Patrick Kevorkian
HW 7
Network Security

11/22/17

Lab 1

4.1

1-3. No screenshot needed

4.

```
Pat-Kevorkians-iMac:Desktop PatrickKevorkian$ shasum file1.txt
f4720c14e4d72ab61defffdcbaf8ac762fa23a70  file1.txt
Pat-Kevorkians-iMac:Desktop PatrickKevorkian$
```

```
Pat-Kevorkians-iMac:Desktop PatrickKevorkian$ shasum file2.txt
4265a029bac26bcaac15c49224366c1222ae3a00  file2.txt
Pat-Kevorkians-iMac:Desktop PatrickKevorkian$
```

5-6.

```
Pat-Kevorkians-iMac:Desktop PatrickKevorkian$ shasum file1.txt
f4720c14e4d72ab61defffdcbaf8ac762fa23a70  file1.txt
Pat-Kevorkians-iMac:Desktop PatrickKevorkian$ shasum file2.txt
4265a029bac26bcaac15c49224366c1222ae3a00  file2.txt
Pat-Kevorkians-iMac:Desktop PatrickKevorkian$ cat > sha1sum.txt
f4720c14e4d72ab61defffdcbaf8ac762fa23a70  file1.txt
4265a029bac26bcaac15c49224366c1222ae3a00  file2.txt
Pat-Kevorkians-iMac:Desktop PatrickKevorkian$ shasum -c sha2sum.txt
shasum: sha2sum.txt: No such file or directory
Pat-Kevorkians-iMac:Desktop PatrickKevorkian$ shasum -c sha1sum.txt
file1.txt: OK
file2.txt: OK
Pat-Kevorkians-iMac:Desktop PatrickKevorkian$
```

7.

```
Pat-Kevorkians-iMac:Desktop PatrickKevorkian$ md5sum file1.txt
4a8b946a7386abcbd0d7e284ae8c5871  file1.txt
Pat-Kevorkians-iMac:Desktop PatrickKevorkian$ md5sum file2.txt
80a9ddb2544b575c4d121f59f7dde77f  file2.txt
Pat-Kevorkians-iMac:Desktop PatrickKevorkian$ md5sum -c md5sum.txt
file1.txt: OK
file2.txt: OK
Pat-Kevorkians-iMac:Desktop PatrickKevorkian$
```

Questions:

1. Yes, length 32
2. Most of the time but not always there is a possibility of collision.
3. Sha1 hasn't been broken, and has a 160 bit output compare to md5 at 128 bit. Although I think recently google has broken Sha1, its much more difficult than md5.

4.2

1-6.

```
[Pat-Kevorkians-iMac:Desktop PatrickKevorkian$ gpg --symmetric file1.txt
gpg: directory '/Users/PatrickKevorkian/.gnupg' created
gpg: keybox '/Users/PatrickKevorkian/.gnupg/pubring.kbx' created
[Pat-Kevorkians-iMac:Desktop PatrickKevorkian$ cat file1.txt.gpg
PS??Q[??Z
??      ??0!
[Pat-Kevorkians-iMac:Desktop PatrickKevorkian$ gpg -d file1.txt.gpg
gpg: AES encrypted data
gpg: encrypted with 1 passphrase
This is the first file
This is line 2
Pat-Kevorkians-iMac:Desktop PatrickKevorkian$
```

7-9.

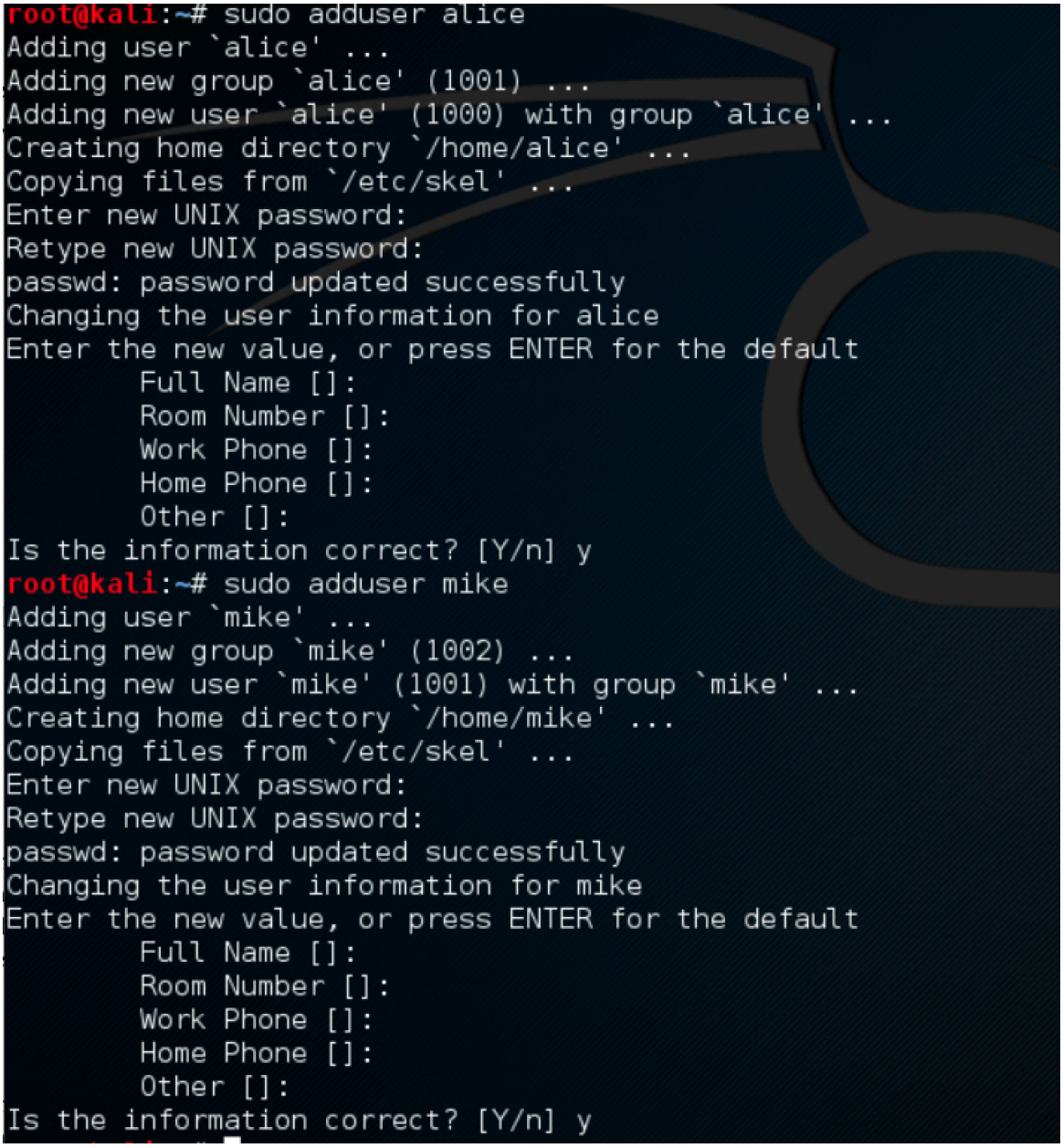
```
[Pat-Kevorkians-iMac:Desktop PatrickKevorkian$ gpg --symmetric --armor file1.txt
[Pat-Kevorkians-iMac:Desktop PatrickKevorkian$ cat file1.txt.asc
-----BEGIN PGP MESSAGE-----

jA0EBwMC0Th+M3BcgsXq0loBPmfF0iCIbWq2TrVGut6L9OfwjRXnNS+pTOC7XFfI
Gp5h5FffRpJT8pvElJ5x99B/BJo1Vj7agvbxMiV5NlYIs3wxPaps9zJlEw7NfSg+
zFVffbD6/5IM8+w=
=tgoI
-----END PGP MESSAGE-----
[Pat-Kevorkians-iMac:Desktop PatrickKevorkian$ gpg --armor -d file1.txt.asc
gpg: AES encrypted data
gpg: encrypted with 1 passphrase
This is the first file
This is line 2
Pat-Kevorkians-iMac:Desktop PatrickKevorkian$
```

