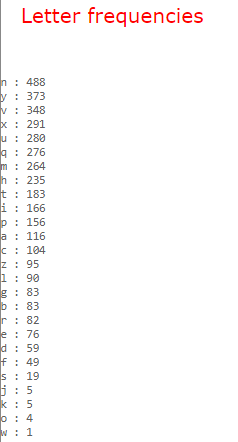
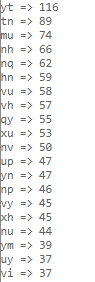
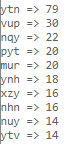
Task 1: Frequency Analysis Against Monoalphabetic Substitution Cipher



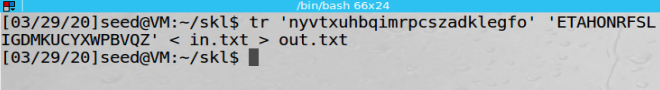
Top 20 Bigram Frequencies



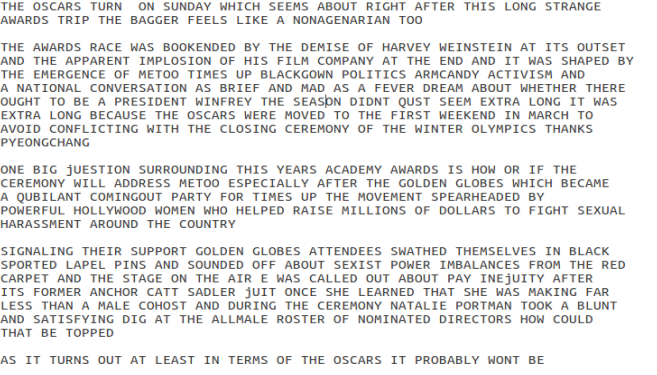
Top 10 Trigram Frequencies

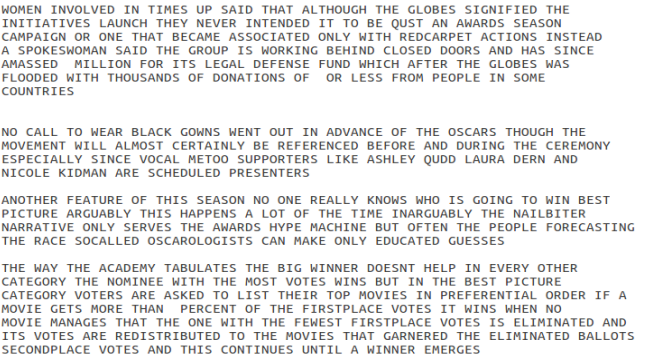


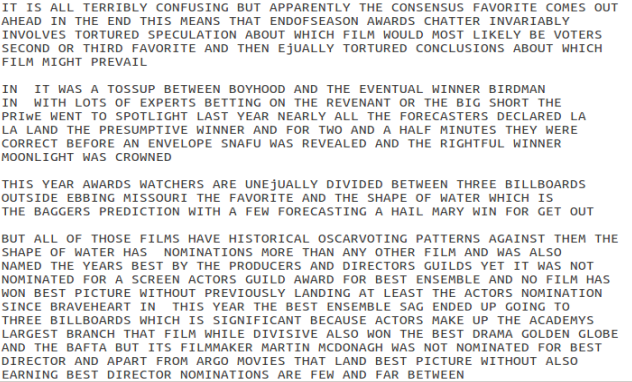
Command used to decipher ciphertext:



Deciphered Ciphertext:

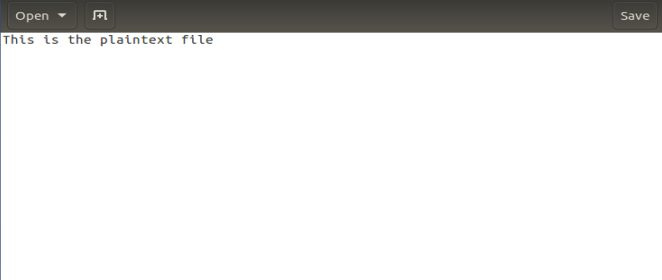






Task 2: Encryption using Different Ciphers and Modes

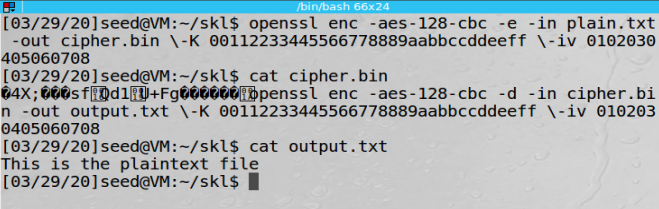
Plaintext file:



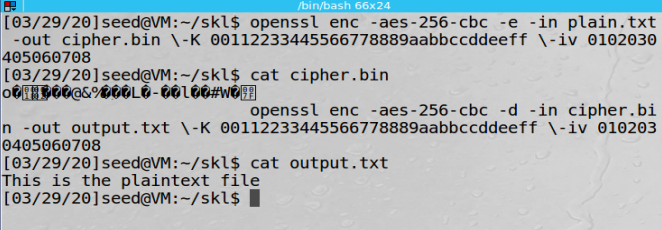
First Cipher Output:



Second Cipher Output:



Third Cipher Output:

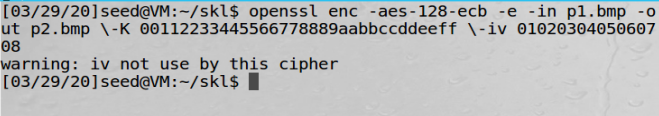


Task 3: Encryption Mode – ECB vs. CBC

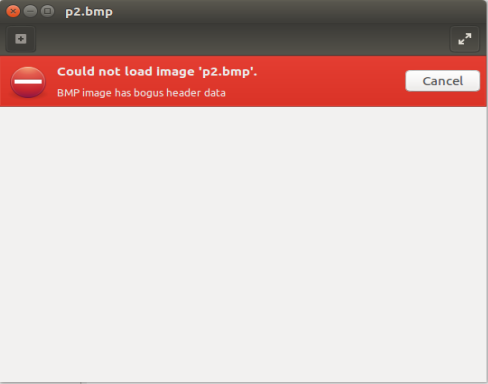
Given Original Picture:



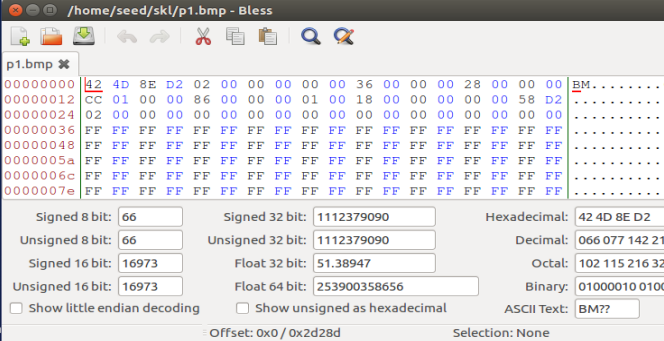
ECB Mode:



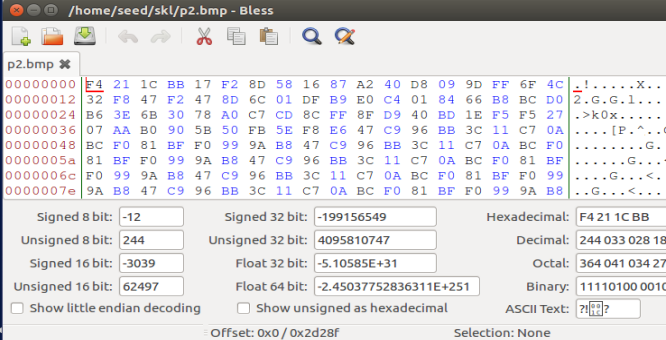
Command used to encrypt the picture in ECB mode.



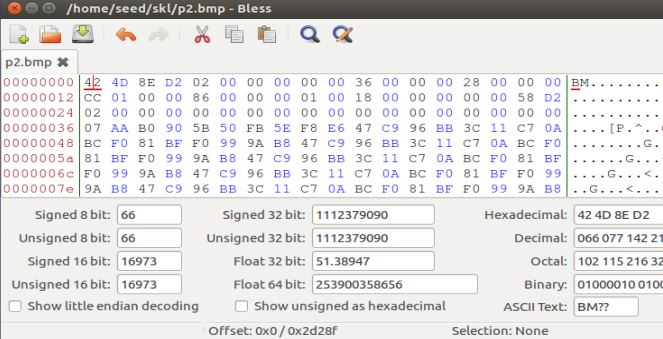
The encrypted picture cannot be displayed.



