Week 2

A)

bce0408@15BCE0408:~$ echo 'for your eye only' > fyi.txt

bce0408@15BCE0408:~$ openssl enc -aes-256-cbc -salt -in fyi.txt -out fyi.enc

enter aes-256-cbc encryption password:

Verifying - enter aes-256-cbc encryption password:

bce0408@15BCE0408:~$ openssl enc -a -md md5 -nosalt -in fyi.txt -out fyimd5.ent

bce0408@15BCE0408:~$ openssl enc -a -md sha1 -nosalt -in yi.txt -out fyisha1.entyi.txt: No such file or directory

140605113067160:error:02001002:system library:fopen:No such file or directory:bss\_file.c:398:fopen('yi.txt','r')

140605113067160:error:20074002:BIO routines:FILE\_CTRL:system lib:bss\_file.c:400:

bce0408@15BCE0408:~$ openssl enc -a -md sha1 -nosalt -in fyi.txt -out fyisha1.ent

bce0408@15BCE0408:~$ openssl enc -a -nosalt -in fyi.txt -out fyi.ent

bce0408@15BCE0408:~$ cat fyi.enc

Salted\_\_�T�˞�t7��Ҏ`x;2U�=�%‑���,��

v���J�8�+bce0408@15BCE0408:~$ openssl enc -d -aes-256-cbc -salt -in fyi.enc -out fyi.dec

enter aes-256-cbc decryption password:

bce0408@15BCE0408:~$ cat fyi.dec

for your eye only

B)

bce0408@15BCE0408:~$ time openssl enc -aes-256-cbc -salt -pass pass:'fyi00' -in connect.zip -out connect.zip.enc2

real 0m0.018s

user 0m0.012s

sys 0m0.004s

bce0408@15BCE0408:~$ time openssl enc -aes-256-cbc -salt -pass pass:'fyi00' -in connect.zip -out connect.zip.enc3

real 0m0.023s

user 0m0.016s

sys 0m0.004s

bce0408@15BCE0408:~$ time openssl enc -d -aes-256-cbc -salt -pass pass:'fyi00' -in connect.zip.enc2 -out connect.zip.dec2

real 0m0.009s

user 0m0.004s

sys 0m0.004s

bce0408@15BCE0408:~$ time openssl enc -d -aes-256-cbc -salt -pass pass:'fyi00' -in connect.zip.enc3 -out connect.zip.dec3

real 0m0.010s

user 0m0.004s

sys 0m0.004s

Week 3

A)

bce0408@15BCE0408:~$ bc

bc 1.06.95

Copyright 1991-1994, 1997, 1998, 2000, 2004, 2006 Free Software Foundation, Inc.

This is free software with ABSOLUTELY NO WARRANTY.

For details type `warranty'.

17^5%53

40

17^7%53

6

40^7%53

38

6^5%53

38

B)

bce0408@15BCE0408:~$ echo 'U2FsdGVkX19jmwScyxpj2tnRIm1UKK0WJVTv7PNXAE4=' > proj2bmsg.ent

bce0408@15BCE0408:~$ openssl enc -d -aes-128-ecb -a -pass pass:'38' -in proj2bmsg.ent -out proj2bmsg.dec

bce0408@15BCE0408:~$ cat proj2bmsg.dec

I love you!

Final Output:

I love you!