Question 01: What is the latest stable version of OpenSSL? Which version is installed on your machine?

(Hint: You can find the latest stable version from the Downloads page in OpenSSL web site.)

3.0.11  
  
Question 02: What is the command you would use to display all of the cyphers that are implemented in

OpenSSL?  
openssl list -cipher-commands  
  
Question 03: As you can see, -aes-192-cbc is one of the ciphers. What does the number 192 mean that is

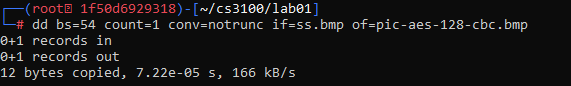
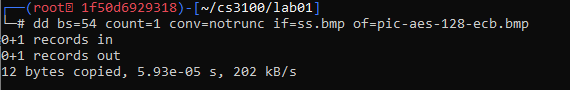
used in the name of the cipher?  
length of the bites  
  
Question 04: What ciphers did you try?  
-aes-192-cbc

-aes-128-cbc

-aes-256-cbc

Question 05: Could the plain text be correctly recovered from the corresponding cipher text? If not,

explain why.

I was able to decrypt the files after encypting them using openssl enc  
  
Question 06: Take screenshots that show the encrypted pictures (both ECB and CBC modes) and attach  
them here. Indicate the operation mode that is used to encrypt the file, respectively.

Question 07: Please explain your observations of the results for the previous question. More specifically,

please argue the ECB mode against the CBC mode. For example, which operation mode can more

completely hide the original information and is more secure? Explain your argument.  
  
ECB can show a same pattern due to the block of ciphertext if the image has same pattern while the CBC model uses XORed with each plaintext blocks  
  
Question 08: Please report which modes have padding, which modes do not have padding. For those

modes that do not have paddings, please explain why they do not need padding?  
ECB and CBC has padding due to the last block needing to be filled while CFB and OFB does not need to have padding due to the way the each encrypts.  
  
Question 09: Which of the cipher text files are padded? Which are not padded?   
  
f1 was not but f2 and f3 was padded

Question 10: Please report what are the padded values in hex decimal format for f1.recovered,  
f2.recovered, f3.recovered, respectively?

F3.recover  
A screenshot of a computer

Description automatically generated  
  
f2.recover  
A screenshot of a computer

Description automatically generated  
  
f1.recover  
A screenshot of a computer

Description automatically generated

Which padding string, PKCS#5 or PKCS#7, is used in OpenSSL?

Openssl uses pkcs#7 as diffence between 5 and 7 is the block size of 8 byte and 255 byte