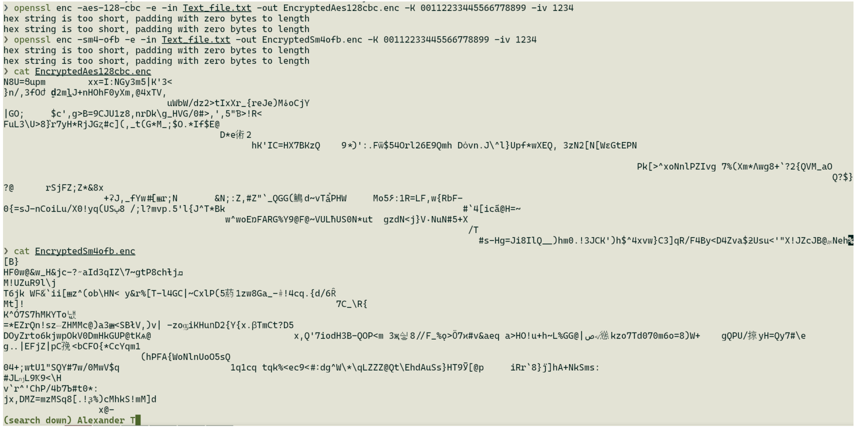
CSEC Week 04 Lab 03

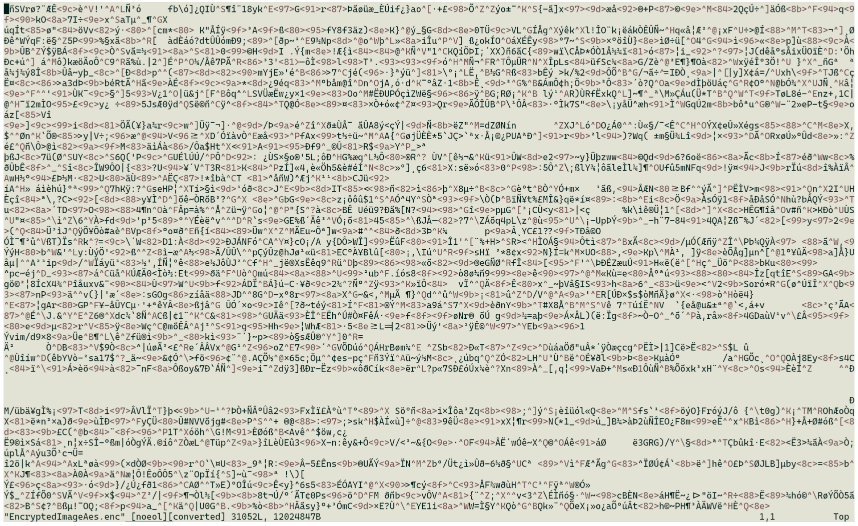
Task 1 - Basic encryption and decryption using OpenSSL

1. The two outputs are both encrypted and both look different. The commands I used were:
   `openssl enc -aes-128-cbc -e -in Text_file.txt -out EncryptedAes128cbc.enc -K 00112233445566778899 -iv 1234` and
   `openssl enc -sm4-ofb -e -in Text_file.txt -out EncryptedSm4ofb.enc -K 00112233445566778899 -iv 1234`
   Screenshot:



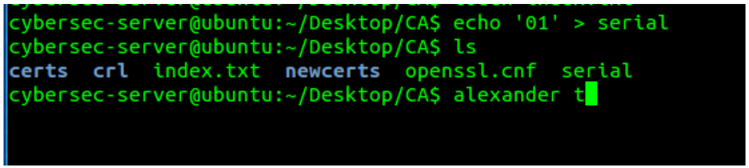
```
❯ openssl enc -aes-128-cbc -e -in Text_file.txt -out EncryptedAes128cbc.enc -K 00112233445566778899 -iv 1234
hex string is too short, padding with zero bytes to length
hex string is too short, padding with zero bytes to length
❯ openssl enc -sm4-ofb -e -in Text_file.txt -out EncryptedSm4ofb.enc -K 00112233445566778899 -iv 1234
hex string is too short, padding with zero bytes to length
hex string is too short, padding with zero bytes to length
❯ cat EncryptedAes128cbc.enc
N8U=8upm        xx=I:NGy3m5|K'3<
}n/,3fOd d2mlJ+nHOhF0yXm,@4xTV,
                               uWbW/dz2>tIxXr_{reJe)M&oCjY
|GO;     $c',g>B=9CJU1z8,nrDk\g_HVG/0#>,',5"B>!R<
FuL3\U>8}r7yH*RjJGz#c](,_t(G*M_;$O.*If$E@
                                         D*e術2
                                               hK'IC=HX7BKzQ    9*)':.Fw$54Orl26E9Qmh Dovn.J\^l}Upf*wXEQ, 3zN2[N[WεGtEPN

                                                                                                                        Pk[>^xoNnlPZIvg 7%(Xm*Λwg8+`?2{QVM_aO
                                                                                                                                                             Q?$}
?@      rSjFZ;Z*&8x
                   +?J,_fYw#[r;N       &N;:Z,#Z"`_QGG(鰆d~vTảPHW     Mo5ร:1R=LF,w{RbF-
0{=sJ-nCoiLu/X0!yq(US8 /;l?mvp.5'l{J^T*Bk                                                                #`4[icã@H=~
                                          w^woEDFARG%Y9@F@~VULħUS0N*ut  gzdN<j}V·NuN#5+X
                                                                                         /T
                                                                                           #s-Hg=Ji8IlQ__)hm0.!3JCK')h$^4xvw}C3]qR/F4By<D4Zva$2Usu<'"X!JZcJB@Neh%
❯ cat EncryptedSm4ofb.enc
[B}
HF0w@&w_H&jc-?~aId3qIZ\7~gtP8chłj
M!UZuR9l\j
T6jk WF&`ii[z^(ob\HN< y&r%[T-l4GC|~CxlP(5葯1zw8Ga_-#!4cq.{d/6R̂
Mt]!                                                                    7C_\R{
K^Ó7S7hMKYTo
=*EZrQn!sz~ZHMMc@)a3<SBłV,)v| -zoiKHunD2{Y{x.βTmCt?D5
DOyZrto6kjwpOkV0DmHkGUP@tK@                                 x,Q'7iodH3B-QOP<m 3ж8//F_%ϙ>Ö7ĸ#v&aeq a>HO!u+h~L%GG@|ص kzo7Td070m6o=8)W+    gQPU/掠yH=Qy7#\e
g..|EFjZ|pC<bCFO{*CcYqm1
                          (hPFA{WoNlnUoO5sQ
04+;wtU1"SQY#7w/0MwV$q                    1q1cq tqk%<ec9<#:dg^W\*\qLZZZ@Qt\EhdAuSs}HT9ȳ[@p     iRr`8}ǰ]hA+NkSms:
#JLL9K9<\H
v`r^'ChP/4b7b#t0*:
jx,DMZ=mzMSq8[.!%)cMhkS!mM]d
                 x@-
(search down) Alexander T
```

