CMPSC443

Ahmet Putun

Crypto Lab- Secret Key Encryption

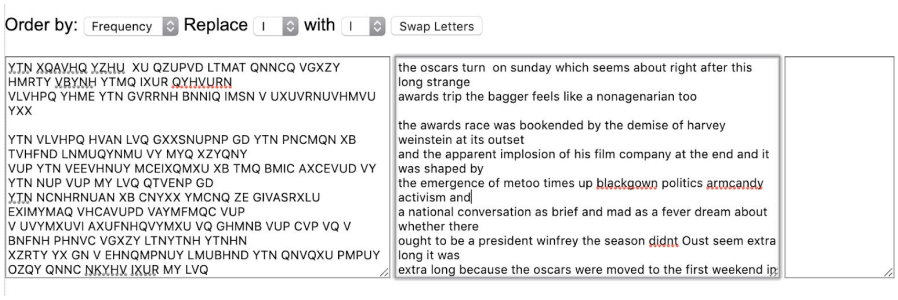
Mr. Sencun Zhu

09/23/2019

Task 1: Frequency Analysis Against Monoalphabetic Substitution Cipher

- For this task, I have used the frequency search tool's website that was provided in the lab requirements pdf, http://www.richkni.co.uk/php/crypta/freq.php, and analyzed the frequency of the text inside the file.

- I've focused on looking over the frequent 2 and 3 letter forms of the letters in order to capture different english meaning words to decrypt the rest of the message.



Plain Text Using Frequency Analysis

the oscars turn on sunday which seems about right after this long strange awards trip the bagger feels like a nonagenarian too

the awards race was bookended by the demise of harvey weinstein at its outset and the apparent implosion of his film company at the end and it was shaped by the emergence of metoo times up blackgown politics armcandy activism and a national conversation as brief and mad as a fever dream about whether there ought to be a president winfrey the season didnt Oust seem extra long it was extra long because the oscars were moved to the first weekend in march to avoid conflicting with the closing ceremony of the winter olympics thanks pyeongchang

one big Juestion surrounding this years academy awards is how or if the ceremony will address metoo especially after the golden globes which became a Oubilant comingout party for times up the movement spearheaded by powerful hollywood women who helped raise millions of dollars to fight sexual harassment around the country

signaling their support golden globes attendees swathed themselves in black sported lapel pins and sounded off about sexist power imbalances from the red carpet and the stage on the air e was called out about pay ineJuity after its former anchor catt sadler Juit once she learned that she was making far less than a male cohost and during the ceremony natalie portman took a blunt and satisfying dig at the allmale roster of nominated directors how could that be topped

as it turns out at least in terms of the oscars it probably wont be

women involved in times up said that although the globes signified the initiatives launch they never intended it to be Oust an awards season campaign or one that became associated only with redcarpet actions instead a spokeswoman said the group is working behind closed doors and has since amassed million for its legal defense fund which after the globes was flooded with thousands of donations of or less from people in some countries

no call to wear black gowns went out in advance of the oscars though the movement will almost certainly be referenced before and during the ceremony especially since vocal metoo supporters like ashley Oudd laura dern and nicole kidman are scheduled presenters

another feature of this season no one really knows who is going to win best picture arguably this happens a lot of the time inarguably the nailbiter narrative only serves the awards hype machine but often the people forecasting the race socalled oscarologists can make only educated guesses

the way the academy tabulates the big winner doesnt help in every other category the nominee with the most votes wins but in the best picture category voters are asked to list their top movies in preferential order if a movie gets more than percent of the firstplace votes it wins when no movie manages that the one with the fewest firstplace votes is eliminated and its votes are redistributed to the movies that garnered the eliminated ballots secondplace votes and this continues until a winner emerges

it is all terribly confusing but apparently the consensus favorite comes out ahead in the end this means that endofseason awards chatter invariably involves tortured speculation about which film would most likely be voters second or third favorite and then eJually tortured conclusions about which film might prevail

in it was a tossup between boyhood and the eventual winner birdman in with lots of experts betting on the revenant or the big short the priWe went to spotlight last year nearly all the forecasters declared la la land the presumptive winner and for two and a half minutes they were correct before an envelope snafu was revealed and the rightful winner moonlight was crowned

this year awards watchers are uneJually divided between three billboards outside ebbing missouri the favorite and the shape of water which is the baggers prediction with a few forecasting a hail mary win for get out