Questions:

4. Run “gpg --armor -d message.txt.asc” and enter the passphrase.

4.3.2

1.


root@kali:~# sudo adduser alice
Adding user `alice' ...
Adding new group `alice' (1001) ...
Adding new user `alice' (1000) with group `alice' ...
Creating home directory `/home/alice' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for alice
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y
root@kali:~# sudo adduser mike
Adding user `mike' ...
Adding new group `mike' (1002) ...
Adding new user `mike' (1001) with group `mike' ...
Creating home directory `/home/mike' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for mike
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

2.

```
root@kali:~# sudo usermod -aG sudo alice
root@kali:~# sudo usermod -aG sudo mike
```

3.

```
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
alice@kali:~$ gpg --gen-key
gpg (GnuPG) 1.4.18; Copyright (C) 2014 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: directory `/home/alice/.gnupg' created
gpg: new configuration file `/home/alice/.gnupg/gpg.conf' created
gpg: WARNING: options in `/home/alice/.gnupg/gpg.conf' are not yet active during this run
gpg: keyring `/home/alice/.gnupg/secring.gpg' created
gpg: keyring `/home/alice/.gnupg/pubring.gpg' created
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 2
DSA keys may be between 1024 and 3072 bits long.
What keysize do you want? (2048) 2048
Requested keysize is 2048 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Alice
Email address: alice@pace.edu
```

```
Real name: Alice
Email address: alice@pace.edu
Comment: Alice's keys
You selected this USER-ID:
    "Alice (Alice's keys) <alice@pace.edu>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
You need a Passphrase to protect your secret key.

passphrase not correctly repeated; try again.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: WARNING: some OpenPGP programs can't handle a DSA key with this digest size
++++++++++++++++++++++++...++++++++++++++++++++++++.++++++++++++++++++.+++++.++++++++++....++++++++++..+++++
....+++++.++++++++++.+++++.++++++++++++++>+++++>+++++.....................................................
.........................+++++

Not enough random bytes available.  Please do some other work to give
the OS a chance to collect more entropy! (Need 247 more bytes)
```

```
gpg: /home/alice/.gnupg/trustdb.gpg: trustdb created
gpg: key F8D51AA9 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
pub   2048D/F8D51AA9 2017-11-25
      Key fingerprint = 3E12 88C9 0616 A1E3 4BE7  FF0C 34D7 6CC0 F8D5 1AA9
uid                  Alice (Alice's keys) <alice@pace.edu>
sub   2048g/DDC9BA6F 2017-11-25

alice@kali:~$
alice@kali:~$
```

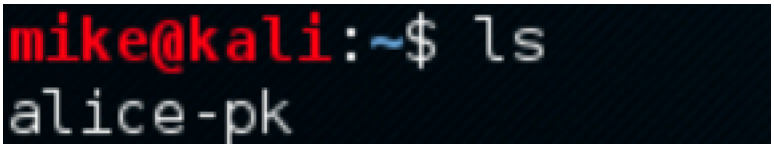
4.

```
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
.+++++.++++++++++.+++++..+++++.+++++++++++++++.+++++.++++++++++++++++++++++..++++++++++++++
++++++++...+++++...++++++++++..++++++++++++++++++>++++++++++>+++++>+++++.....................
.....................................................................................
.................+++++^^^
gpg: /home/mike/.gnupg/trustdb.gpg: trustdb created
gpg: key 90C53543 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
pub   2048D/90C53543 2017-11-25
      Key fingerprint = F9CE 17DD 6FAC C0D6 723E  1F29 58AA 4BF5 90C5 3543
uid                  Michael (Mike's keys) <mike@pace.edu>
sub   2048g/518BB307 2017-11-25

mike@kali:~$
mike@kali:~$
```