2. Exact same as above

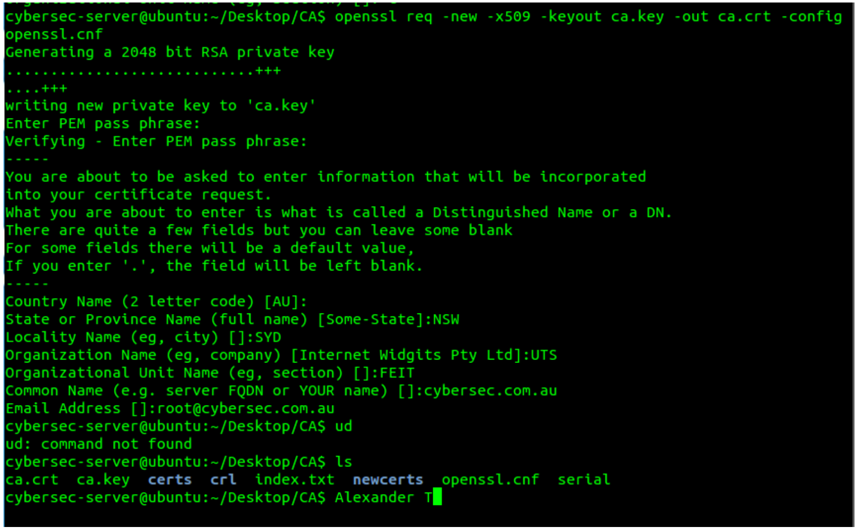


```
"EncryptedImageAes.enc" [noeol][converted] 31052L, 12024847B                                   1,1          Top
```

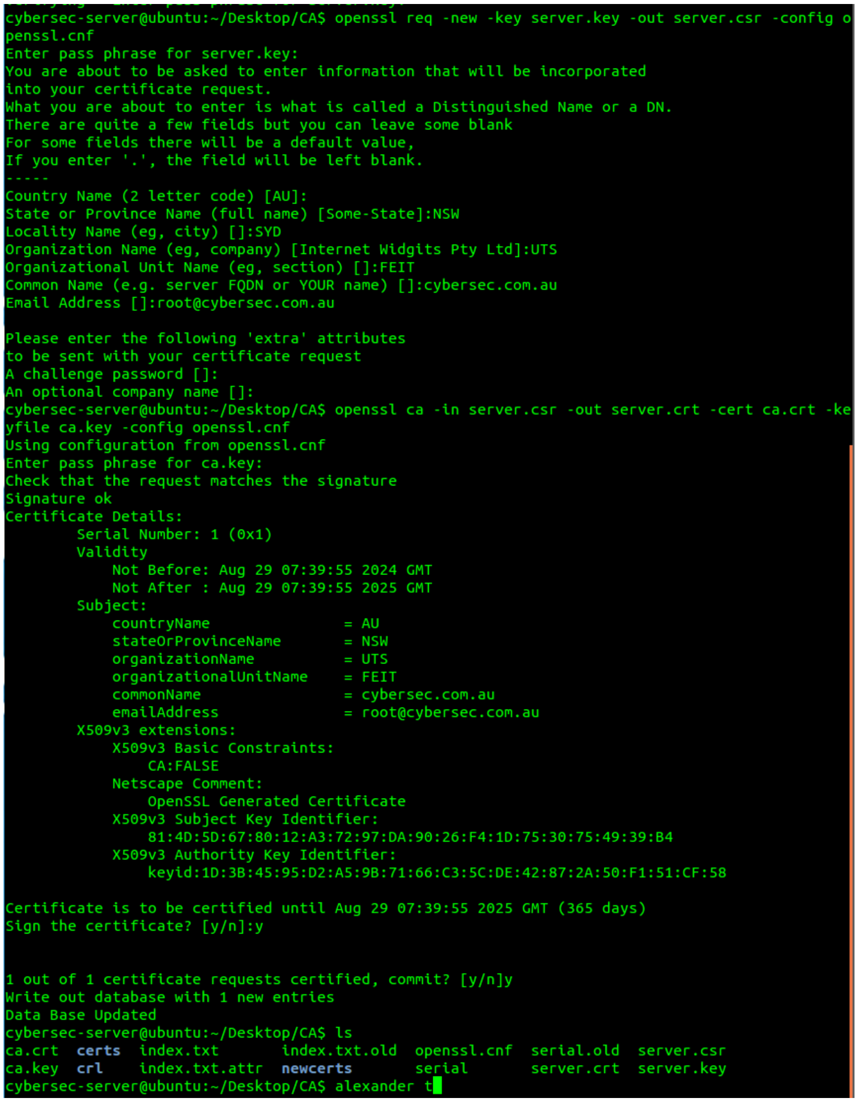
Task 2 - Become a Certificate Authority (CA)

1. 