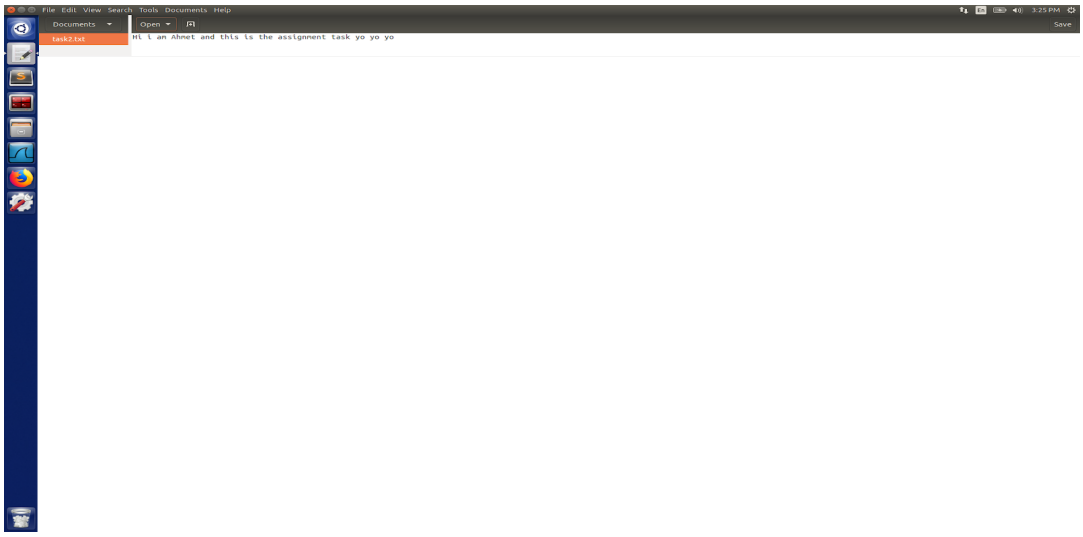
but all of those films have historical oscarvoting patterns against them the shape of water has nominations more than any other film and was also named the years best by the producers and directors guilds yet it was not nominated for a screen actors guild award for best ensemble and no film has won best picture without previously landing at least the actors nomination since braveheart in this year the best ensemble sag ended up going to three billboards which is significant because actors make up the academys largest branch that film while divisive also won the best drama golden globe and the bafta but its filmmaker martin mcdonagh was not nominated for best director and apart from argo movies that land best picture without also earning best director nominations are few and far between

Task 2: Encryption using Different Ciphers and Modes

- For this task, I was given a task of encrypting a text file that I created in my virtual machine.

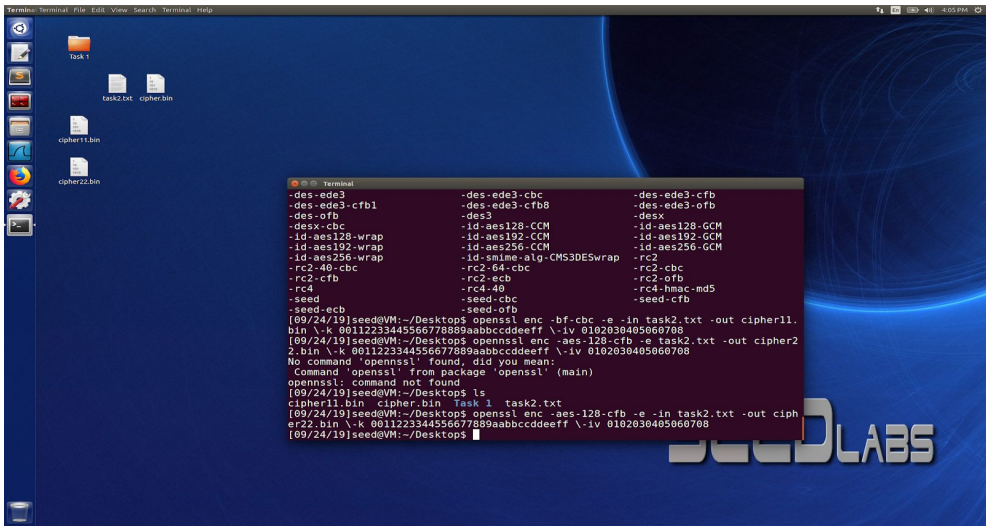
- Given 3 different “ciphertype”, -aes-128-cbc, -bf-cbc, -aes-128-cfb, I encrypted the my random text file.
- The context of my text file is;