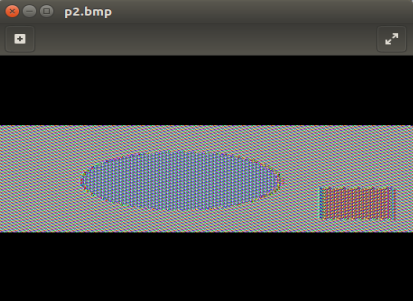
P1.bmp file viewed using the ‘bless’ hex editor tool.



P2.bmp file viewed using the ‘bless’ hex editor tool.

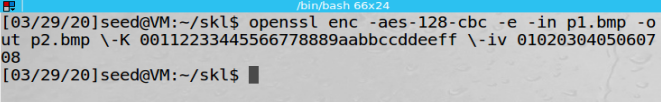


Replacing the header of p2.bmp with the header of p1.bmp.

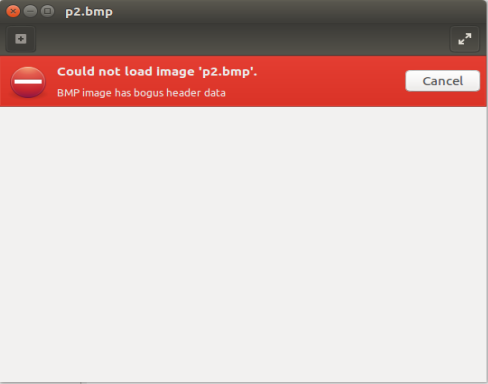


The encrypted file can now be viewed. We can clearly make out the shapes and colors from the original picture.

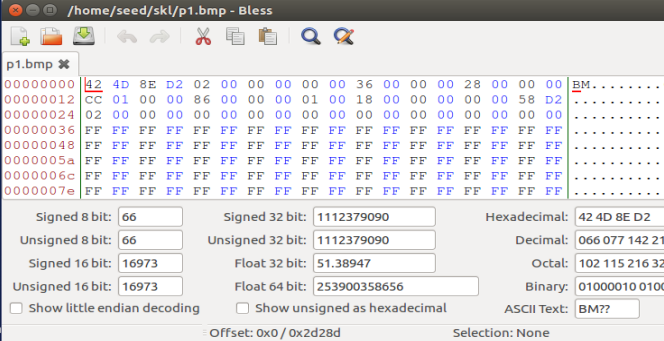
CBC Mode:



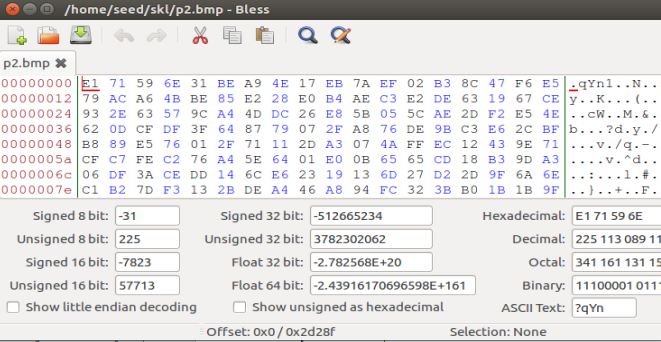
Command used to encrypt the picture in CBC mode.



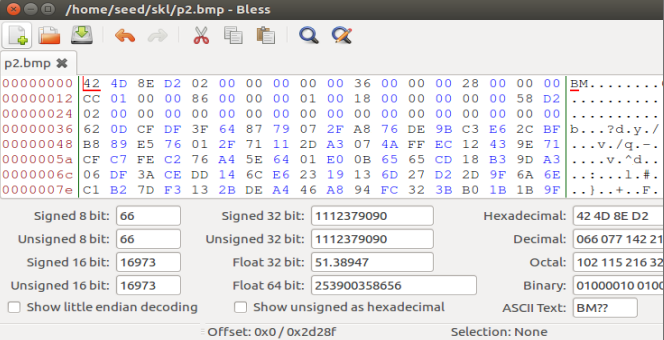
The encrypted file cannot be viewed.



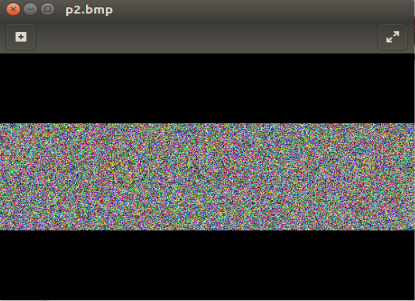
P1.bmp file viewed using the ‘bless’ hex editor tool.



