Cybersecurity Week 4 - Cryptography

Task 1

Perform two types of encryptions with different cyphers on “Text_file.txt” and compare outputs.

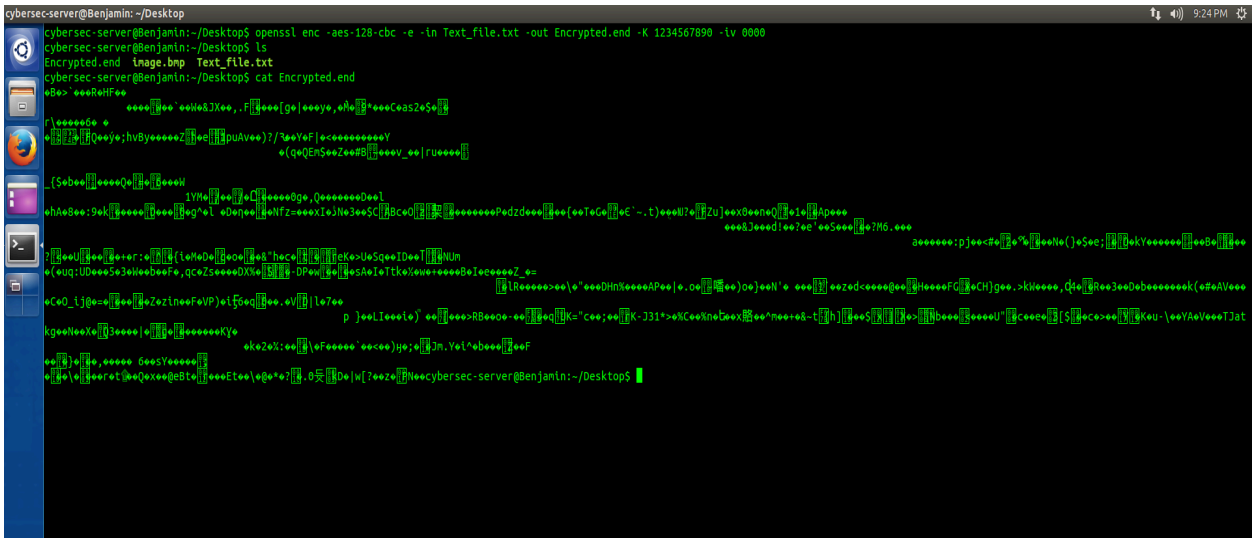
The command to Encrypt the files was

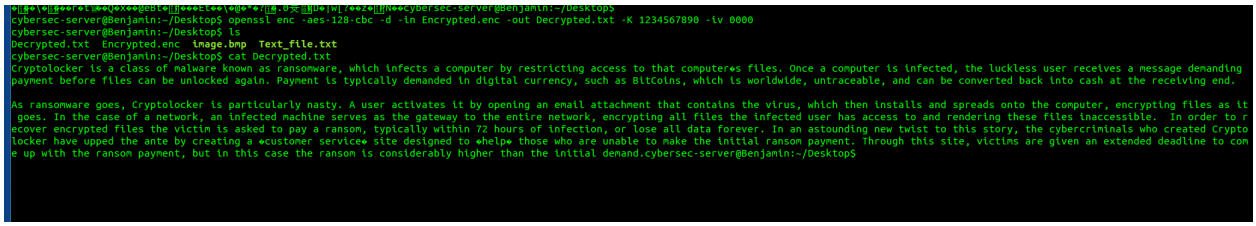
Openssl enc -aes-128-cbc -e -in Text_file.txt - Out Encrypted.enc -K 1234567890 - iv0000

In this command the -aes-128-cbc can be altered for different type of encryption methods while the -in/-out can be modified for different files.