  Hi i am Ahmet and this is the assignment task yo yo yo

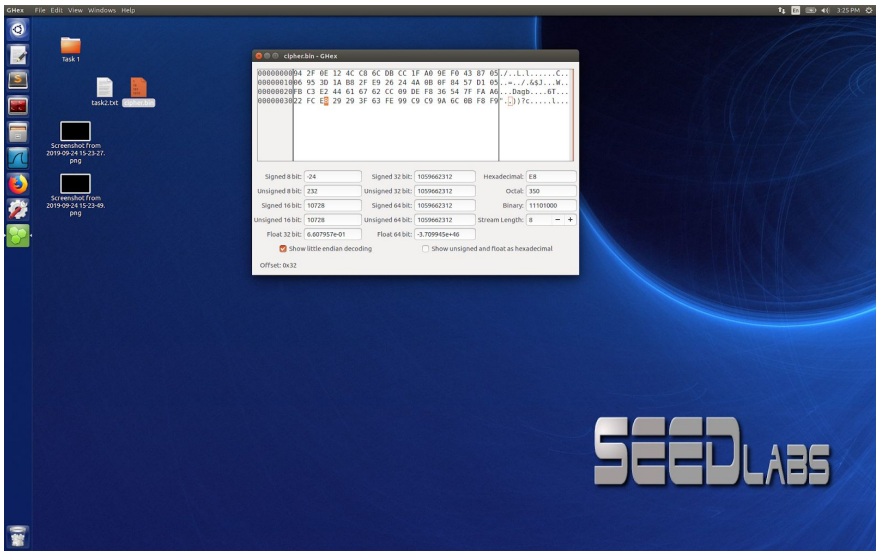


- I’ve encrypted my text file using 3 different modes:

  Openssl enc **-aes-128-cbc** -e -in task2.txt -out cipher.bin \-k 00112233445566778889aabbccddeeff \-iv 0102030405060708
  Openssl enc **-bf-cbc** -e -in task2.txt -out cipher11.bin \-k 00112233445566778889aabbccddeeff \-iv 0102030405060708
  Openssl enc **-aes-128-cfb** in task2.txt -out cipherenc22.bin \-k 00112233445566778889aabbccddeeff \-iv 0102030405060708

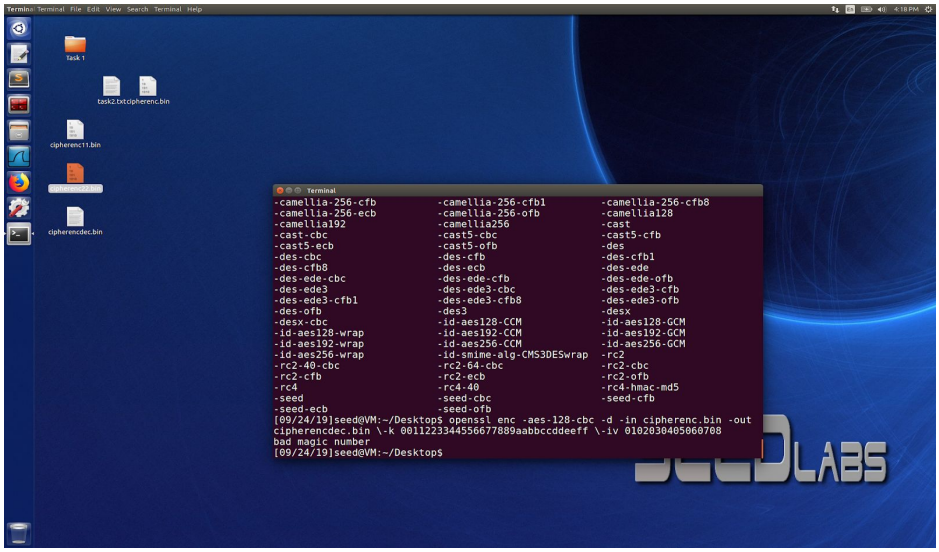


I used GHex editor to open the encrypted file in binary file.