5.

```
alice@kali:~$ gpg --armor --output alice-pk --export alice@pace.edu
alice@kali:~$ more alice-pk
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQMuBFoY4W8RCADD1xRCURtu2eu5EyJ2JowU91G9J/ypLZAAtlB/ihAlQEqyYHE6
7BT6ktIOO1oBUuaLdZtSWkTZ0dUxcIKP8sm0nsZ2NN0kRwR0wz5h4vI/xn3QmUn3
/nFj1QpqkBYnE6zNLPs0dtQ006DL99nJ0I4xtXYqTelXQYlUYEIe0NAeD3TD8Fc6
i05/5/+2g/lKdkIQZ3mQVQJuP0W3NRh6LnIF1Biw+hZubkrknI4jN9RMjcbxgY7V
1BKQJpQ0Fnd1oAsDw3PBQpqX/CJnFKOzB6rCjpZYxU1HpeJJ1BKz3402cf1H0U2X
QeHdwU3/MS82kMFS4l3jTyi8Jx11PHmMT7xjAQCGjVfAszDP9wPNWMvSrHt14pgB
QeDUUgpBwf9dvPtEewf/T18cyY32A/rL9TubhZdblggn6G1cy2tipmHdpozsz7w7
qqzJXXWhoxeML960trhvdii4UPYD6UIUopZAluxNHGvhDycQnkI05NfzUva3Oeqk
QRy1SIpJ9CVMl7H2hUw+VIBjUXo6H0/6Pi2z080Oh8rVsJF3gyGHm3wSQgNAtitr
h0NeMeF9LD7/up2OTkOEVAatLCtGSJbDku/pc3AdK3h4V1O+8Jd7brDhTPgs8zlf
cGX3NVo0XKbU9N01+4yK5D6zZgAABwPS4d+DplHN3Au+FQDx/2fIPYg6QNyFIAwF
hhQsEPLwBbbbfe8jh1OzYbodjS9x4875DB7IA4CKgAf+N0A9p/gZwme+6dKAbBS0
GqBW9I8kgFttTOUVKXIi+ifKyRNn19ECb9JcGB4NIkbgeghXvD7McAL7eHyxOh6m
Ic5XAuiCI3xp22bPMtBkM3ggWGPrpdITWqDlK5pFKXaiIcmXW0SBSi3dwDVR6EQK
fQqvx03xKClvWhNmiBsTwCMurLlFRP4DYEWfnCDdkkmjczPH19RgMKvlW+eqJixX
cxy5tNaXBTkHiYnUL/HU1RkG9ij/iY6cHHWYjUQnxTKi5hZc7pSZm+NVMlCh14Bl
VbMC5lxXTZBMACLA3ZZ3SLJU840EOpMrj4Q0PmPxeXPoEFEqWRsVMGUR+IR9olEQ
mLQlQWxpY2UgKEFsaWNlJ3Mga2V5cykgPGFsaWNlQHBhY2UuZWR1Poh6BBMRCAAi
BQJaGOFvAhsDBgsJCAcDAgYVCAIJCgsEFgIDAQIeAQIXgAAKCRA012zA+NUaqTHm
AP4/KxeNeL87NoxGYysLYrpVqSQpQjOeGitG6pVZAW1f4gD/U8oAkH7QtsgAOJ7p
KPUa2P0LfYJsqHm2qqxwOjx2il+5Ag0EWhjhbxAIAMR9cCAh7gy2guUkLLw9/uJu
FJpIj0KDSfyIcL4m/CD2vkvB+6lKTzItzYe/AK/9tkEJ0dBSG71nYQU/cfIeNRrh
lS11J9Vx1DcUUwo5YSGoLlOWwcSDgWb3OBW0Bmz9gvgbH9PcqRyv2hjVtGUyyNfM
lb+bsd++ETueOzrow+jcozJ6vgk5bSV0Ei9Jfx/8/zz8AmxJkkPtnv1oi6zxMqun
mbQbgWQpTE9h4hnax1BvjH5etuEfZ7vxHERg6C6c0d8glz2eNJTKj+XDCyKGIgl3
eACWzb6kf+TfB/v9vWM9UA5sCwnmnxpSh/Zy8UVGG9lwNnOXjli5QCLVVOg7+AMA
AwUH/3qK9C1zVQTwOOnUE5SMV9rU327rMPrxENU85Gz6unaKhbzleyqEARaWRZWj
0L6z/oR/5mI/AHbIyMBpSKSy9M5u1BJzzhnLspHDSiiy8WsjvnXEvtsSzvS9rq00
wk0JBNBA1uF0+pDTQMU35g4mlsIvnJ11xOsMuxF4i9KMSIEVbG/jvD/FKiCtnYhx
ToxnOH3gXnQx8+TDKd5TCSGQFNw7xu4t/unzJ90F2F2Q8g/I0Xy91bvYvBDfifEo
2EkyBjUBpU3pfTvS8B2/bhIGcuLNEmbSF4q1BAPlzgiko+G8e2MnyPWAoqf7zgDS
2f90WLU4ijyeI0v6BBMTa+h5E30IYQQYEQgACQUCWhjhbwIbDAAKCRA012zA+NUa
```

```
alice@kali:~$ sudo cp alice-pk /home/mike

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for alice:
```




```
gpg> check
uid  Alice (Alice's keys) <alice@pace.edu>
sig!3        F8D51AA9 2017-11-25  [self-signature]
sig!         90C53543 2017-11-25  Michael (Mike's keys) <mike@pace.edu>

This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.


pub  2048D/F8D51AA9  created: 2017-11-25  expires: never       usage: SC
                     trust: unknown       validity: unknown
sub  2048g/DDC9BA6F  created: 2017-11-25  expires: never       usage: E
[ unknown] (1). Alice (Alice's keys) <alice@pace.edu>

gpg> fpr
pub   2048D/F8D51AA9 2017-11-25 Alice (Alice's keys) <alice@pace.edu>
 Primary key fingerprint: 3E12 88C9 0616 A1E3 4BE7  FF0C 34D7 6CC0 F8D5 1AA9

gpg> sign

pub  2048D/F8D51AA9  created: 2017-11-25  expires: never       usage: SC
                     trust: unknown       validity: unknown
 Primary key fingerprint: 3E12 88C9 0616 A1E3 4BE7  FF0C 34D7 6CC0 F8D5 1AA9

     Alice (Alice's keys) <alice@pace.edu>

Are you sure that you want to sign this key with your
key "Michael (Mike's keys) <mike@pace.edu>" (90C53543)

Really sign? (y/N) y

You need a passphrase to unlock the secret key for
user: "Michael (Mike's keys) <mike@pace.edu>"
2048-bit DSA key, ID 90C53543, created 2017-11-25
```

```
gpg> check
uid  Alice (Alice's keys) <alice@pace.edu>
sig!3        F8D51AA9 2017-11-25  [self-signature]
sig!         90C53543 2017-11-25  Michael (Mike's keys) <mike@pace.edu>
```

6.

```
mike@kali:~$ cat > msg-to-alice
Alice's secret message
mike@kali:~$ gpg --recipient alice@pace.edu --output secret-to-alice --encrypt msg-to-alice
gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   1  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: depth: 1  valid:   1  signed:   0  trust: 1-, 0q, 0n, 0m, 0f, 0u
mike@kali:~$ more secret-to-alice
5[illegible]
[illegible]
Y[illegible]
w8[illegible]
9$A[illegible]
F6^Lx{[illegible]
~J6 ;[illegible]
mike@kali:~$
mike@kali:~$
mike@kali:~$
mike@kali:~$
mike@kali:~$ sudo cp secret-to-alice /home/alice

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for mike:
mike@kali:~$
```

```
alice@kali:~$ ls
alice-pk  secret-to-alice
```

7.

```
alice@kali:~$ gpg --output msg-from-mike --decrypt secret-to-alice

You need a passphrase to unlock the secret key for
user: "Alice (Alice's keys) <alice@pace.edu>"
2048-bit ELG-E key, ID DDC9BA6F, created 2017-11-25 (main key ID F8D51AA9)

gpg: encrypted with 2048-bit ELG-E key, ID DDC9BA6F, created 2017-11-25
      "Alice (Alice's keys) <alice@pace.edu>"
alice@kali:~$ more msg-from-mike
Alice's secret message
alice@kali:~$
```