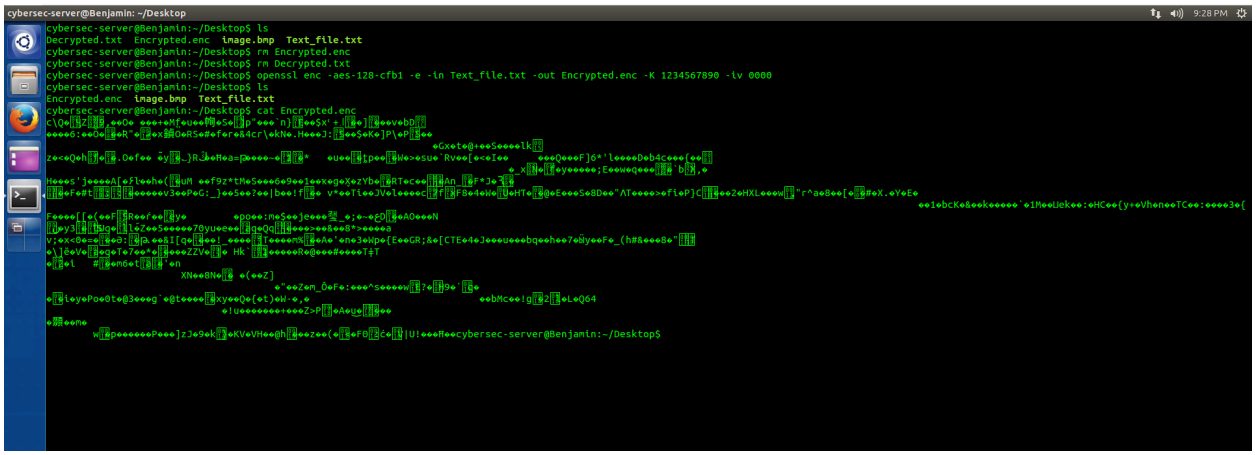
Decrpyting uses a similar command
(Openssl enc -aes-128-cbc -d -in Encrypted.end - Out Decrpyted.txt -K 1234567890 - iv0000)
Replacing -e (Encrypt) with -d (Decrypt) and targeting the encrypted file to be decrypted

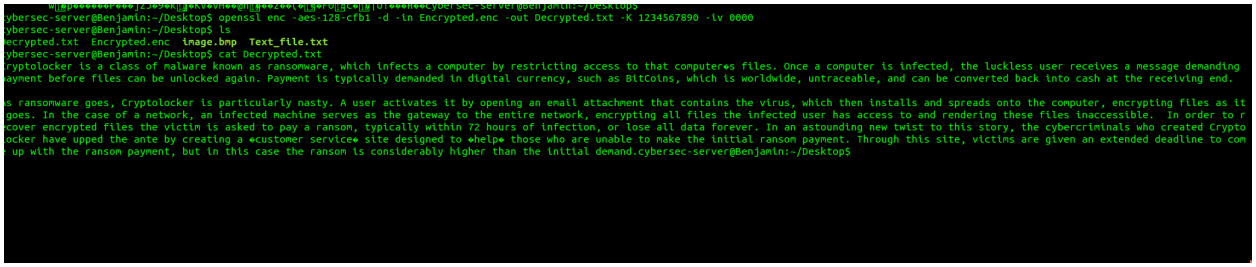
Encryption 1 with Decrpytion using aes-128-cbc





