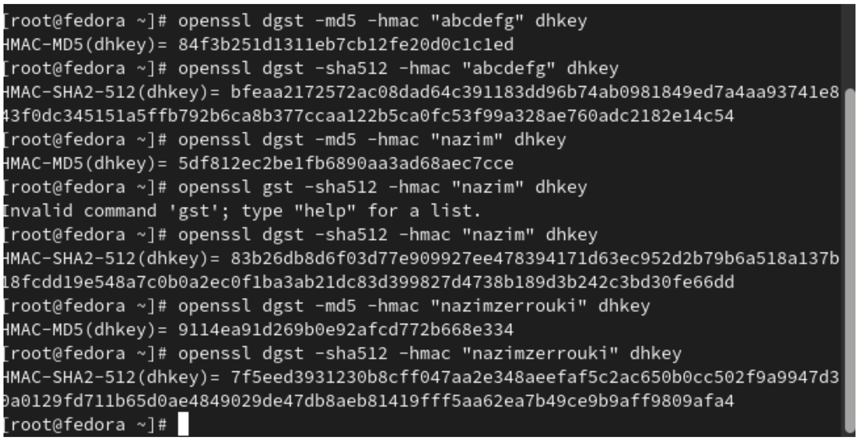


```
[root@fedora ~]# echo "projectkez" > dhkey
[root@fedora ~]# openssl dgst -md5 dhkey
MD5(dhkey)= f5c803a88a2658d49d239688cd2ad888
[root@fedora ~]# openssl dgst -sha256 dhkey
SHA2-256(dhkey)= 4f706ded8b4f96d402cf22b3ba3c748b10853bbe9d1e8ea18b6115b605a3496
2
[root@fedora ~]# openssl dgst -sha512 dhkey
SHA2-512(dhkey)= e0ca4ccd475f110de6d29e4e26ae3a8d3fb6ee796b301f2f21382fe4ffc1000
aebb4cafe0b7a395c27109b3d64a02a13e51a270a44a4daccebdc73b2db6d6585
[root@fedora ~]#
```

Just by altering the last letter in the original file, you can see that each one-way hash function generated drastically different hash values compared to the original file.

<u>Question 6.2.1:</u>

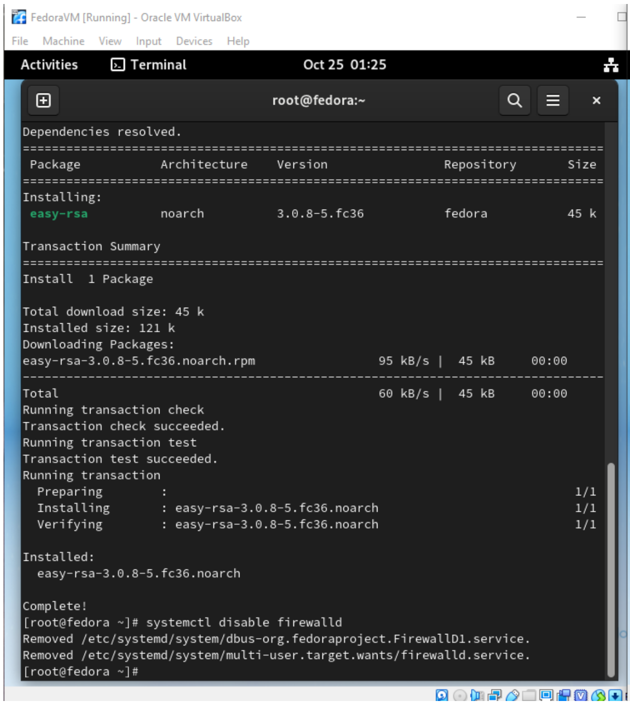
Based on the results, changing key size does not matter. The hash functions still create hash values of the same length. It seems only altering the original file is relevant.