P2.bmp file viewed using the ‘bless’ hex editor tool.

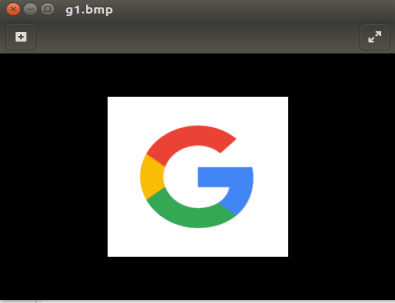


Replacing the header of p2.bmp with the header of p1.bmp.

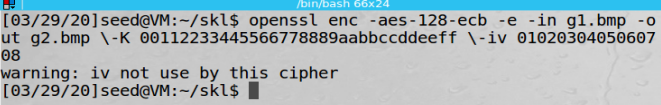


The encrypted file can now be viewed. We cannot discern anything from the original picture from this image.

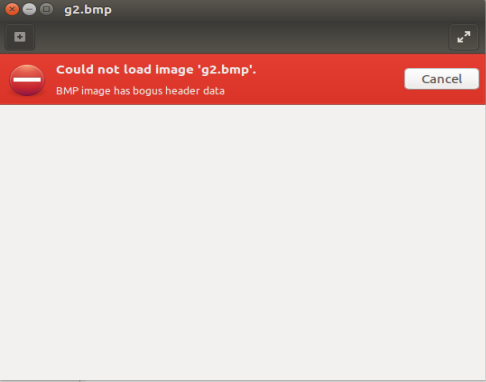
Chosen Original Picture:



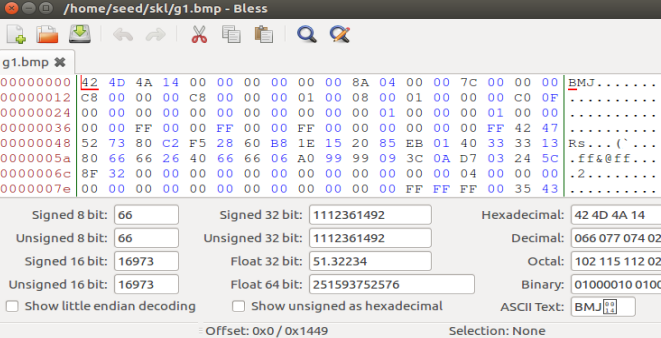
ECB Mode:



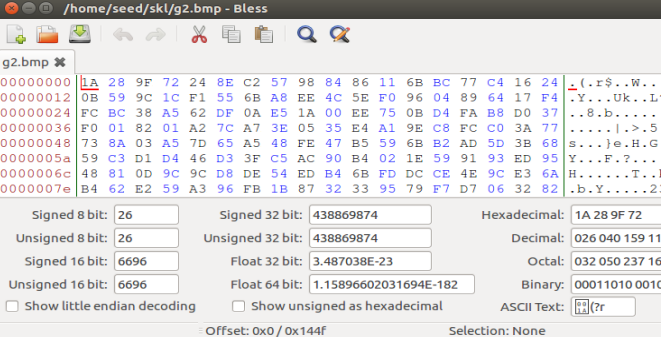
Command used to encrypt the picture in ECB mode.



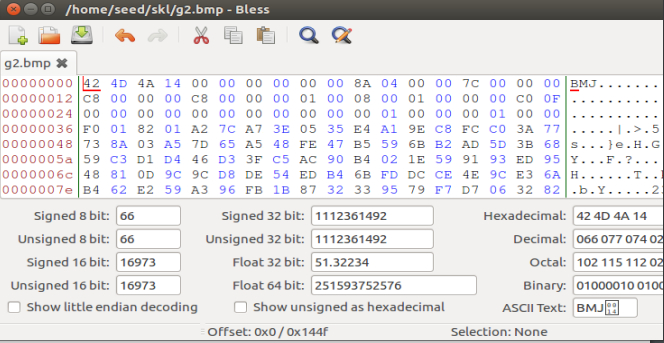
The encrypted file cannot be viewed.



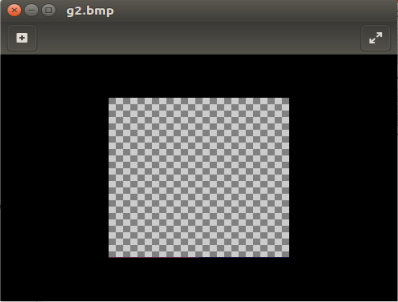
G1.bmp file viewed using the ‘bless’ hex editor tool.