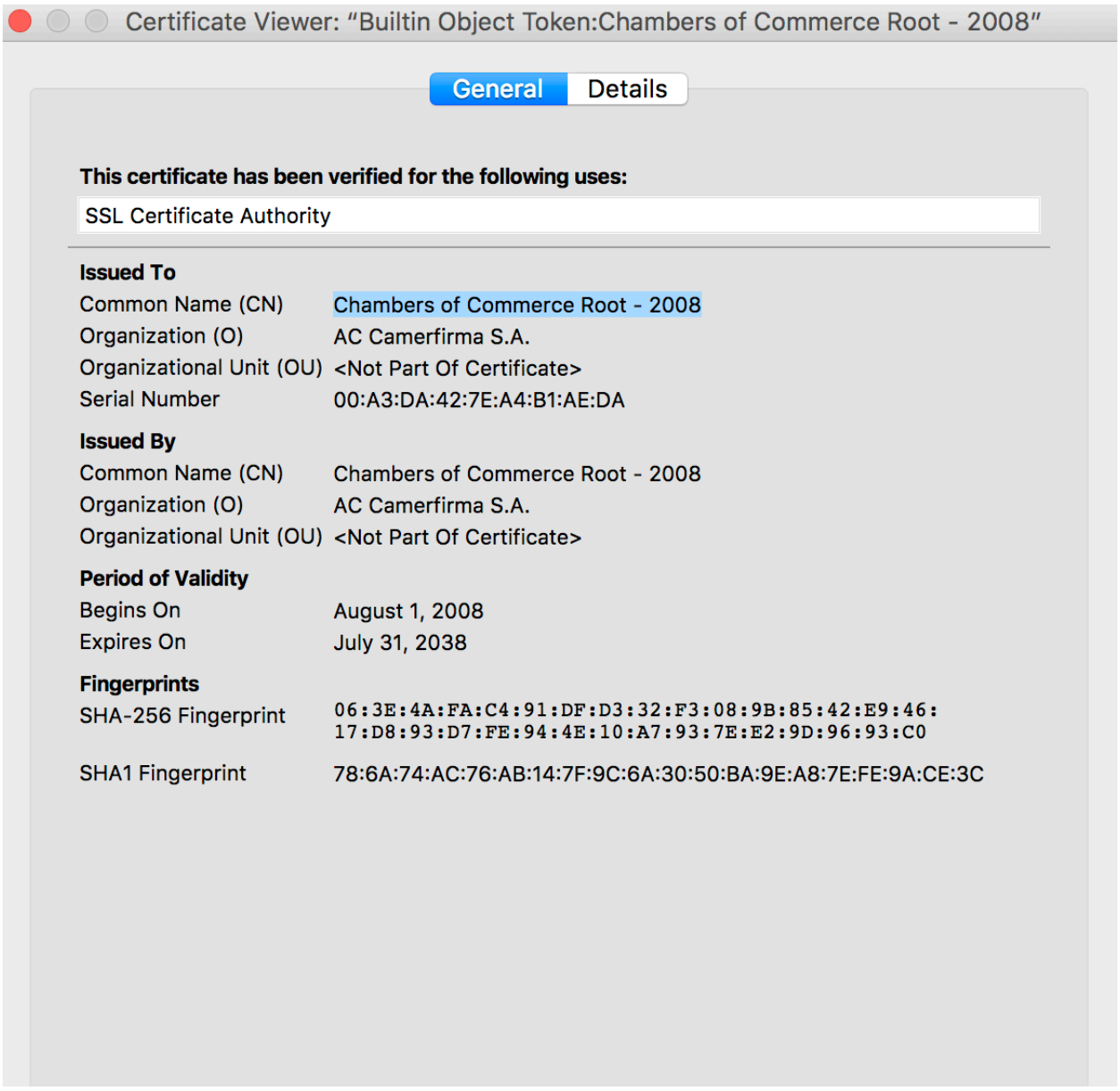
Questions:

5. Key servers, cloud.
6. Yes, but how do users know its your key?
7. Diffie-Hellman
8. Many ways, the message is encrypted.
9. Yes
10. Yes
11. No

Lab 2

4.1

1 - 2. TLS/SSL
3. AC Camerafirma S.A. , Atos
4.



5. Sha1 with RSA encryption

6. 4096 bits
7. TLS
8. It Expired

4.1 Creating Certificates

1-5.

```
patrick@patrick-VirtualBox:/etc/apache2/ssl$ sudo openssl genrsa -des3 -out server.key 1024
Generating RSA private key, 1024 bit long modulus
..............++++++
.....................++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
patrick@patrick-VirtualBox:/etc/apache2/ssl$ ls
server.key
patrick@patrick-VirtualBox:/etc/apache2/ssl$
```

Passphrase: snapple

6-7.

```
patrick@patrick-VirtualBox:/etc/apache2/ssl$ sudo 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]:US
State or Province Name (full name) [Some-State]:New York
Locality Name (eg, city) []:New York
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Pace University
Organizational Unit Name (eg, section) []:CSIS-IT300
Common Name (e.g. server FQDN or YOUR name) []:www.BadStore.net
Email Address []:patrickkevorkian@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:12345
An optional company name []:CSIS
patrick@patrick-VirtualBox:/etc/apache2/ssl$ ls
server.csr  server.key
patrick@patrick-VirtualBox:/etc/apache2/ssl$
```

8-10

```
patrick@patrick-VirtualBox:/etc/apache2/ssl$ sudo openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
Signature ok
subject=/C=US/ST=New York/L=New York/O=Pace University/OU=CSIS-IT300/CN=www.BadStore.net/emailAddress=patrickkevorkian@gmail.com
Getting Private key
Enter pass phrase for server.key:
patrick@patrick-VirtualBox:/etc/apache2/ssl$
```

```
patrick@patrick-VirtualBox:/etc/apache2/ssl$ ls
server.crt  server.csr  server.key
patrick@patrick-VirtualBox:/etc/apache2/ssl$
```