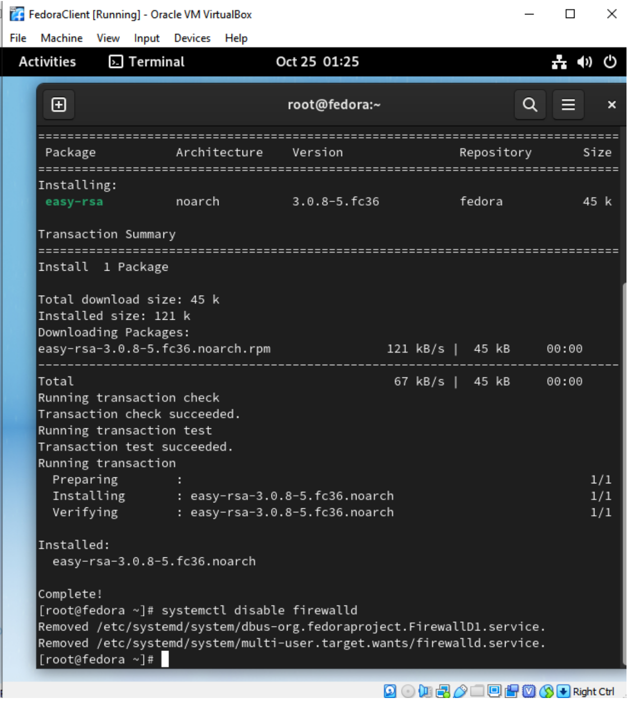
```
[root@fedora ~]# openssl dgst -md5 -hmac "abcdefg" dhkey
HMAC-MD5(dhkey)= 84f3b251d1311eb7cb12fe20d0c1c1ed
[root@fedora ~]# openssl dgst -sha512 -hmac "abcdefg" dhkey
HMAC-SHA2-512(dhkey)= bfeaa2172572ac08dad64c391183dd96b74ab0981849ed7a4aa93741e8
43f0dc345151a5ffb792b6ca8b377ccaa122b5ca0fc53f99a328ae760adc2182e14c54
[root@fedora ~]# openssl dgst -md5 -hmac "nazim" dhkey
HMAC-MD5(dhkey)= 5df812ec2be1fb6890aa3ad68aec7cce
[root@fedora ~]# openssl gst -sha512 -hmac "nazim" dhkey
Invalid command 'gst'; type "help" for a list.
[root@fedora ~]# openssl dgst -sha512 -hmac "nazim" dhkey
HMAC-SHA2-512(dhkey)= 83b26db8d6f03d77e909927ee478394171d63ec952d2b79b6a518a137b
18fcdd19e548a7c0b0a2ec0f1ba3ab21dc83d399827d4738b189d3b242c3bd30fe66dd
[root@fedora ~]# openssl dgst -md5 -hmac "nazimzerrouki" dhkey
HMAC-MD5(dhkey)= 9114ea91d269b0e92afcd772b668e334
[root@fedora ~]# openssl dgst -sha512 -hmac "nazimzerrouki" dhkey
HMAC-SHA2-512(dhkey)= 7f5eed3931230b8cff047aa2e348aeefaf5c2ac650b0cc502f9a9947d3
0a0129fd711b65d0ae4849029de47db8aeb81419fff5aa62ea7b49ce9b9aff9809afa4
[root@fedora ~]#
```

Question 7:

Lab SetUp on Server & Client:


FedoraVM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 25 01:25
root@fedora:~

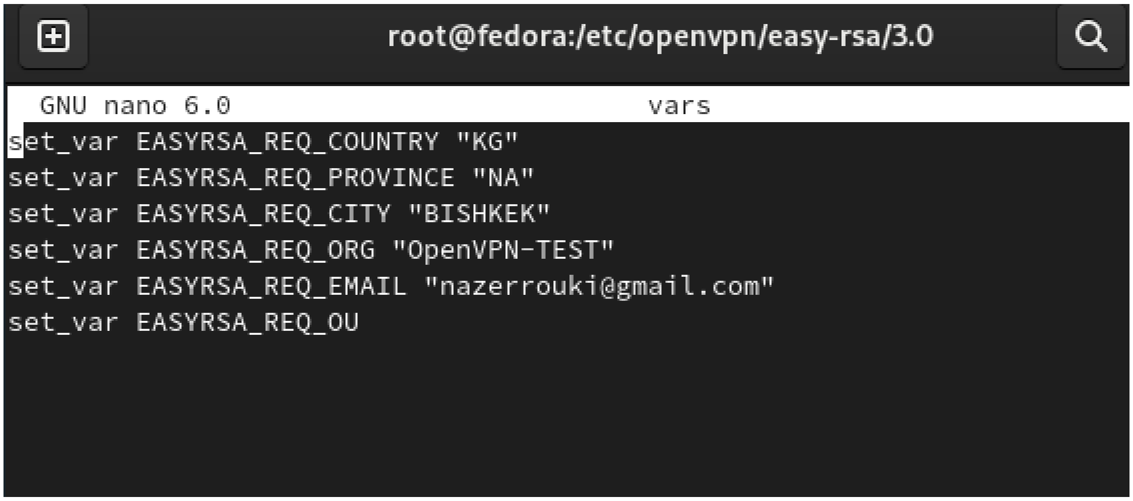
```
Dependencies resolved.
================================================================================
 Package           Architecture    Version                 Repository      Size
================================================================================
Installing:
 easy-rsa          noarch          3.0.8-5.fc36            fedora          45 k

Transaction Summary
================================================================================
Install  1 Package

Total download size: 45 k
Installed size: 121 k
Downloading Packages:
easy-rsa-3.0.8-5.fc36.noarch.rpm                 95 kB/s |  45 kB     00:00
--------------------------------------------------------------------------------
Total                                            60 kB/s |  45 kB     00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1
  Installing       : easy-rsa-3.0.8-5.fc36.noarch                           1/1
  Verifying        : easy-rsa-3.0.8-5.fc36.noarch                           1/1

Installed:
  easy-rsa-3.0.8-5.fc36.noarch

Complete!
[root@fedora ~]# systemctl disable firewalld
Removed /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
Removed /etc/systemd/system/multi-user.target.wants/firewalld.service.
[root@fedora ~]#
```