G2.bmp file viewed using the ‘bless’ hex editor tool.

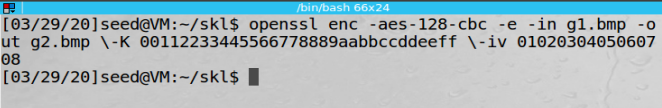


Replacing the header of g2.bmp with the header of g1.bmp.

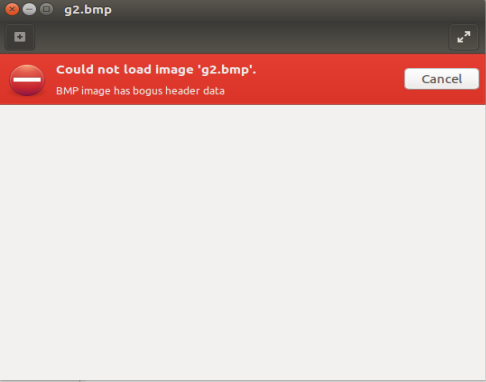


The encrypted file can now be viewed. We cannot discern anything from the original picture from this image.

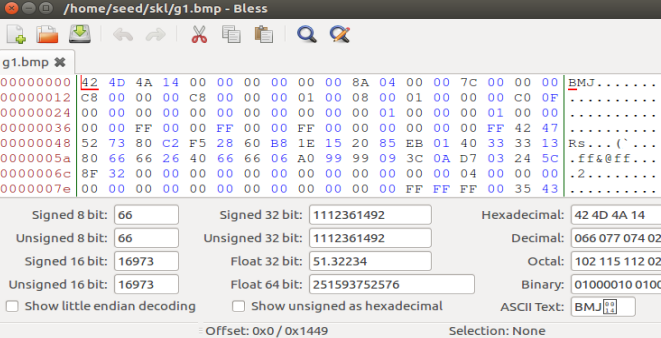
CBC Mode:



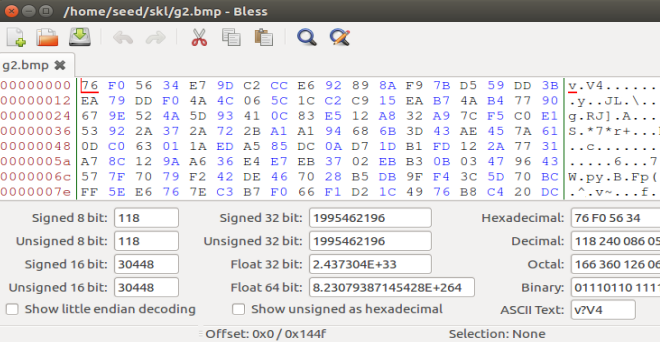
Command used to encrypt the picture in CBC mode.



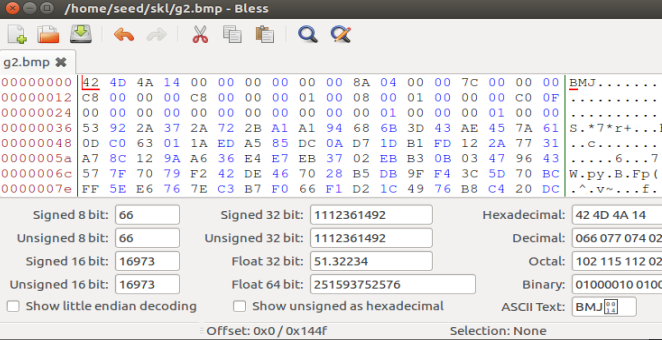
The encrypted file cannot be viewed.



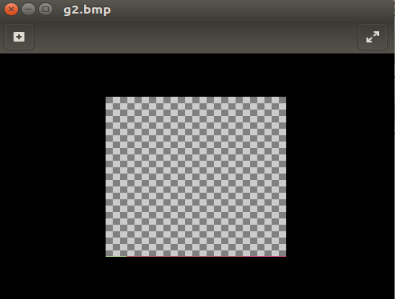
G1.bmp file viewed using the ‘bless’ hex editor tool.



G2.bmp file viewed using the ‘bless’ hex editor tool.



Replacing the header of g2.bmp with the header of g1.bmp.