Encryption 2 with Decrpytion using aes-128-cfb1





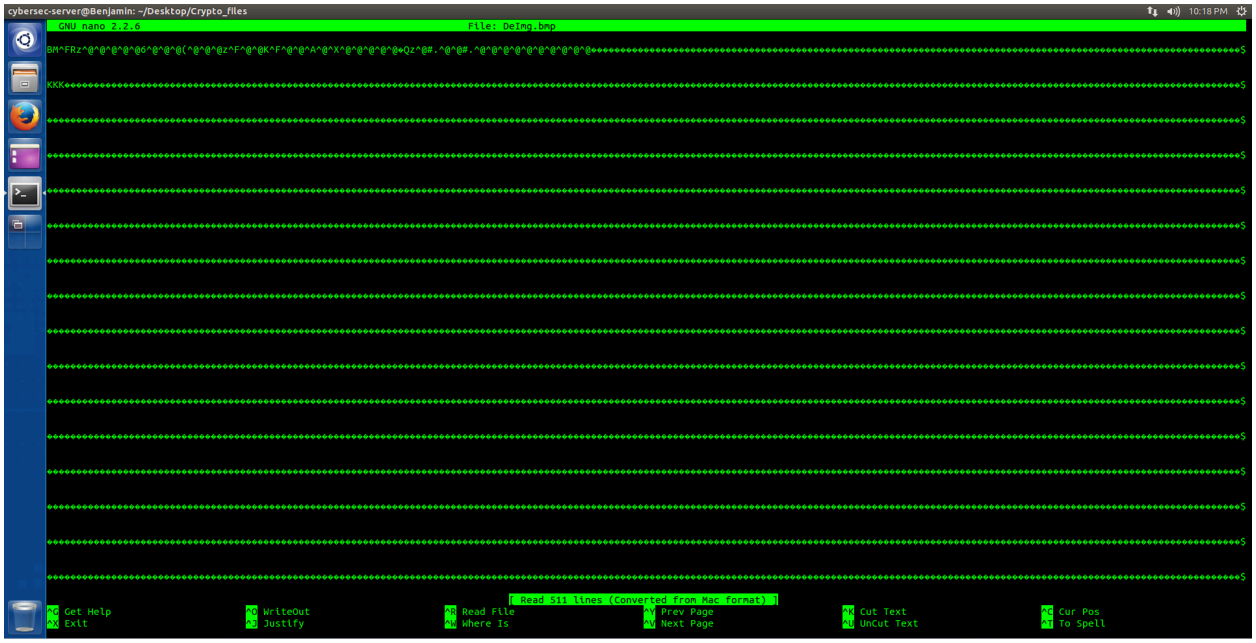
Question 2

Two types of Encrpytion on Image.bmp using different ciphers

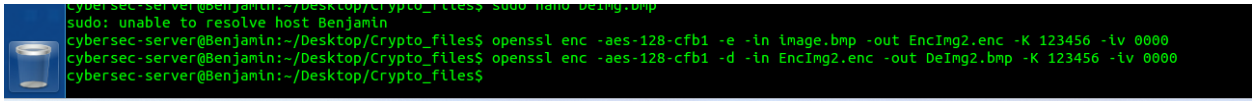
```
cybersec-server@Benjamin:~/Desktop/Crypto_files$ openssl enc -aes-128-cbc -e -in image.bmp -out EncImg.enc -K 123456 -iv 0000
cybersec-server@Benjamin:~/Desktop/Crypto_files$ openssl enc -aes-128-cbc -d -in EncImg.enc -out DeImg.bmp -K 123456 -iv 0000
```