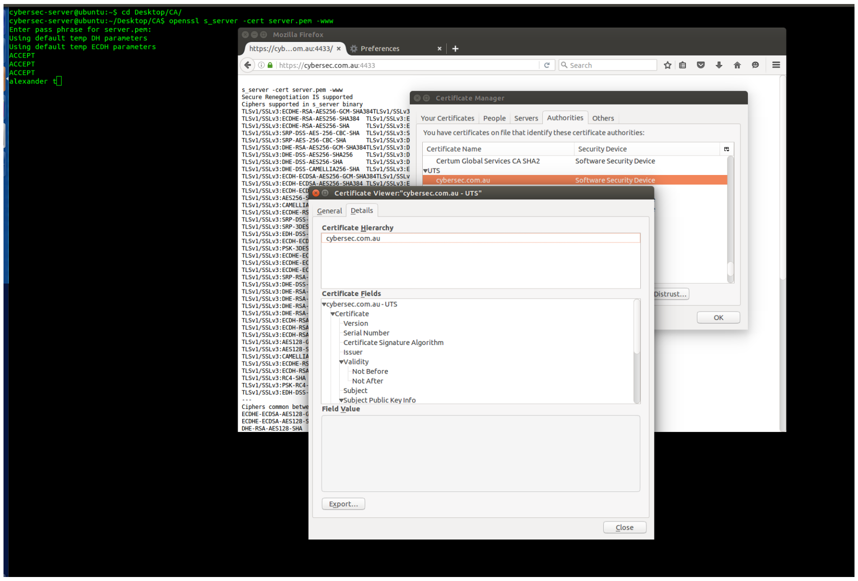
```
cybersec-server@ubuntu:~/Desktop/CA$ echo '01' > serial
cybersec-server@ubuntu:~/Desktop/CA$ ls
certs  crl  index.txt  newcerts  openssl.cnf  serial
cybersec-server@ubuntu:~/Desktop/CA$ alexander t
```

2. 

```
cybersec-server@ubuntu:~/Desktop/CA$ openssl req -new -x509 -keyout ca.key -out ca.crt -config
openssl.cnf
Generating a 2048 bit RSA private key
............................+++
....+++
writing new private key to 'ca.key'
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]:
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) []:cybersec.com.au
Email Address []:root@cybersec.com.au
cybersec-server@ubuntu:~/Desktop/CA$ ud
ud: command not found
cybersec-server@ubuntu:~/Desktop/CA$ ls
ca.crt  ca.key  certs  crl  index.txt  newcerts  openssl.cnf  serial
cybersec-server@ubuntu:~/Desktop/CA$ Alexander T
```

3. 

```
cybersec-server@ubuntu:~/Desktop/CA$ openssl req -new -key server.key -out server.csr -config o
penssl.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]:
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) []: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@ubuntu:~/Desktop/CA$ openssl ca -in server.csr -out server.crt -cert ca.crt -ke
yfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Aug 29 07:39:55 2024 GMT
            Not After : Aug 29 07:39:55 2025 GMT
        Subject:
            countryName               = AU
            stateOrProvinceName       = NSW
            organizationName          = UTS
            organizationalUnitName    = FEIT
            commonName                = cybersec.com.au
            emailAddress              = root@cybersec.com.au
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                81:4D:5D:67:80:12:A3:72:97:DA:90:26:F4:1D:75:30:75:49:39:B4
            X509v3 Authority Key Identifier:
                keyid:1D:3B:45:95:D2:A5:9B:71:66:C3:5C:DE:42:87:2A:50:F1:51:CF:58

Certificate is to be certified until Aug 29 07:39:55 2025 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
cybersec-server@ubuntu:~/Desktop/CA$ ls
ca.crt  certs  index.txt       index.txt.old  openssl.cnf  serial.old  server.csr
ca.key  crl    index.txt.attr  newcerts       serial       server.crt  server.key
cybersec-server@ubuntu:~/Desktop/CA$ alexander t
```