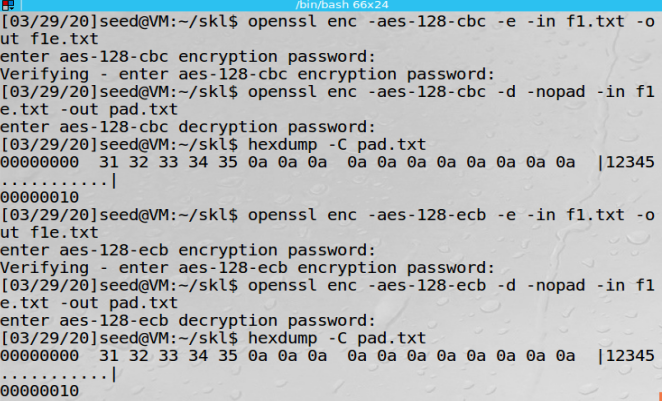
The encrypted file can now be viewed. We cannot discern anything from the original picture from this image.

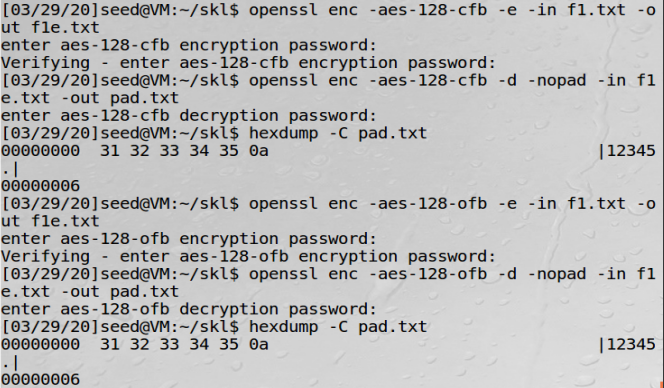
Task 4: Padding

Part 1:



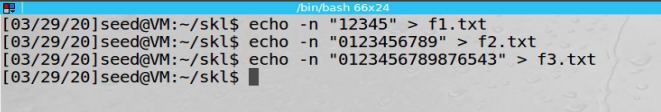
The text file used for encryption.



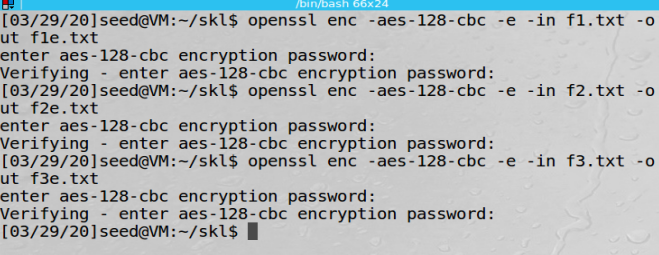


The file is encrypted and then decrypted using the 4 different modes. We can see that the ECB and CBC modes have padding while the CFB and OFB modes do not have padding. The reason the CFB and OFB modes do not have padding is because their ciphertexts are always the same length as the plaintext and hence padding is not required.

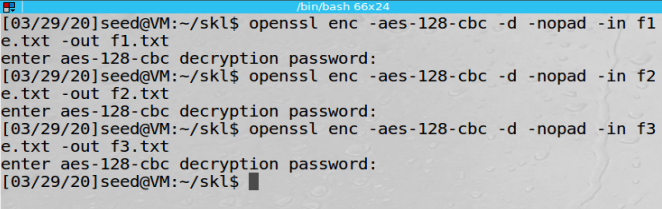
Part 2:



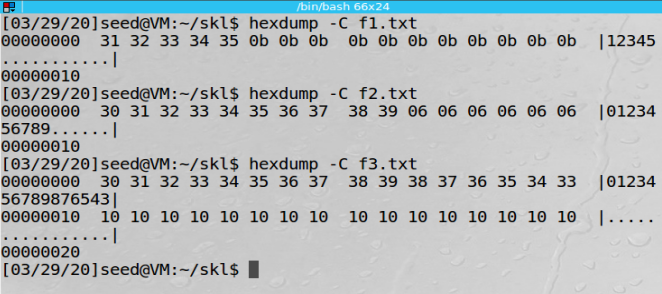
Creating the three text files of length 5 bytes, 10 bytes, and 16 bytes respectively.



Encrypting the three text files.



Decrypting the three text files.



The padding used in the three files shown using the hex tool.