#Task 01

Commands:

1. openssl enc -aes-128-cbc -e -in plain.txt -out cipher_cbc.bin -K 00112233445566778889aabbccddeeff -iv 0102030405060708
2. openssl enc -aes-128-cbc -d -in cipher_cbc.bin -out decipher_cbc.txt -K 00112233445566778889aabbccddeeff -iv 0102030405060708
3. openssl enc -aes-128-cfb -e -in plain.txt -out cipher_cfb.bin -K 00112233445566778889aabbccddeeff -iv 0102030405060708
4. openssl enc -aes-128-cfb -d -in cipher_cfb.bin -out dicipher_cfb.txt -K 00112233445566778889aabbccddeeff -iv 0102030405060708
5. openssl enc -bf-cbc -e -in plain.txt -out cipher_bf_cbc.bin -K 00112233445566778889aabbccddeeff -iv 0102030405060708
6. openssl enc -bf-cbc -d -in cipher_bf_cbc.bin -out dicipher_bf_cbc.txt -K 00112233445566778889aabbccddeeff -iv 0102030405060708

#Task 02

1. openssl enc -aes-128-cbc -e -in image.jpg -out cipher_image.bin -K 00112233445566778889aabbccddeeff -iv 0102030405060708

#Task 03

1. ECB
   ï»¿Our concept o,ºĐ€·b#§*×Ç} #Wth the creation of the universe. Therefore if the laws of nature created the universe, these laws must have existed prior to time.
2. CBC
   ï»¿Our concept oäCL˜Ç’ &uP
   W…jröÈth the creati/n of the universe. Therefore if the laws of nature created the universe, these laws must have existed prior to time.
3. CFB
   ï»¿Our concept of time begins!wiÄŠZ ‘[û8’ ÏJ0<of the universe. Therefore if the laws of nature created the universe, these laws must have existed prior to time.
4. OFB
   ï»¿Our concept of time begins with the creation of the universe. Therefore if the laws of nature created the universe, these laws must have existed prior to time.

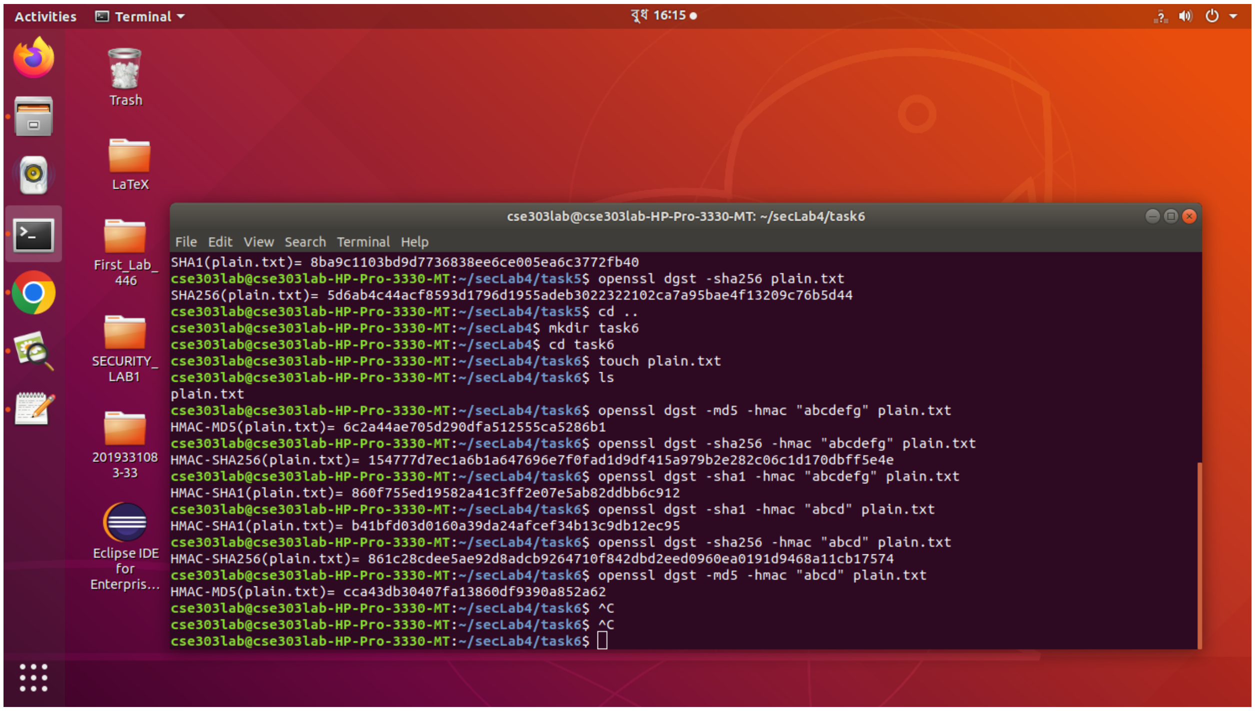
#Task4

ECB, CBC need padding.