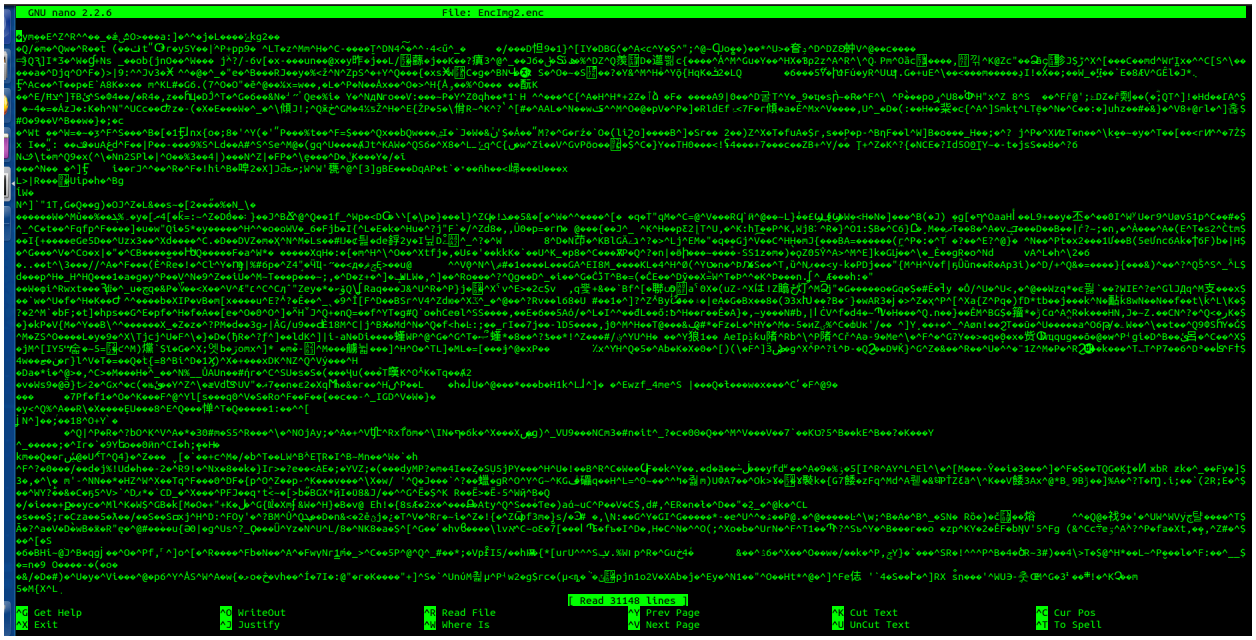
Encrypted

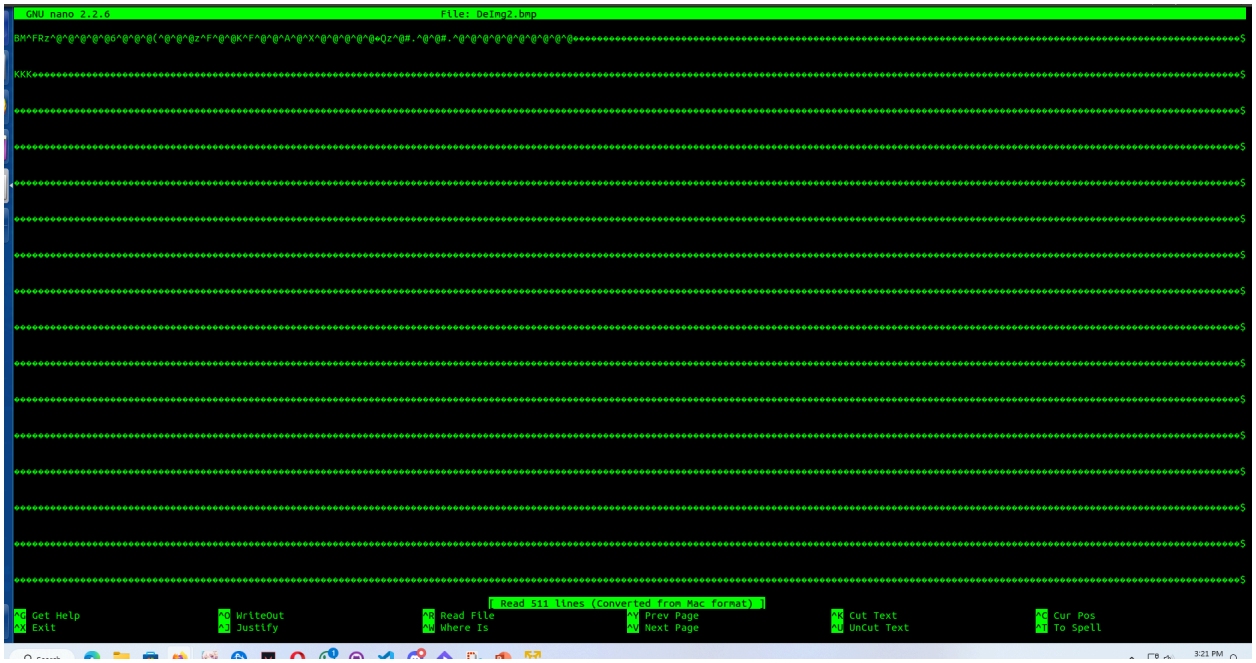
Decrypted



Encryption 2 with Decrpytion using aes-128-cfb1







Top: Encrypted , Bottom : Decrypted

For this task. Both Decryptred results should be the same as the original file with the only difference being the encrypted preview due to the different method of encryption applied

Task 2

1) Command To Generate Selfsigned Certificate

```
cybersec-server@Benjamin:~/Desktop/CA$ openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf
Generating a 2048 bit RSA private key
```

2) Information given for generating the 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) [AU]:Au
State or Province Name (full name) [Some-State]:NSW
Locality Name (eg, city) []:Sydney
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UTS
Organizational Unit Name (eg, section) []:FEIT
Common Name (e.g. server FQDN or YOUR name) []:cybersec.com.au
Email Address []:root@cybersec.com.au
cybersec-server@Benjamin:~/Desktop/CA$
```

Note: This file was remade with capitalisation so the information matches (Case sensitivity)

3) List of files After generated

```
cybersec-server@Benjamin:~/Desktop/CA$ ls
ca.crt  ca.key  certs  crl  index.txt  newcerts  openssl.cnf  serial
cybersec-server@Benjamin:~/Desktop/CA$
```

Task 3

1) Command used tto generate CSR (See screenshot Below)
2) Information used to generate CSR