FedoraClient [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Oct 25 01:25
root@fedora:~
Right Ctrl

```
================================================================================
 Package           Architecture    Version                 Repository      Size
================================================================================
Installing:
 easy-rsa          noarch          3.0.8-5.fc36            fedora          45 k

Transaction Summary
================================================================================
Install  1 Package

Total download size: 45 k
Installed size: 121 k
Downloading Packages:
easy-rsa-3.0.8-5.fc36.noarch.rpm                121 kB/s |  45 kB     00:00
--------------------------------------------------------------------------------
Total                                            67 kB/s |  45 kB     00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1
  Installing       : easy-rsa-3.0.8-5.fc36.noarch                           1/1
  Verifying        : easy-rsa-3.0.8-5.fc36.noarch                           1/1

Installed:
  easy-rsa-3.0.8-5.fc36.noarch

Complete!
[root@fedora ~]# systemctl disable firewalld
Removed /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
Removed /etc/systemd/system/multi-user.target.wants/firewalld.service.
[root@fedora ~]#
```

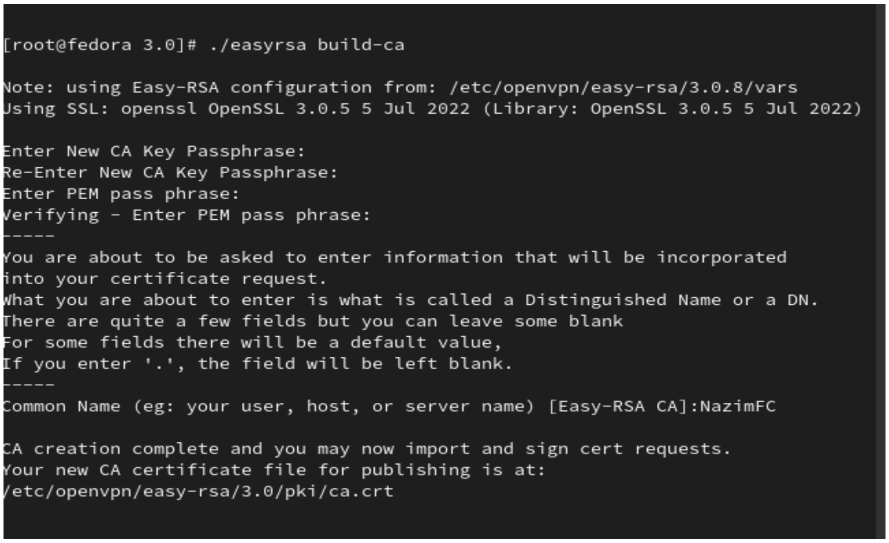
Question 7.1:

Vars file:



```
  GNU nano 6.0                          vars
set_var EASYRSA_REQ_COUNTRY "KG"
set_var EASYRSA_REQ_PROVINCE "NA"
set_var EASYRSA_REQ_CITY "BISHKEK"
set_var EASYRSA_REQ_ORG "OpenVPN-TEST"
set_var EASYRSA_REQ_EMAIL "nazerrouki@gmail.com"
set_var EASYRSA_REQ_OU
```