4. 

```
cybersec-server@ubuntu:~$ cd Desktop/CA/
cybersec-server@ubuntu:~/Desktop/CA$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Using default temp DH parameters
Using default temp ECDH parameters
ACCEPT
ACCEPT
ACCEPT
alexander t
```

https://cybersec.com.au:4433

```
s_server -cert server.pem -www
Secure Renegotiation IS supported
Ciphers supported in s_server binary
TLSv1/SSLv3:ECDHE-RSA-AES256-GCM-SHA384TLSv1/SSLv3
TLSv1/SSLv3:ECDHE-RSA-AES256-SHA384  TLSv1/SSLv3:E
TLSv1/SSLv3:ECDHE-RSA-AES256-SHA     TLSv1/SSLv3:E
TLSv1/SSLv3:SRP-DSS-AES-256-CBC-SHA  TLSv1/SSLv3:S
TLSv1/SSLv3:SRP-AES-256-CBC-SHA      TLSv1/SSLv3:D
TLSv1/SSLv3:DHE-RSA-AES256-GCM-SHA384TLSv1/SSLv3:D
TLSv1/SSLv3:DHE-DSS-AES256-SHA256    TLSv1/SSLv3:D
TLSv1/SSLv3:DHE-DSS-AES256-SHA       TLSv1/SSLv3:D
TLSv1/SSLv3:DHE-DSS-CAMELLIA256-SHA  TLSv1/SSLv3:E
TLSv1/SSLv3:ECDH-ECDSA-AES256-GCM-SHA384TLSv1/SSLv
TLSv1/SSLv3:ECDH-ECDSA-AES256-SHA384 TLSv1/SSLv3:E
TLSv1/SSLv3:ECDH-ECD
TLSv1/SSLv3:AES256-S
TLSv1/SSLv3:CAMELLIA
TLSv1/SSLv3:ECDHE-RS
TLSv1/SSLv3:SRP-DSS-
TLSv1/SSLv3:SRP-3DES
TLSv1/SSLv3:EDH-DSS-
TLSv1/SSLv3:ECDH-ECD
TLSv1/SSLv3:PSK-3DES
TLSv1/SSLv3:ECDHE-EC
TLSv1/SSLv3:ECDHE-EC
TLSv1/SSLv3:ECDHE-EC
TLSv1/SSLv3:SRP-RSA-
TLSv1/SSLv3:DHE-DSS-
TLSv1/SSLv3:DHE-RSA-
TLSv1/SSLv3:DHE-RSA-
TLSv1/SSLv3:DHE-RSA-
TLSv1/SSLv3:DHE-RSA-
TLSv1/SSLv3:ECDH-RSA
TLSv1/SSLv3:ECDH-RSA
TLSv1/SSLv3:ECDH-RSA
TLSv1/SSLv3:AES128-G
TLSv1/SSLv3:AES128-S
TLSv1/SSLv3:CAMELLIA
TLSv1/SSLv3:ECDHE-RS
TLSv1/SSLv3:ECDH-RSA
TLSv1/SSLv3:RC4-SHA
TLSv1/SSLv3:PSK-RC4-
TLSv1/SSLv3:EDH-DSS-
---
Ciphers common betwe
ECDHE-ECDSA-AES128-G
ECDHE-ECDSA-AES128-S
DHE-RSA-AES128-SHA
```

Certificate Manager

You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
Certum Global Services CA SHA2	Software Security Device
▾UTS	
cybersec.com.au	Software Security Device

Certificate Viewer:"cybersec.com.au - UTS"

Certificate Hierarchy

cybersec.com.au

Certificate Fields

```
▾cybersec.com.au - UTS
  ▾Certificate
     Version
     Serial Number
     Certificate Signature Algorithm
     Issuer
    ▾Validity
       Not Before
       Not After
     Subject
    ▾Subject Public Key Info
```

Field Value