```
cybersec-server@Benjamin:~/Desktop/CA$ openssl req -new -key server.key -out server.csr -config openssl.cnf
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:AU
State or Province Name (full name) [Some-State]:NSW
Locality Name (eg, city) []:Sydney
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UTS
Organizational Unit Name (eg, section) []:FEIT
Common Name (e.g. server FQDN or YOUR name) []:Cybersec.com.au
Email Address []:root@cybersec.com.au

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
cybersec-server@Benjamin:~/Desktop/CA$
```

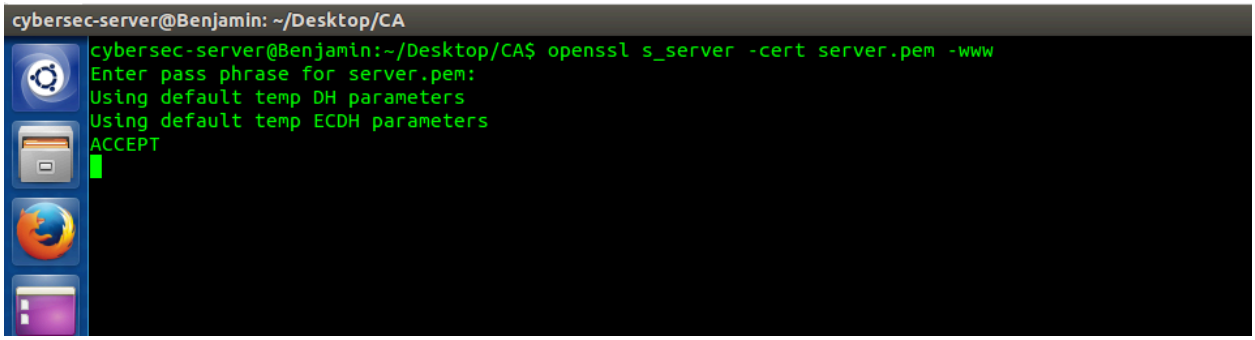
3) Files created until now

```
cybersec-server@Benjamin:~/Desktop/CA$ ls
ca.crt  ca.key  certs  crl  index.txt  newcerts  openssl.cnf  serial  server.csr  server.key
cybersec-server@Benjamin:~/Desktop/CA$
```

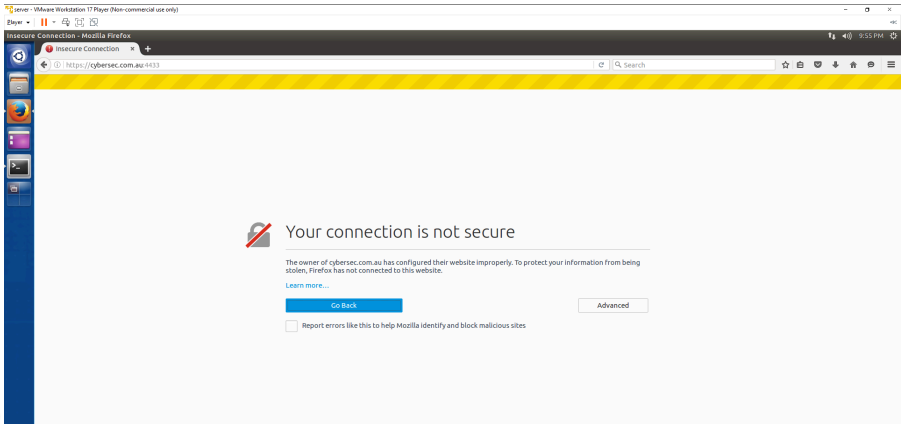
```
cybersec-server@Benjamin:~/Desktop/CA$ ls
ca.crt  ca.key  certs  crl  index.txt  newcerts  openssl.cnf  serial
cybersec-server@Benjamin:~/Desktop/CA$ open ssl genrsa -aes128 -out server.key 1024
open: invalid option -- 'a'
Usage: open [OPTIONS] -- command

This utility help you to start a program on a new virtual terminal (VT).