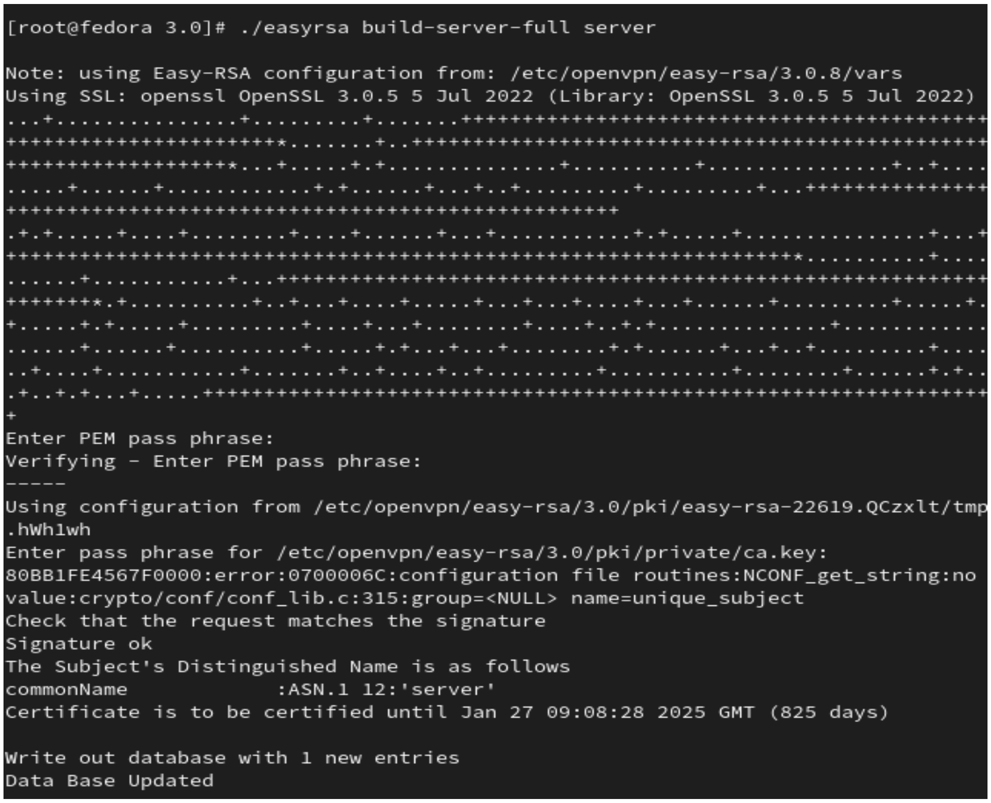
Certificate Authority:



```
[root@fedora 3.0]# ./easyrsa build-ca

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/3.0.8/vars
Using SSL: openssl OpenSSL 3.0.5 5 Jul 2022 (Library: OpenSSL 3.0.5 5 Jul 2022)

Enter New CA Key Passphrase:
Re-Enter New CA Key Passphrase:
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:NazimFC

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/etc/openvpn/easy-rsa/3.0/pki/ca.crt
```

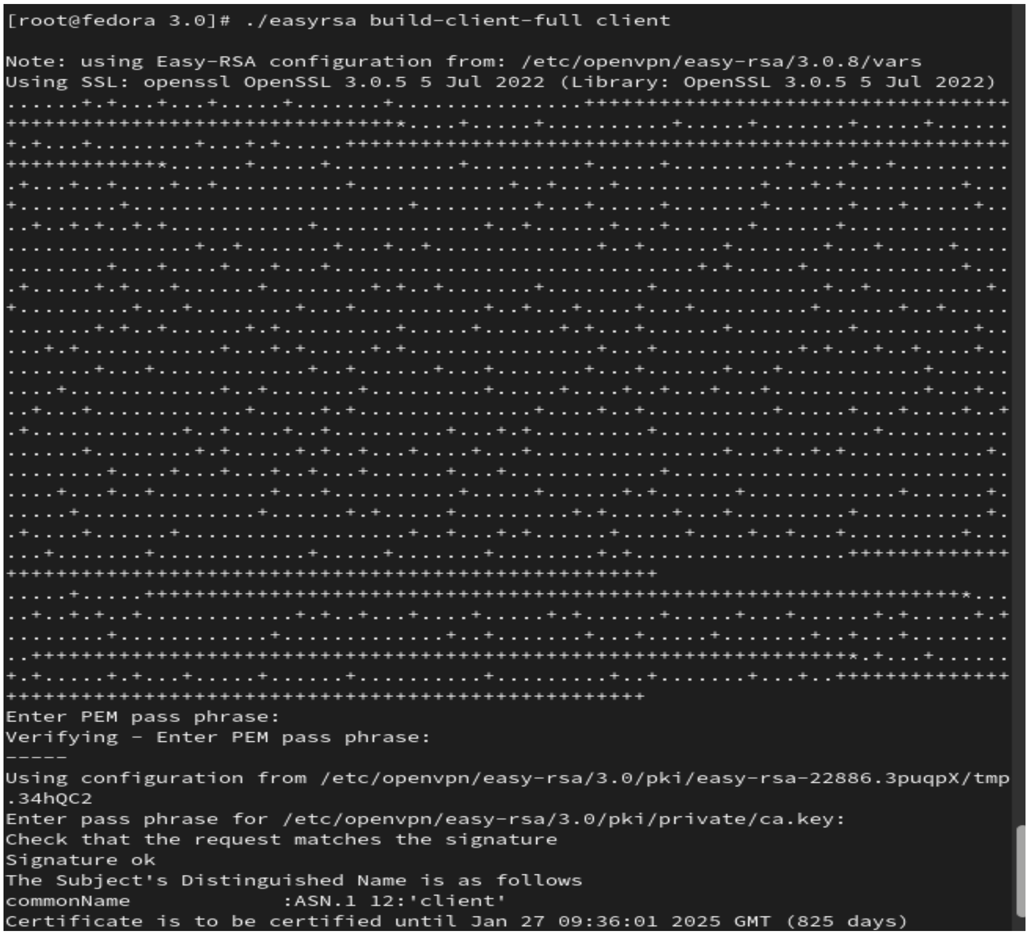
Question 7.2:

Build Server Credentials:



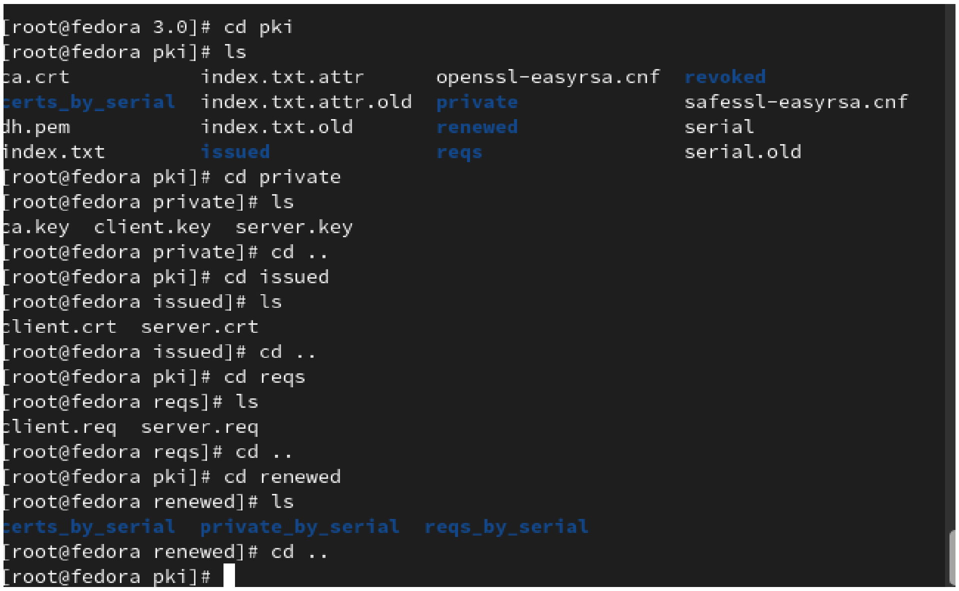
```
[root@fedora 3.0]# ./easyrsa build-server-full server

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/3.0.8/vars
Using SSL: openssl OpenSSL 3.0.5 5 Jul 2022 (Library: OpenSSL 3.0.5 5 Jul 2022)
...+...............+.........+.......++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++*.......+..++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++*...+.....+.+...............+..........+...............+..+....
.....+......+............+.+......+...+..+..........+.........+...+++++++++++++++
+++++++++++++++++++++++++++++++++++++++++++++++++++
.+.+.....+....+........+....+......+...+............+.+.....+...............+...+
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*..........+....
......+...........+...+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++*.+..........+..+...+....+.....+...+....+....+...+......+.........+.....+.
+.....+.+.....+.........+....+...+........+.....+..+.+..............+............
......+......+..........+.....+.+...+...+.........+.+......+...+..+.........+....
..+....+...........+.......+..+....+..+..........+..........+........+......+.+..
.+..+.+...+.....+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
Using configuration from /etc/openvpn/easy-rsa/3.0/pki/easy-rsa-22619.QCzxlt/tmp
.hWh1wh
Enter pass phrase for /etc/openvpn/easy-rsa/3.0/pki/private/ca.key:
80BB1FE4567F0000:error:0700006C:configuration file routines:NCONF_get_string:no
value:crypto/conf/conf_lib.c:315:group=<NULL> name=unique_subject
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'server'
Certificate is to be certified until Jan 27 09:08:28 2025 GMT (825 days)

Write out database with 1 new entries
Data Base Updated
```

Build Client Credentials:



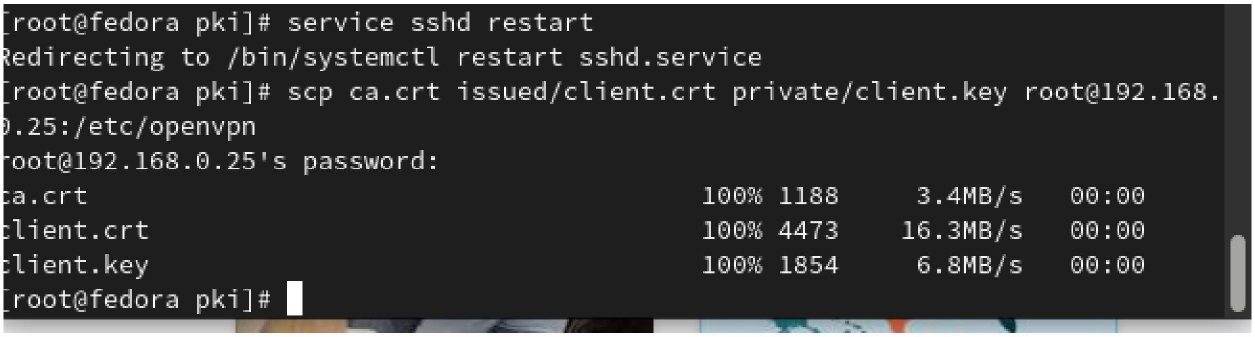
```
[root@fedora 3.0]# ./easyrsa build-client-full client

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/3.0.8/vars
Using SSL: openssl OpenSSL 3.0.5 5 Jul 2022 (Library: OpenSSL 3.0.5 5 Jul 2022)
......+.+...+...+.....+.......+...............++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++*....+.....+..........+.....+.......+.....+......
+.+...+........+...+.+.....+++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++*......+.....+..........+.........+.....+.........+....+..+.........
.+...+..+....+..+..........+............+..+....+...........+...+.+.........+...
+........+......................+.........+...+.....+.......+......+...+.....+..
..+..+.+..+.+...........+.............+..+......+...+......+......+.............
...............+..+.......+...+..+.............+..+......+.......+...+.....+....
........+...+....+...+...+.............................+.+.....+............+...
.+.....+.+...+......+........+.+..+.......+........+.............+..+.........+.
+.........+...+........+...+..........+..+...+....+...+.........+......+..+.....
.......+.+..+......+.+.........+.....+......+.+...+......+.........+.........+..
...+.+...........+...+.+.....+.+...............+...+...........+.+...+..+....+..
.......+...+............+..+......+...+.......+...+......+...+...........+......
....+............+..+.......+.........+.....+....+..+...+...+............+...+..
..+...+............+.....+.+..............+....+..+..........+.....+...+....+..+
.+............+..+....+..+.........+...+.+.........+.................+..........
......+........+.+.....+.+..+...+....+...+...............+...+..+.+...........+.
........+....+...+...+..+...+......+...+............+...........................
....+...+..+.........+...+..........+.....+......+.+......+............+......+.
.....+..............+......+.+.....+.........+.+.....+...+.........+..........+.
.+....+......+..................+..+...+.+......+.....+....+..+...+.........+...
...+.......+............+.....+.......+........+.+.................+++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++
.....+.....+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*...
..+..+.+..+............+.+..+...+....+.....+.+......+.....+...+......+.+.....+.+
........+............+.............+..+.......+...+.....+.......+..+...+........
..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+...+......
+.+.....+.+...+.....+......+..........+.........+..+.......+...+..++++++++++++++
+++++++++++++++++++++++++++++++++++++++++++++++++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
Using configuration from /etc/openvpn/easy-rsa/3.0/pki/easy-rsa-22886.3puqpX/tmp
.34hQC2
Enter pass phrase for /etc/openvpn/easy-rsa/3.0/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'client'
Certificate is to be certified until Jan 27 09:36:01 2025 GMT (825 days)
```

Location of Credentials:



```
[root@fedora 3.0]# cd pki
[root@fedora pki]# ls
a.crt           index.txt.attr      openssl-easyrsa.cnf  revoked
erts_by_serial  index.txt.attr.old  private              safessl-easyrsa.cnf
dh.pem          index.txt.old       renewed              serial
index.txt       issued              reqs                 serial.old
[root@fedora pki]# cd private
[root@fedora private]# ls
a.key  client.key  server.key
[root@fedora private]# cd ..
[root@fedora pki]# cd issued
[root@fedora issued]# ls
lient.crt  server.crt
[root@fedora issued]# cd ..
[root@fedora pki]# cd reqs
[root@fedora reqs]# ls
lient.req  server.req
[root@fedora reqs]# cd ..
[root@fedora pki]# cd renewed
[root@fedora renewed]# ls
erts_by_serial  private_by_serial  reqs_by_serial
[root@fedora renewed]# cd ..
[root@fedora pki]#
```