4.2

1-4.

```
patrick@patrick-VirtualBox:/etc/apache2/sites-available$ sudo gedit www.badstore.net
No protocol specified
Unable to init server: Could not connect: Connection refused

(gedit:2984): Gtk-WARNING **: cannot open display: :0
patrick@patrick-VirtualBox:/etc/apache2/sites-available$ sudo gedit /www.badstore.net
No protocol specified
Unable to init server: Could not connect: Connection refused

(gedit:2989): Gtk-WARNING **: cannot open display: :0
patrick@patrick-VirtualBox:/etc/apache2/sites-available$ sudo nano www.badstore.net
Use "fg" to return to nano.

[1]+  Stopped                 sudo nano www.badstore.net
patrick@patrick-VirtualBox:/etc/apache2/sites-available$ sudo nano www.badstore.net
patrick@patrick-VirtualBox:/etc/apache2/sites-available$ sudo nano www.badstore.net
patrick@patrick-VirtualBox:/etc/apache2/sites-available$ sudo a2ensite www.badstore.net
ERROR: Site www.badstore.net does not exist!
patrick@patrick-VirtualBox:/etc/apache2/sites-available$ ls
000-default.conf  default  default-ssl.conf  www.badstore.net
patrick@patrick-VirtualBox:/etc/apache2/sites-available$ cd default
patrick@patrick-VirtualBox:/etc/apache2/sites-available/default$ ls
patrick@patrick-VirtualBox:/etc/apache2/sites-available/default$ cd ../
patrick@patrick-VirtualBox:/etc/apache2/sites-available$ ^C
patrick@patrick-VirtualBox:/etc/apache2/sites-available$ cd ../
patrick@patrick-VirtualBox:/etc/apache2$ cd ssl
patrick@patrick-VirtualBox:/etc/apache2/ssl$ sudo a2ensite www.badstore.net
ERROR: Site www.badstore.net does not exist!
patrick@patrick-VirtualBox:/etc/apache2/ssl$ cd .//
patrick@patrick-VirtualBox:/etc/apache2/ssl$ cd ../
patrick@patrick-VirtualBox:/etc/apache2$ cd sites-available
patrick@patrick-VirtualBox:/etc/apache2/sites-available$ ls
000-default.conf  default  default-ssl.conf  www.badstore.net
patrick@patrick-VirtualBox:/etc/apache2/sites-available$ mv www.badstore.net www.badstore.net.conf
mv: cannot move 'www.badstore.net' to 'www.badstore.net.conf': Permission denied
patrick@patrick-VirtualBox:/etc/apache2/sites-available$ sudo mv www.badstore.net www.badstore.net.conf
patrick@patrick-VirtualBox:/etc/apache2/sites-available$ sudo a2ensite www.badstore.net.conf
Enabling site www.badstore.net.
To activate the new configuration, you need to run:
  systemctl reload apache2
patrick@patrick-VirtualBox:/etc/apache2/sites-available$ systemctl reload apache2
Job for apache2.service failed because the control process exited with error code.
See "systemctl  status apache2.service" and "journalctl  -xe" for details.
patrick@patrick-VirtualBox:/etc/apache2/sites-available$ sudo service apache2 restart
Job for apache2.service failed because the control process exited with error code.
See "systemctl  status apache2.service" and "journalctl  -xe" for details.
patrick@patrick-VirtualBox:/etc/apache2/sites-available$
```

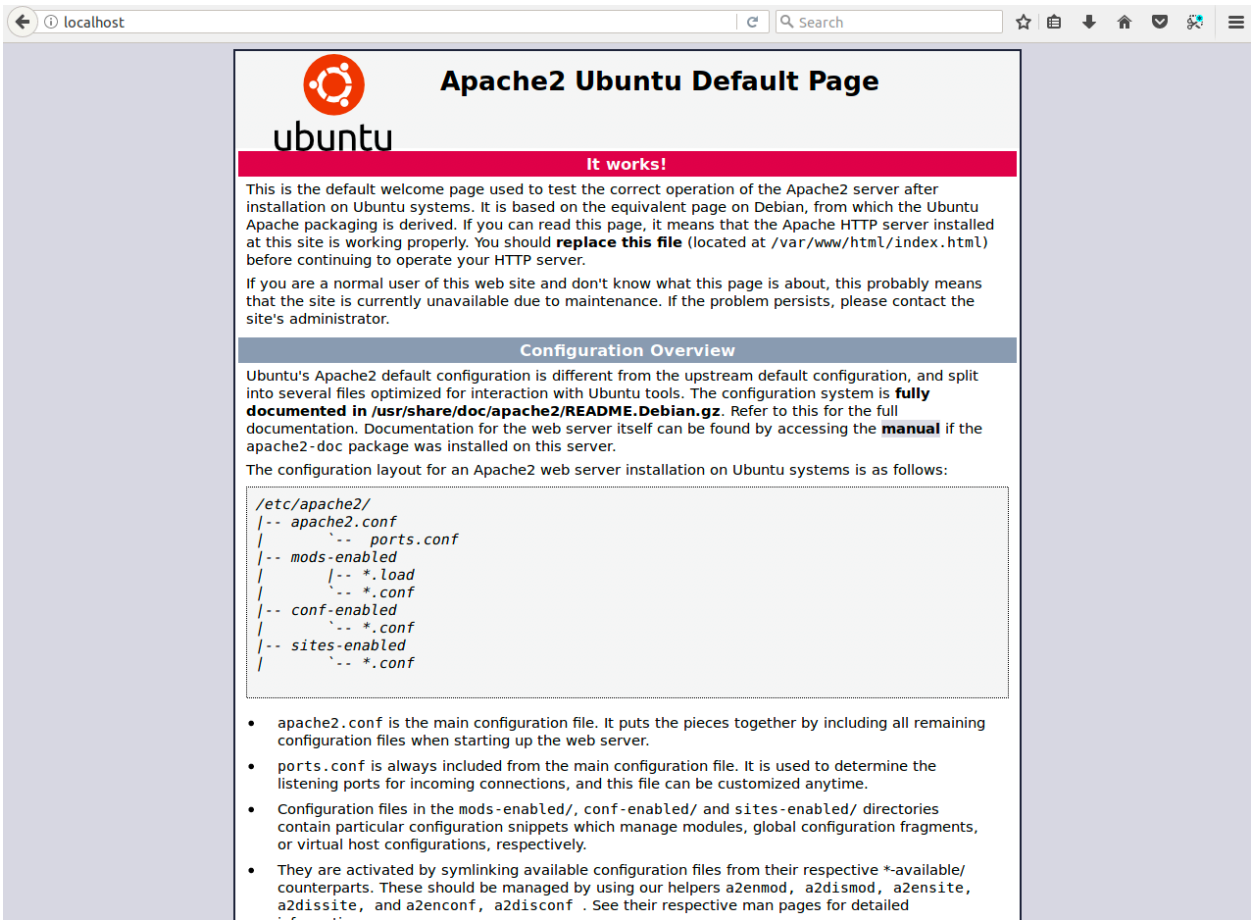
8-9.