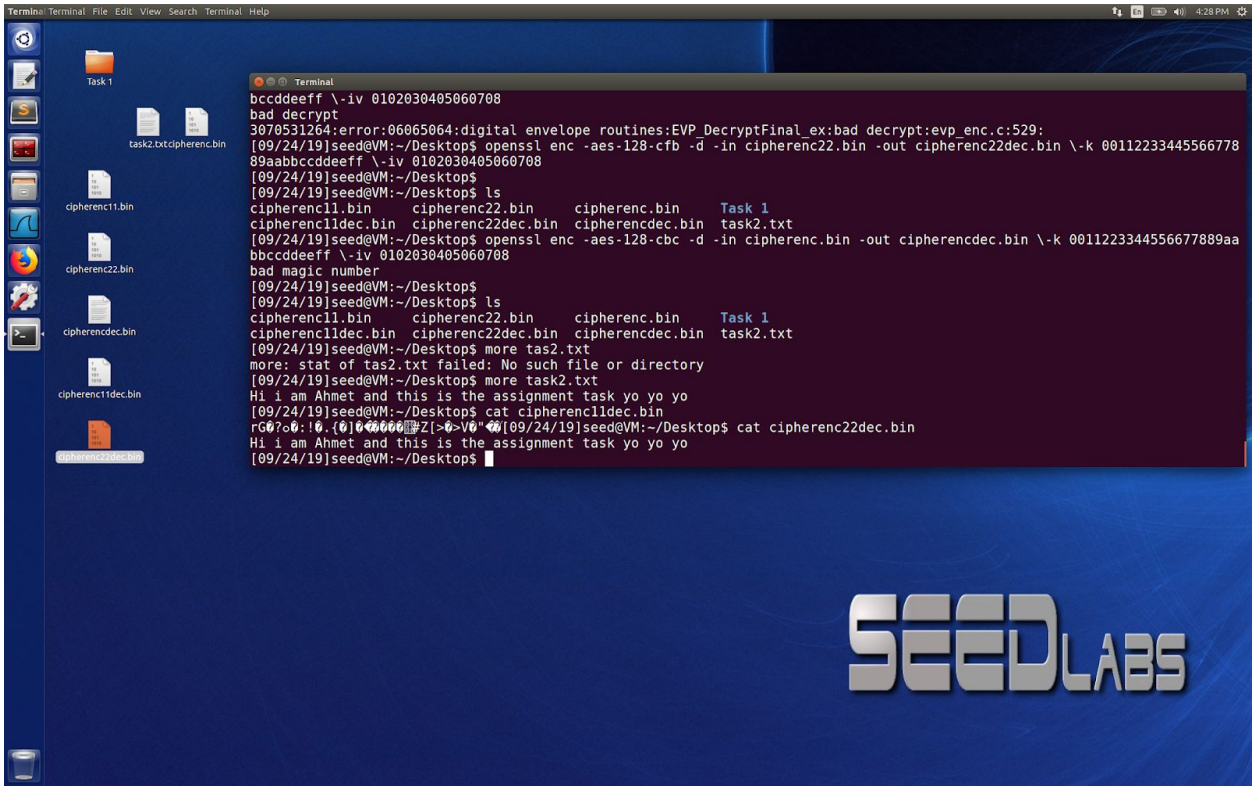


- And decrypted the files using “-d” command instead of “-e”

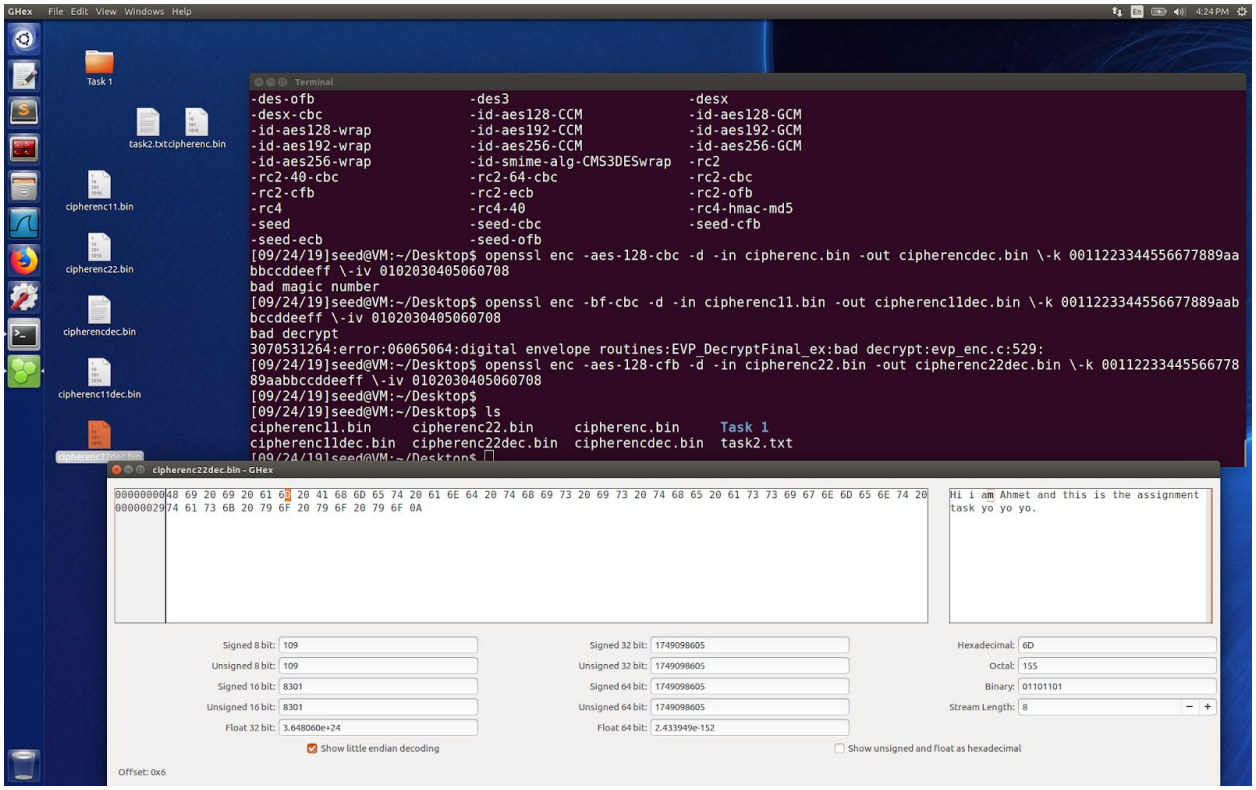
openssl enc **-bf-cbc -d** -in cipherenc22.bin -out cipherenc22dec.bin \-k 00112233445566778889aabbccddeeff \-iv 0102030405060708



The context of my file is shown with more command



Decryption using -aes-128-cfb



Task 3: Encryption Mode – ECB vs. CBC

ECB

- For this task I was given to encrypt a picture provided by the website of the lab. I downloaded the picture, *pic_original.bmp.* Then, I encrypted the image using electronic codebook mode, ECB.