#Task 5

1. MD5(plain.txt)= 61503a6aafaebb3b59204cb4b5609947
2. SHA1(plain.txt)= 8ba9c1103bd9d7736838ee6ce005ea6c3772fb40
3. SHA256(plain.txt)=5d6ab4c44acf8593d1796d1955adeb3022322102ca7a95bae4f13209c76b5d44

#Task 6



```
SHA1(plain.txt)= 8ba9c1103bd9d7736838ee6ce005ea6c3772fb40
cse303lab@cse303lab-HP-Pro-3330-MT:~/secLab4/task5$ openssl dgst -sha256 plain.txt
SHA256(plain.txt)= 5d6ab4c44acf8593d1796d1955adeb3022322102ca7a95bae4f13209c76b5d44
cse303lab@cse303lab-HP-Pro-3330-MT:~/secLab4/task5$ cd ..
cse303lab@cse303lab-HP-Pro-3330-MT:~/secLab4$ mkdir task6
cse303lab@cse303lab-HP-Pro-3330-MT:~/secLab4$ cd task6
cse303lab@cse303lab-HP-Pro-3330-MT:~/secLab4/task6$ touch plain.txt
cse303lab@cse303lab-HP-Pro-3330-MT:~/secLab4/task6$ ls
plain.txt
cse303lab@cse303lab-HP-Pro-3330-MT:~/secLab4/task6$ openssl dgst -md5 -hmac "abcdefg" plain.txt
HMAC-MD5(plain.txt)= 6c2a44ae705d290dfa512555ca5286b1
cse303lab@cse303lab-HP-Pro-3330-MT:~/secLab4/task6$ openssl dgst -sha256 -hmac "abcdefg" plain.txt
HMAC-SHA256(plain.txt)= 154777d7ec1a6b1a647696e7f0fad1d9df415a979b2e282c06c1d170dbff5e4e
cse303lab@cse303lab-HP-Pro-3330-MT:~/secLab4/task6$ openssl dgst -sha1 -hmac "abcdefg" plain.txt
HMAC-SHA1(plain.txt)= 860f755ed19582a41c3ff2e07e5ab82ddbb6c912
cse303lab@cse303lab-HP-Pro-3330-MT:~/secLab4/task6$ openssl dgst -sha1 -hmac "abcd" plain.txt
HMAC-SHA1(plain.txt)= b41bfd03d0160a39da24afcef34b13c9db12ec95
cse303lab@cse303lab-HP-Pro-3330-MT:~/secLab4/task6$ openssl dgst -sha256 -hmac "abcd" plain.txt
HMAC-SHA256(plain.txt)= 861c28cdee5ae92d8adcb9264710f842dbd2eed0960ea0191d9468a11cb17574
cse303lab@cse303lab-HP-Pro-3330-MT:~/secLab4/task6$ openssl dgst -md5 -hmac "abcd" plain.txt
HMAC-MD5(plain.txt)= cca43db30407fa13860df9390a852a62
cse303lab@cse303lab-HP-Pro-3330-MT:~/secLab4/task6$ ^C
cse303lab@cse303lab-HP-Pro-3330-MT:~/secLab4/task6$ ^C
cse303lab@cse303lab-HP-Pro-3330-MT:~/secLab4/task6$ 
```

Key length doesn’t matter.

#Task 07

MD5:

1. HMAC-MD5(plain.txt)= cca43db30407fa13860df9390a852a62
2. HMAC-MD5(plain.txt)= f37f04aa813040bb0969bd940330fcb5

HMAC:

3. HMAC-SHA256(plain2.txt)=861c28cdee5ae92d8adcb9264710f842dbd2eed0960ea0191d9468a11cb17574
4. HMAC-SHA256(plain2.txt)=5e05405062a3f14737fb6bed6429250175291809d2e04ea8d599065ecea553bf