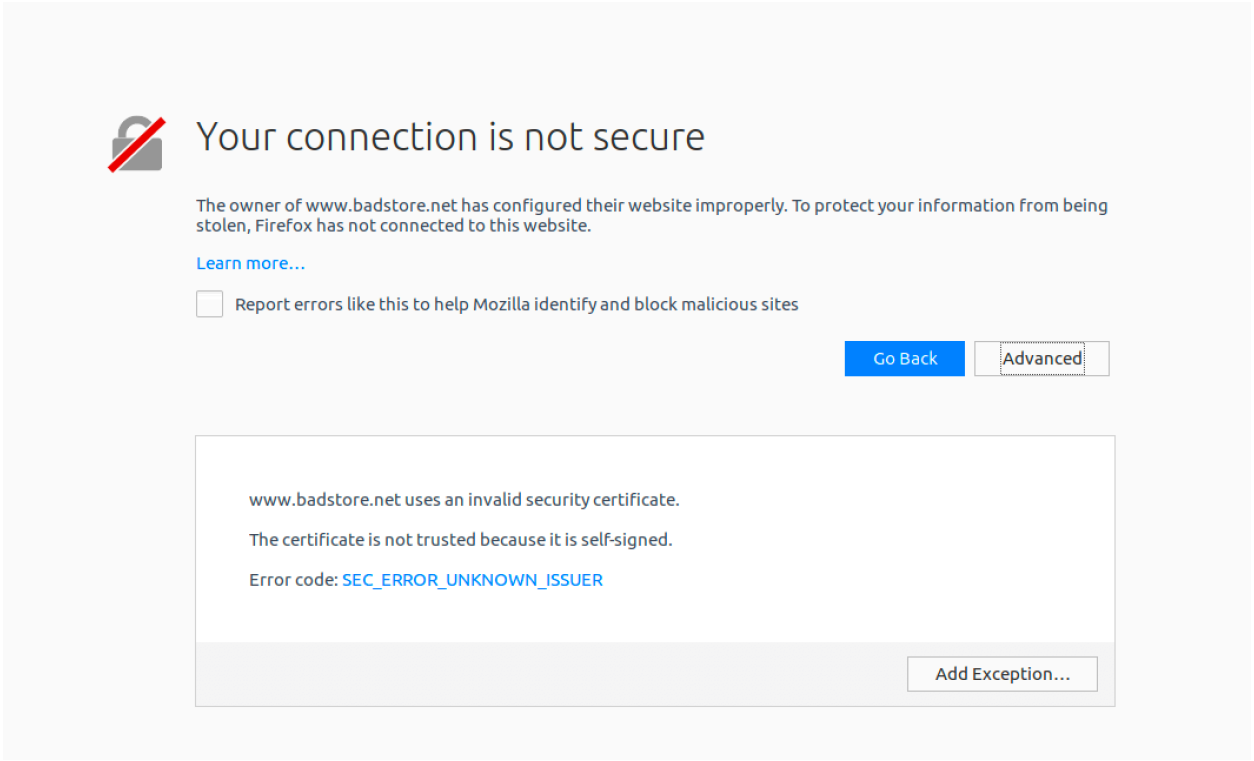
```
127.0.0.1       www.badstore.net
127.0.1.1       patrick-VirtualBox

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

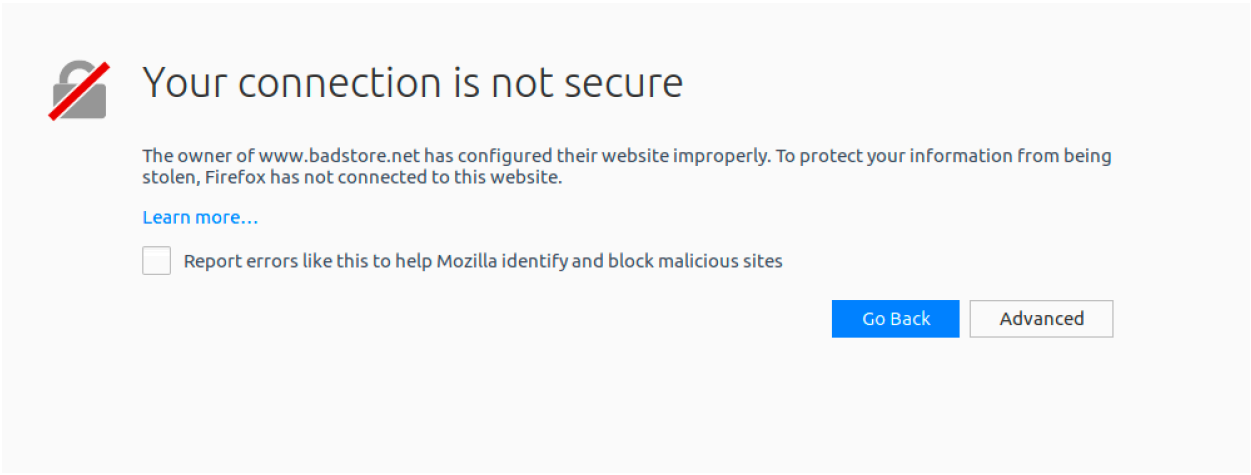
4.3

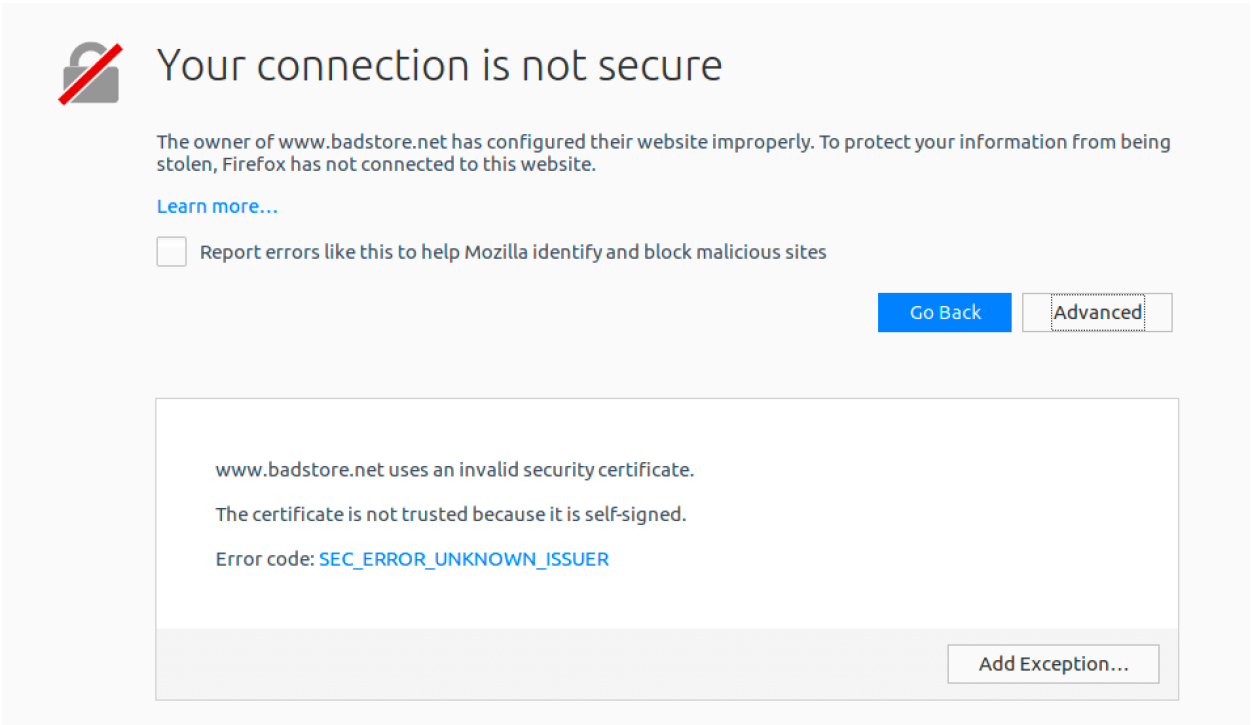
1-2

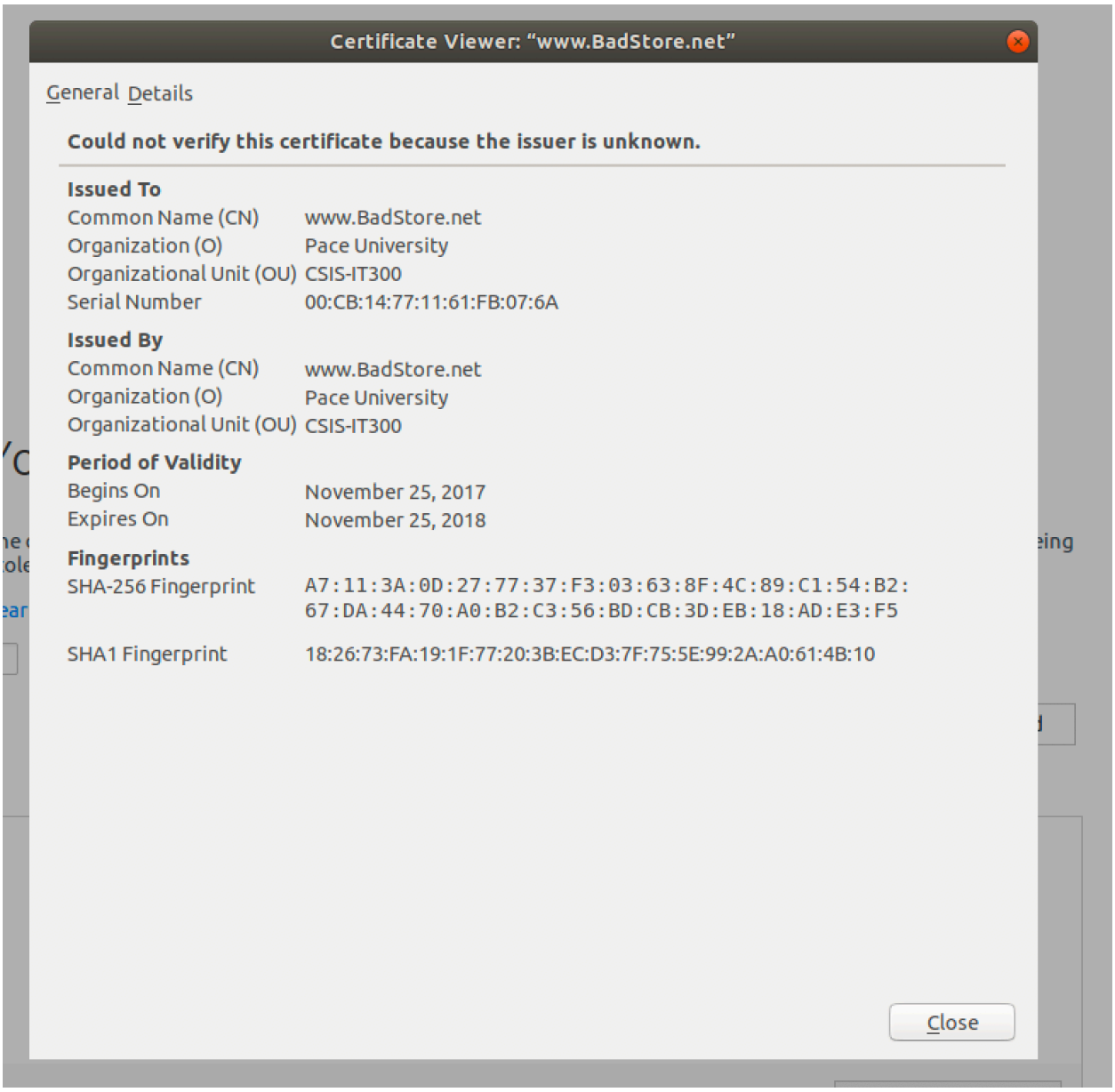
```
patrick@patrick-VirtualBox:/etc/apache2/sites-available$ sudo nano www.badstore.net.conf
patrick@patrick-VirtualBox:/etc/apache2/sites-available$ sudo /etc/init.d/apache2 restart
[....] Restarting apache2 (via systemctl): apache2.serviceEnter passphrase for SSL/TLS keys for www.badstore.net:443 (RSA): *******
. ok
patrick@patrick-VirtualBox:/etc/apache2/sites-available$
```


localhost
Search
Apache2 Ubuntu Default Page
ubuntu
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers a2enmod, a2dismod, a2ensite, a2dissite, and a2enconf, a2disconf . See their respective man pages for detailed


Your connection is not secure
The owner of www.badstore.net has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.
Learn more...
Report errors like this to help Mozilla identify and block malicious sites
Go Back
Advanced
www.badstore.net uses an invalid security certificate.
The certificate is not trusted because it is self-signed.
Error code: SEC_ERROR_UNKNOWN_ISSUER
Add Exception...


Your connection is not secure