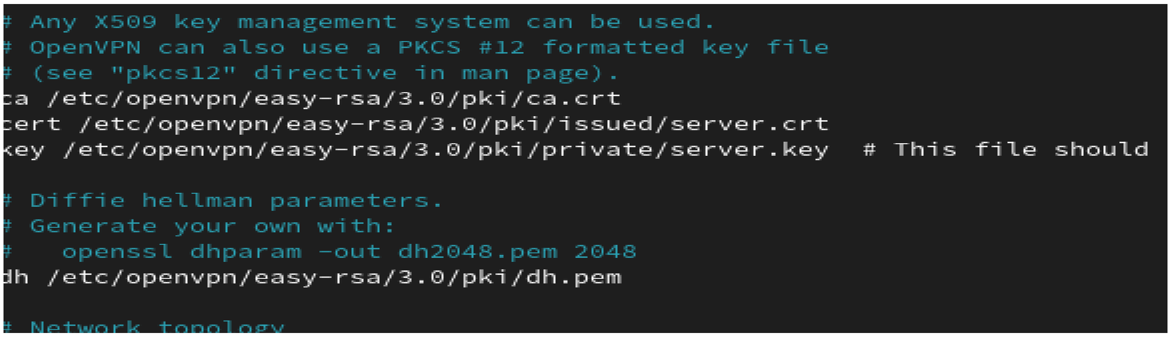
Copy files:



```
[root@fedora pki]# service sshd restart
Redirecting to /bin/systemctl restart sshd.service
[root@fedora pki]# scp ca.crt issued/client.crt private/client.key root@192.168.
0.25:/etc/openvpn
root@192.168.0.25's password:
ca.crt                                        100% 1188     3.4MB/s   00:00
client.crt                                    100% 4473    16.3MB/s   00:00
client.key                                    100% 1854     6.8MB/s   00:00
[root@fedora pki]# 
```

Question 7.3:

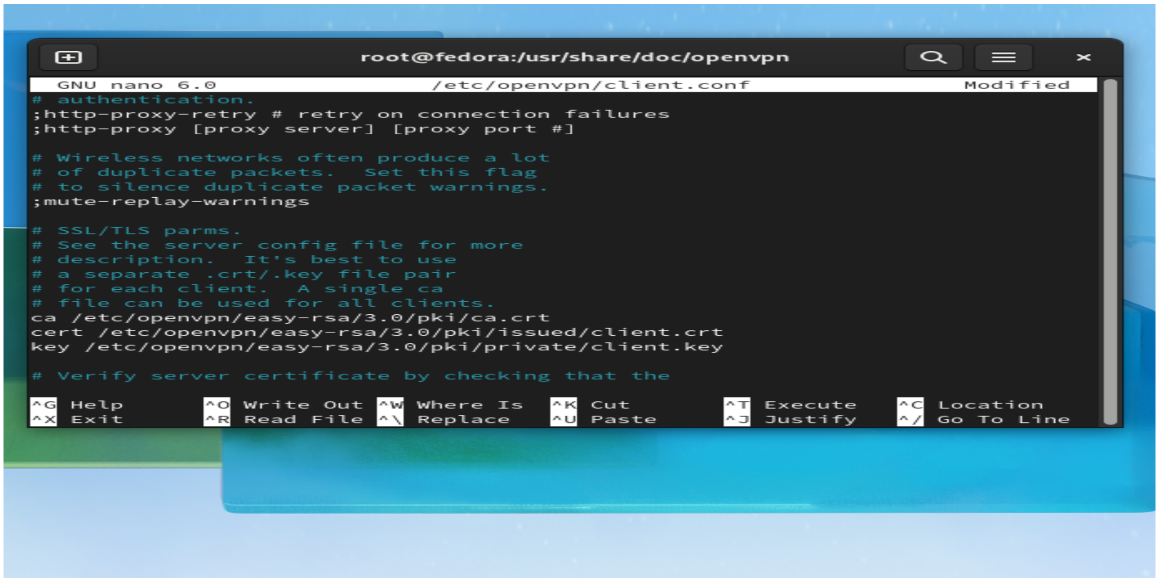
Proper Location of Parameters:



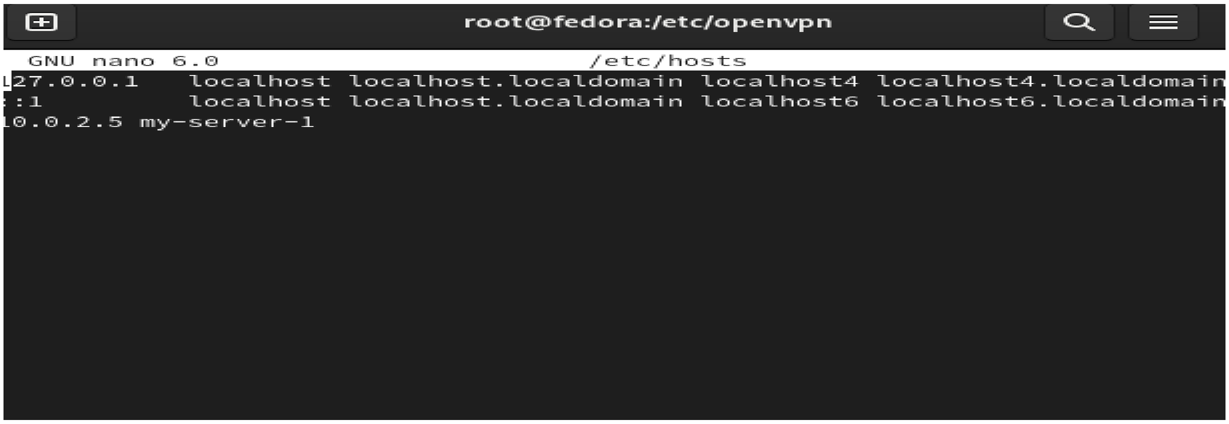
```
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca /etc/openvpn/easy-rsa/3.0/pki/ca.crt
cert /etc/openvpn/easy-rsa/3.0/pki/issued/server.crt
key /etc/openvpn/easy-rsa/3.0/pki/private/server.key  # This file should

# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh2048.pem 2048
dh /etc/openvpn/easy-rsa/3.0/pki/dh.pem

# Network topology
```

Question 7.4:

Client Configuration:

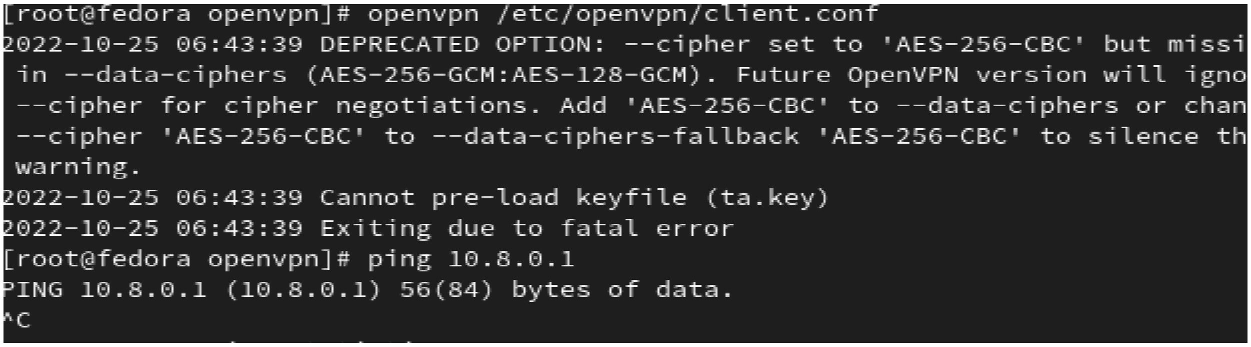


```
  GNU nano 6.0              /etc/openvpn/client.conf                  Modified
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.  Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca /etc/openvpn/easy-rsa/3.0/pki/ca.crt
cert /etc/openvpn/easy-rsa/3.0/pki/issued/client.crt
key /etc/openvpn/easy-rsa/3.0/pki/private/client.key

# Verify server certificate by checking that the

^G Help        ^O Write Out ^W Where Is  ^K Cut         ^T Execute    ^C Location
^X Exit        ^R Read File ^\ Replace   ^U Paste       ^J Justify    ^/ Go To Line
```



```
  GNU nano 6.0                        /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain
::1         localhost localhost.localdomain localhost6 localhost6.localdomain
10.0.2.5 my-server-1
```

Unfortunately, this error occurs. Hope to resolve it with group partner.



```
[root@fedora openvpn]# openvpn /etc/openvpn/client.conf
2022-10-25 06:43:39 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missi
 in --data-ciphers (AES-256-GCM:AES-128-GCM). Future OpenVPN version will igno
 --cipher for cipher negotiations. Add 'AES-256-CBC' to --data-ciphers or chan
 --cipher 'AES-256-CBC' to --data-ciphers-fallback 'AES-256-CBC' to silence th
 warning.
2022-10-25 06:43:39 Cannot pre-load keyfile (ta.key)
2022-10-25 06:43:39 Exiting due to fatal error
[root@fedora openvpn]# ping 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
^C
```

The ping packets are encrypted so that you can switch your IP address without the packets giving away information on your new IP address.