

FILE ENCRYPTION: OPEN SSL

```
aciadmin@acialma:~/file_encryption
[aciadmin@acialma ~]$ mkdir file_encryption
[aciadmin@acialma ~]$ cd file_encryption/
[aciadmin@acialma file_encryption]$ echo "important stuff here" > myStuff.txt
[aciadmin@acialma file_encryption]$ openssl -help
help:

Standard commands
asniparse      ca          ciphers      cmp          dgst
cms            crl          crl2pkcs7    ec           dgst
dhparam        dsa          dsaparam     ec           dgst
ecparam        enc          engine       errstr       errstr
fipsinstall    gensa       genpkey      genrsa      genrsa
help           info        kdf          list         list
mac            nseq        ocsf         passwd       passwd
pkcs12         pkcs7       pkcs8        pkey         pkey
pkeyparam      pkeyutl     prime        rand         rand
rehash         req         rsa          rsautl       rsautl
s_client       s_server    s_time       sess_id      sess_id
smime          speed       spkac        srp          srp
storeutl       ts          verify       version      version
x509

Message Digest commands (see the 'dgst' command for more details)
blake2b512     blake2s256  md2          md4
```

```
aciadmin@acialma:~/file_encryption
idea-ofb      rc2          rc2-40-cbc   rc2-64-cbc
rc2-cbc       rc2-cfb     rc2-ecb      rc2-ofb
rc4           rc4-40      rc5          rc5-cbc
rc5-cfb       rc5-ecb     rc5-ofb      seed
seed-cbc      seed-cfb    seed-ecb     seed-ofb
zlib

[aciadmin@acialma file_encryption]$ openssl enc -aes-128-cbc -in myStuff.txt -out myEncStuff.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.
[aciadmin@acialma file_encryption]$ ls
myEncStuff.txt  myStuff.txt
[aciadmin@acialma file_encryption]$ cat myEncStuff.txt
[aciadmin@acialma file_encryption]$ openssl enc -d -aes-128-cbc -in myEncStuff.txt -out myDecStuff.txt
enter AES-128-CBC decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[aciadmin@acialma file_encryption]$ ls
myDecStuff.txt  myEncStuff.txt  myStuff.txt
[aciadmin@acialma file_encryption]$ cat myDecStuff.txt
important stuff here
[aciadmin@acialma file_encryption]$
```

```
aciadmin@acialma:~/file_encryption
idea-ofb      rc2          rc2-40-cbc   rc2-64-cbc
rc2-cbc       rc2-cfb     rc2-ecb      rc2-ofb
rc4           rc4-40      rc5          rc5-cbc
rc5-cfb       rc5-ecb     rc5-ofb      seed
seed-cbc      seed-cfb    seed-ecb     seed-ofb
zlib

[aciadmin@acialma file_encryption]$ openssl enc -aes-128-cbc -in myStuff.txt -out myEncStuff.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.
[aciadmin@acialma file_encryption]$ ls
myEncStuff.txt  myStuff.txt
[aciadmin@acialma file_encryption]$ cat myEncStuff.txt
[aciadmin@acialma file_encryption]$ openssl enc -d -aes-128-cbc -in myEncStuff.txt -out myDecStuff.txt
enter AES-128-CBC decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
[aciadmin@acialma file_encryption]$ ls
myDecStuff.txt  myEncStuff.txt  myStuff.txt
[aciadmin@acialma file_encryption]$ cat myDecStuff.txt
important stuff here
[aciadmin@acialma file_encryption]$
```