The owner of www.badstore.net has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.
Learn more…
Report errors like this to help Mozilla identify and block malicious sites
Go Back
Advanced


Your connection is not secure
The owner of www.badstore.net has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.
Learn more…
Report errors like this to help Mozilla identify and block malicious sites
Go Back
Advanced
www.badstore.net uses an invalid security certificate.
The certificate is not trusted because it is self-signed.
Error code: SEC_ERROR_UNKNOWN_ISSUER
Add Exception…

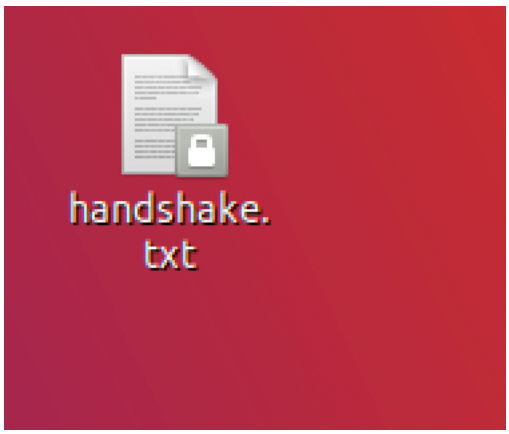

Certificate Viewer: “www.BadStore.net”
General Details
Could not verify this certificate because the issuer is unknown.
Issued To
Common Name (CN) www.BadStore.net
Organization (O) Pace University
Organizational Unit (OU) CSIS-IT300
Serial Number 00:CB:14:77:11:61:FB:07:6A
Issued By
Common Name (CN) www.BadStore.net
Organization (O) Pace University
Organizational Unit (OU) CSIS-IT300
Period of Validity
Begins On November 25, 2017
Expires On November 25, 2018
Fingerprints
SHA-256 Fingerprint A7:11:3A:0D:27:77:37:F3:03:63:8F:4C:89:C1:54:B2:
67:DA:44:70:A0:B2:C3:56:BD:CB:3D:EB:18:AD:E3:F5
SHA1 Fingerprint 18:26:73:FA:19:1F:77:20:3B:EC:D3:7F:75:5E:99:2A:A0:61:4B:10
Close

4.4

1.