  Openssl enc -**aes-128-ecb** -e -in pic_original.bmp -out pic_originaldec.bmp \-k 00112233445566778889aabbccddeeff \-iv 0102030405060708

- Then, I've tried to view the encrypted image, it gave me an error saying that BMP image has bogus header data, because the .bmp file, the first 54 bytes contain header information about the picture, setting it correctly so that the encrypted file can be treated as a .bmp file. I then went on opening the file with GHex editor.

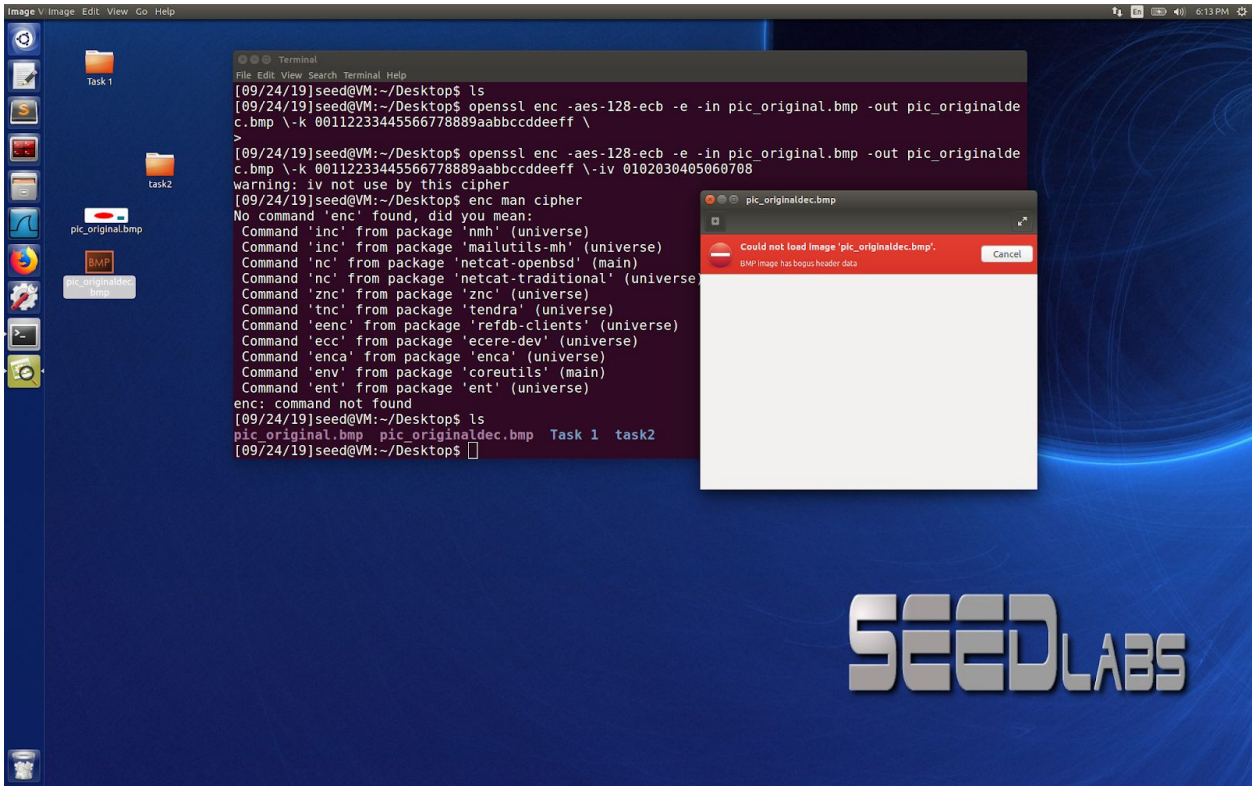
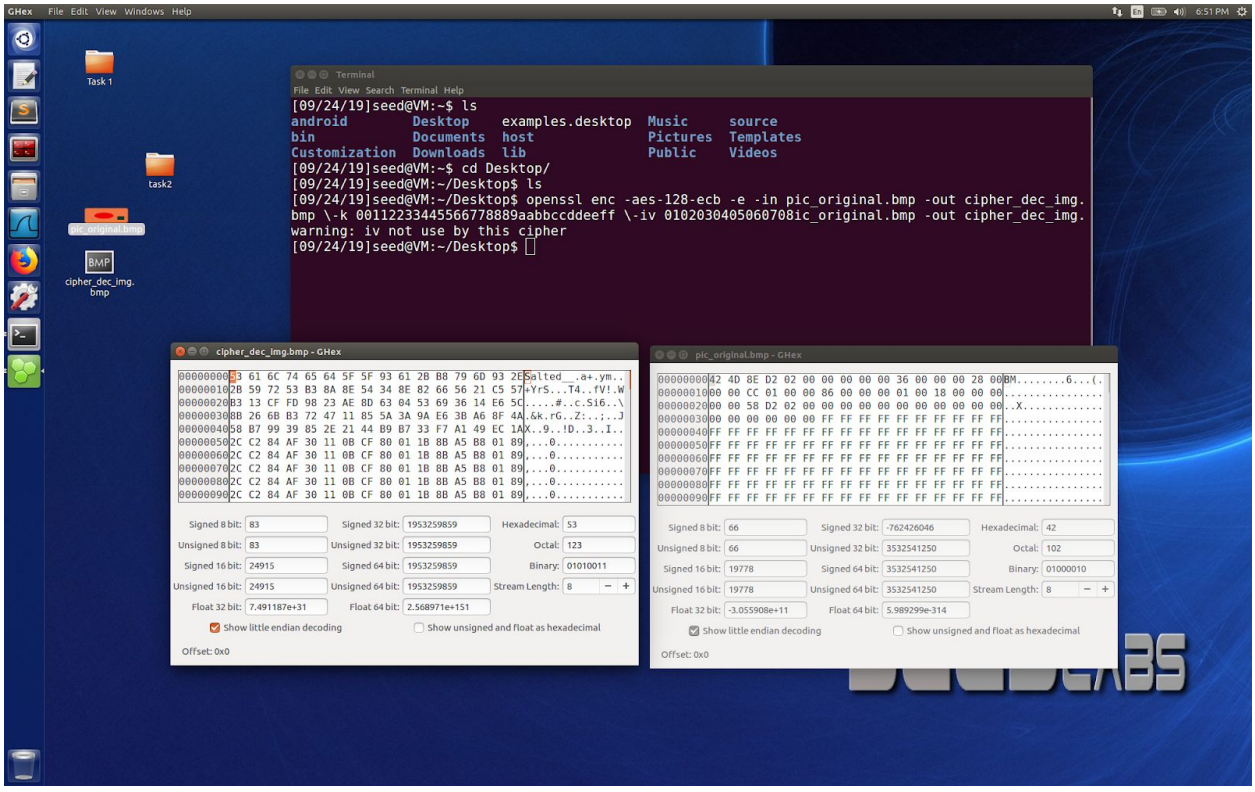
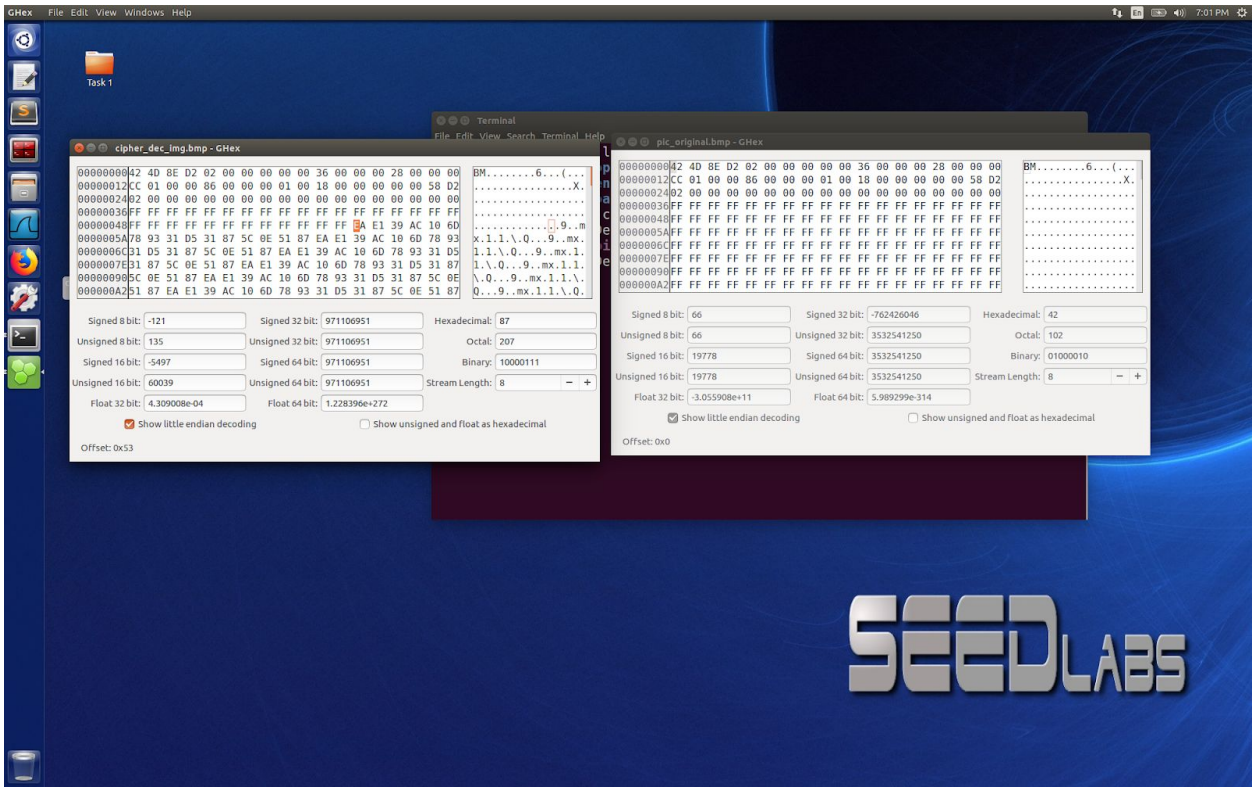


