Microsoft Windows [Version 10.0.18363.1316]

(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Vishal>openssl

OpenSSL> exit

C:\Users\Vishal>cd..

C:\Users>cd..

C:\>cd C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem\CSS\Openssl

C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem\CSS\Openssl>openssl

OpenSSL> enc -aes-256-ecb -a -salt -in Task1.txt -out Task1\_Enc.txt

enter aes-256-ecb encryption password:

Verifying - enter aes-256-ecb encryption password:

OpenSSL> enc -aes-128-cbc -e -in Task1.txt -out Task1\_aes\_cbc.txt -k 1234abcd -iv 1234567890

OpenSSL> enc -aes-128-cfb -e -in Task1.txt -out Task1\_aes\_cfb.txt -k 1234abcd -iv 1234567890

OpenSSL> enc -bf-cbc -e -in Task1.txt -out Task1\_bf\_cbc.txt -k 1234abcd -iv 1234567890

OpenSSL> enc -bf-cbc -d -in Task1\_aes\_cbc.txt -out Task1\_dec\_cbc.txt -k 1234abcd -iv 1234567890

bad decrypt

9128:error:06065064:digital envelope routines:EVP\_DecryptFinal\_ex:bad decrypt:evp\_enc.c:529:

error in enc

OpenSSL> dec -bf-cbc -d -in Task1\_aes\_cbc.txt -out Task1\_dec\_cbc.txt -k 1234abcd -iv 1234567890

openssl:Error: 'dec' is an invalid command.

Standard commands

asn1parse ca ciphers cms

crl crl2pkcs7 dgst dh

dhparam dsa dsaparam ec

ecparam enc engine errstr

gendh gendsa genpkey genrsa

nseq ocsp passwd pkcs12

pkcs7 pkcs8 pkey pkeyparam

pkeyutl prime rand req

rsa rsautl s\_client s\_server

s\_time sess\_id smime speed

spkac srp ts verify

version x509

Message Digest commands (see the `dgst' command for more details)

md4 md5 mdc2 rmd160

sha sha1

Cipher commands (see the `enc' command for more details)

aes-128-cbc aes-128-ecb aes-192-cbc aes-192-ecb

aes-256-cbc aes-256-ecb base64 bf

bf-cbc bf-cfb bf-ecb bf-ofb

camellia-128-cbc camellia-128-ecb camellia-192-cbc camellia-192-ecb

camellia-256-cbc camellia-256-ecb cast cast-cbc

cast5-cbc cast5-cfb cast5-ecb cast5-ofb

des des-cbc des-cfb des-ecb

des-ede des-ede-cbc des-ede-cfb des-ede-ofb

des-ede3 des-ede3-cbc des-ede3-cfb des-ede3-ofb

des-ofb des3 desx idea

idea-cbc idea-cfb idea-ecb idea-ofb

rc2 rc2-40-cbc rc2-64-cbc rc2-cbc

rc2-cfb rc2-ecb rc2-ofb rc4

rc4-40 seed seed-cbc seed-cfb

seed-ecb seed-ofb zlib

OpenSSL> enc -aes-128-cbc -d -in Task1\_aes\_cbc.txt -out Task1\_aes\_cbc\_dec -k 1234abcd -iv 1234567890

OpenSSL> enc -aes-128-cbc -d -in Task1\_aes\_cbc.txt -out Task1\_aes\_cbc\_dec.txt -k 1234abcd -iv 1234567890

OpenSSL> enc -aes-128-cfb -d -in Task1\_aes\_cfb.txt -out Task1\_aes\_cfb\_dec.txt -k 1234abcd -iv 1234567890

OpenSSL> enc -bf-cbc -e -in Task1\_bf\_cbc.txt -out Task1\_bf\_cbc\_dec.txt -k 1234abcd -iv 1234567890

OpenSSL> enc -bf-cbc -d -in Task1\_bf\_cbc.txt -out Task1\_bf\_cbc\_dec.txt -k 1234abcd -iv 1234567890