```
root@patrick-VirtualBox:/home/patrick/Desktop# openssl s_client -connect www.badstore.net:443>handshake.txt
depth=0 C = US, ST = New York, L = New York, O = Pace University, OU = CSIS-IT300, CN = www.BadStore.net, emailAddress = patrickkevorkian@gmail.com
verify error:num=18:self signed certificate
verify return:1
depth=0 C = US, ST = New York, L = New York, O = Pace University, OU = CSIS-IT300, CN = www.BadStore.net, emailAddress = patrickkevorkian@gmail.com
verify return:1
```

2.




```
CONNECTED(00000003)
---
Certificate chain
 0 s:/C=US/ST=New York/L=New York/O=Pace University/OU=CSIS-IT300/CN=www.BadStore.net/emailAddress=patrickkevorkian@gmail.com
   i:/C=US/ST=New York/L=New York/O=Pace University/OU=CSIS-IT300/CN=www.BadStore.net/emailAddress=patrickkevorkian@gmail.com
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICyTCCAjICCQDLFHcRYfsHajANBgkqhkiG9w0BAQsFADCBqDELMAkGA1UEBhMC
VVMxETAPBgNVBAgMCE5ldyBZb3JrMREwDwYDVQQHDAhOZXcgWW9yazEYMBYGA1UE
CgwPUGFjZSBVbml2ZXJzaXR5MRMwEQYDVQQLDApDU0lTLUlUMzAwMRkwFwYDVQQD
DBB3d3cuQmFkU3RvcmUubmV0MSkwJwYJKoZIhvcNAQkBFhpwYXRyaWNra2V2b3Jr
aWFuQGdtYWlsLmNvbTAeFw0xNzExMjUwNTQ5NDVaFw0xODExMjUwNTQ5NDVaMIGo
MQswCQYDVQQGEwJVUzERMA8GA1UECAwITmV3IFlvcmsxETAPBgNVBAcMCE5ldyBZ
b3JrMRgwFgYDVQQKDA9QYWNlIFVuaXZlcnNpdHkxEzARBgNVBAsMCkNTSVMtSVQz
MDAxGTAXBgNVBAMMEHd3dy5CYWRTdG9yZS5uZXQxKTAnBgkqhkiG9w0BCQEWGnBh
dHJpY2trZXZvcmtpYW5AZ21haWwuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQDqul5ZEgvQYuLeXW6t6rsTzUUxQanD7kHxUwt0owaAasFme1p9hG1eEtaq
dwXb1L2ogMqkqHLyjMvE/uKfswMkNmy46n2gC8siAyfiQnwNwFe71RZ3J2iU+1C9
fGL0fLkw8jNy9NYl1G3xl6/+UhNqg7ldAFEwaofzXvp4O9gMQwIDAQABMA0GCSqG
SIb3DQEBCwUAA4GBAIYBTmviNk4XpU588e6GtcZTRs07qWiINGuWdtE02xak514w
WWHq0ruz6WtSjXlPZ9/ec1YmfJgcnZ4KdKzyw26mgTAWg2YuXpEZP0b1mzsKNdQx
oZi9A0zsgU7cvYH8k1CdJFFICWpcqc/xJRSXHMVJo176+h31S6itu8UaAGl0
-----END CERTIFICATE-----
subject=/C=US/ST=New York/L=New York/O=Pace University/OU=CSIS-IT300/CN=www.BadStore.net/emailAddress=patrickkevorkian@gmail.com
issuer=/C=US/ST=New York/L=New York/O=Pace University/OU=CSIS-IT300/CN=www.BadStore.net/emailAddress=patrickkevorkian@gmail.com
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 1280 bytes and written 431 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: 4526376C1388D3204E854783BAFA56C14985C86007F417A5DF0F686CED4C2CC0
    Session-ID-ctx:
    Master-Key: BA45C5BE1F99DC07E9BC54742DE81C1191A4021CED8426883678E4523DC01A26C6A499048AFF473914766BBB654E3E5E
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - c1 6f 0d e5 5b e0 f5 d8-e5 43 7e 35 0f da fc 41   .o..[....C~5...A
    0010 - 89 9c f6 f9 07 a5 eb e5-59 38 a0 cc 9c ab 76 30   ........Y8....v0
    0020 - e4 04 5e 0b f4 c2 7f 9f-59 2f 87 c3 dd 5c e3 c0   ..^.....Y/...\..
    0030 - 2a 20 64 54 59 86 6f ef-4e 3e 4c c9 a6 ae 7e d7   * dTY.o.N>L...~.
    0040 - f4 5b 85 25 8a 4f 89 4c-3e 67 80 40 78 88 76 60   .[.%.O.L>g.@x.v`
```

```
    0040 - f4 5b 85 25 8a 4f 89 4c-3e 67 80 40 78 88 76 60   .[.%.O.L>g.@x.v`
    0050 - d6 81 87 ac 83 90 c3 b7-4e be 91 3b e7 f6 84 6b   ........N..;...k
    0060 - 0b cc d6 6f fb 6b 2f cc-5d 0b ca f6 3a 62 ee 86   ...o.k/.]...:b..
    0070 - 86 2a cd f0 ff 35 4d 7f-ef 23 0d 3f 65 9d 8f bf   .*...5M..#.?e...
    0080 - 3f 39 76 17 59 1b 1a 9e-34 f9 8a 6f 87 5a dc 05   ?9v.Y...4..o.Z..
    0090 - 15 bb b0 12 c4 ba 7f 26-45 76 5a e5 87 f7 52 2f   .......&EvZ...R/
    00a0 - 38 ed c4 c3 ce fd 34 3a-27 6a d1 61 bf bd bc f8   8.....4:'j.a....
    00b0 - 9a 18 2d 52 85 9c 99 02-e2 d8 5e d6 8a 61 35 12   ..-R......^..a5.

    Start Time: 1511634130
    Timeout   : 300 (sec)
    Verify return code: 18 (self signed certificate)
---
closed
```