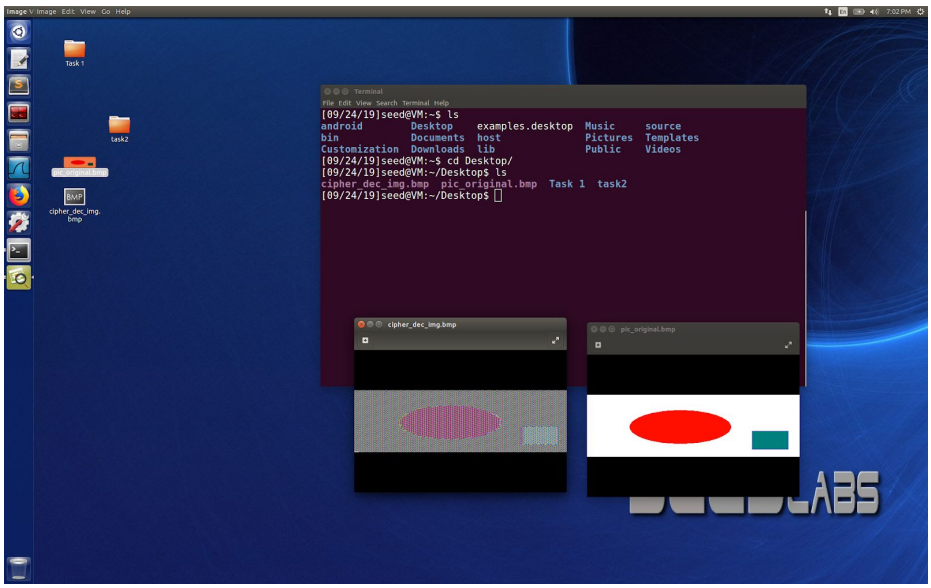
Image View Image Edit View Go Help
6:13 PM
Task 1
task2
pic_original.bmp
pic_originaldec.bmp
Terminal
File Edit View Search Terminal Help
[09/24/19]seed@VM:~/Desktop$ ls
[09/24/19]seed@VM:~/Desktop$ openssl enc -aes-128-ecb -e -in pic_original.bmp -out pic_originaldec.bmp \-k 00112233445566778889aabbccddeeff \
>
[09/24/19]seed@VM:~/Desktop$ openssl enc -aes-128-ecb -e -in pic_original.bmp -out pic_originaldec.bmp \-k 00112233445566778889aabbccddeeff \-iv 0102030405060708
warning: iv not use by this cipher
[09/24/19]seed@VM:~/Desktop$ enc man cipher
No command 'enc' found, did you mean:
Command 'inc' from package 'nmh' (universe)
Command 'inc' from package 'mailutils-mh' (universe)
Command 'nc' from package 'netcat-openbsd' (main)
Command 'nc' from package 'netcat-traditional' (universe)
Command 'znc' from package 'znc' (universe)
Command 'tnc' from package 'tendra' (universe)
Command 'eenc' from package 'refdb-clients' (universe)
Command 'ecc' from package 'ecere-dev' (universe)
Command 'enca' from package 'enca' (universe)
Command 'env' from package 'coreutils' (main)
Command 'ent' from package 'ent' (universe)
enc: command not found
[09/24/19]seed@VM:~/Desktop$ ls
pic_original.bmp pic_originaldec.bmp Task 1 task2
[09/24/19]seed@VM:~/Desktop$
pic_originaldec.bmp
Could not load image 'pic_originaldec.bmp'.
BMP image has bogus header data
Cancel
SEEDLABS