Options:
  -c, --console=NUM   use the given VT number;
  -e, --exec          execute the command, without forking;
  -f, --force         force opening a VT without checking;
  -l, --login         make the command a login shell;
  -u, --user          figure out the owner of the current VT;
  -s, --switch        switch to the new VT;
  -w, --wait          wait for command to complete;
  -v, --verbose       print a message for each action;
  -V, --version       print program version and exit;
  -h, --help          output a brief help message.

cybersec-server@Benjamin:~/Desktop/CA$ openssl genrsa -aes128 -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:
```

Task 4

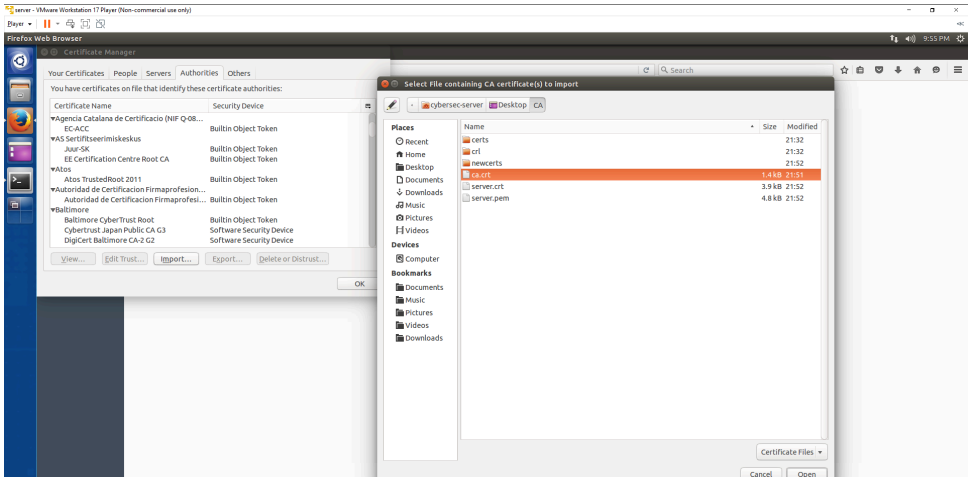
1) Launching the webserver using server.pem

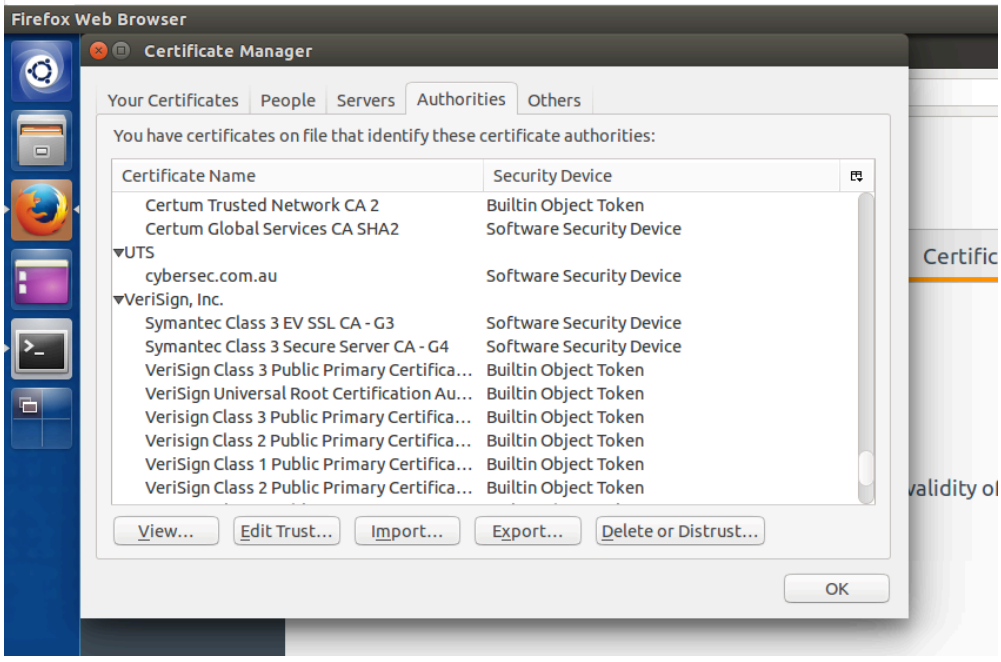


2) Screenshot of certificate manager



(Before Certificate)





3) Website Post certificate