OpenSSL> enc -aes-128-ecb -e -in original.bmp -out original\_enc.bmp -k 1234abcd -iv 1234567890

warning: iv not use by this cipher

OpenSSL> enc -aes-128-ecb -e -in original.bmp -out original\_enc.bmp -k 1234abcd

OpenSSL> enc -aes-128-cbc -e -in original.bmp -out original\_cbc.bmp -k 1234abcd

OpenSSL> enc -aes-128-ecb -e -in original.bmp -out original\_ecb\_enc.bmp -k 1234abcd

OpenSSL> enc -aes-128-cbc -e -in original.bmp -out original\_cbc\_enc.bmp -k 1234abcd

OpenSSL> enc -aes-128-cbc -e -in original\_cbc\_enc\_ghx.bmp -out original\_cbc\_enc\_ghx\_enc.bmp -k 1234abcd

original\_cbc\_enc\_ghx.bmp: No such file or directory

9128:error:02001002:system library:fopen:No such file or directory:bss\_file.c:402:fopen('original\_cbc\_enc\_ghx.bmp','rb')

9128:error:20074002:BIO routines:FILE\_CTRL:system lib:bss\_file.c:404:

error in enc

OpenSSL> enc -aes-128-cbc -e -in original\_ecb\_enc\_ghx.bmp -out original\_ecb\_enc\_ghx\_enc.bmp -k 1234abcd

OpenSSL> enc -aes-128-ecb -e -in original.bmp -out original\_ecb\_enc.bmp -k 1234abcd

OpenSSL> enc -aes-128-cbc -e -in original.bmp -out original\_cbc\_enc.bmp -k 1234abcd

OpenSSL> enc -aes-128-ecb -e -in original.bmp -out original\_enc.bmp -k 1234abcd -iv 1234567890

warning: iv not use by this cipher

OpenSSL> enc -aes-128-cbc -e -in original.bmp -out original\_enc.bmp -k 1234abcd -iv 1234567890

OpenSSL> exit

C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem\CSS\Openssl>cd..

C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem\CSS>cd..

C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem>cd..

C:\Users\Vishal\Desktop\Vishal\Third Year BTECH>cd..

C:\Users\Vishal\Desktop\Vishal>cd..

C:\Users\Vishal\Desktop>cd..

C:\Users\Vishal>cd..

C:\Users>cd..

C:\>cd C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem\CSS\Openssl\Task\_3

C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem\CSS\Openssl\Task\_3>openssl

OpenSSL> enc -aes-128-ecb -e -in Task3.txt -out Task3\_aes\_ecb.txt -k 1234abcd -iv 1234567890

warning: iv not use by this cipher

OpenSSL> enc -aes-128-ecb -e -in Task3.txt -out Task3\_aes\_ecb.txt -k 1234abcd

OpenSSL> enc -aes-128-ecb -d -in Task3\_aes\_ecb.txt -out Task3\_aes\_ecb\_dec.txt -k 1234abcd

bad decrypt

1764:error:0606506D:digital envelope routines:EVP\_DecryptFinal\_ex:wrong final block length:evp\_enc.c:518:

error in enc

OpenSSL> enc -aes-128-cbc -e -in light.bmp -out light\_enc.bmp -k 1234abcd -iv 1234567890

light.bmp: No such file or directory

1764:error:02001002:system library:fopen:No such file or directory:bss\_file.c:402:fopen('light.bmp','rb')

1764:error:20074002:BIO routines:FILE\_CTRL:system lib:bss\_file.c:404:

error in enc

OpenSSL> exit

C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem\CSS\Openssl\Task\_3>cd..

C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem\CSS\Openssl>opensll

'opensll' is not recognized as an internal or external command,

operable program or batch file.

C:\Users\Vishal\Desktop\Vishal\Third Year BTECH\Third Year 6th Sem\CSS\Openssl>openssl

OpenSSL> enc -aes-128-cbc -e -in light.bmp -out light\_enc.bmp -k 1234abcd -iv 1234567890

OpenSSL>