GHex File Edit View Windows Help
6:51 PM
Task 1
task2
pic_original.bmp
cipher_dec_img.bmp
Terminal
File Edit View Search Terminal Help
[09/24/19]seed@VM:~$ ls
android Desktop examples.desktop Music source
bin Documents host Pictures Templates
Customization Downloads lib Public Videos
[09/24/19]seed@VM:~$ cd Desktop/
[09/24/19]seed@VM:~/Desktop$ ls
[09/24/19]seed@VM:~/Desktop$ openssl enc -aes-128-ecb -e -in pic_original.bmp -out cipher_dec_img.bmp \-k 00112233445566778889aabbccddeeff \-iv 0102030405060708ic_original.bmp -out cipher_dec_img.bmp \-k 00112233445566778889aabbccddeeff \-iv 0102030405060708
warning: iv not use by this cipher
[09/24/19]seed@VM:~/Desktop$
cipher_dec_img.bmp - GHex
pic_original.bmp - GHex
Show little endian decoding
Show unsigned and float as hexadecimal
Offset: 0x0
SEEDLABS

- Then I changed the first 54 bytes for the header information to match it with pic_original.bmp



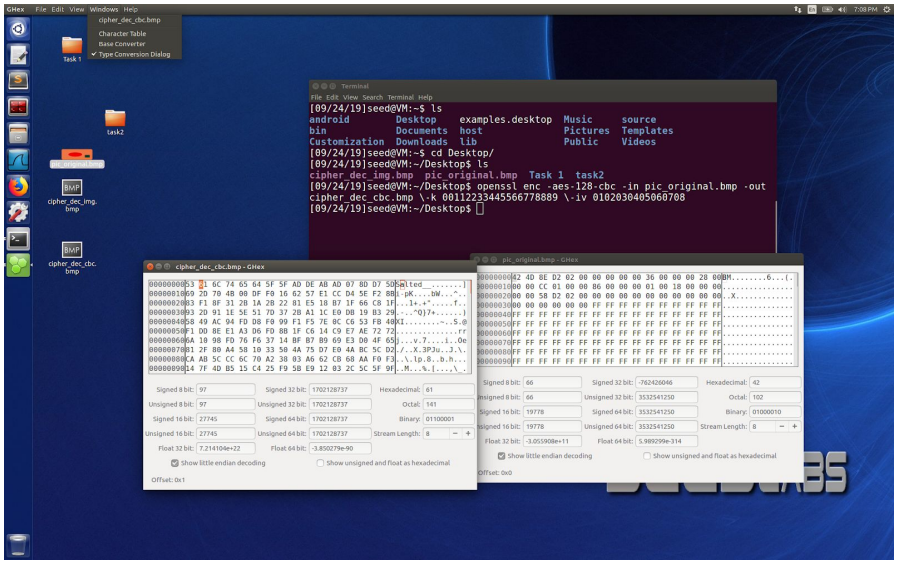
After changing the bytes in the Ghex, I've encrypted the picture



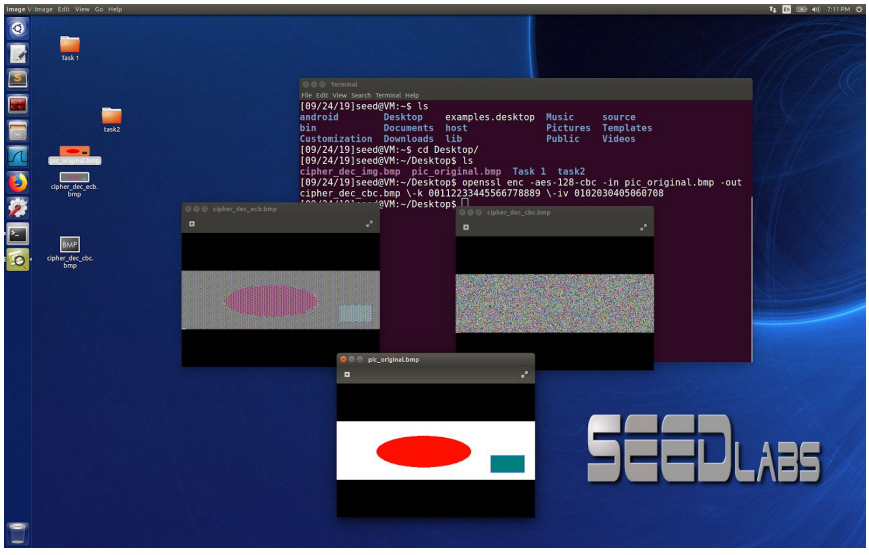
CBC

- Now, I did the same encryption using cipher block chaining, CBC.
  Openssl enc -**aes-128-cbc** -e -in pic_original.bmp -out cipher_dec_cbc.bmp \-k 00112233445566778889aabbccddeeff \-iv 0102030405060708

- Besides, same error appeared again because of the bytes I need to play around with. To be able to view the image, I have to change the 54 bytes header of the encrypted image.



- And the final images of the encrypted version of p*ic_original.bmp* using ECB and CBC



Observations

- Doing ECB, identical plaintext blocks are encrypted into identical ciphertext blocks which claims that the data patterns are not well hidden.(https://crypto.stackexchange.com/questions/20941/why-shouldnt-i-use-ecb-encryption)

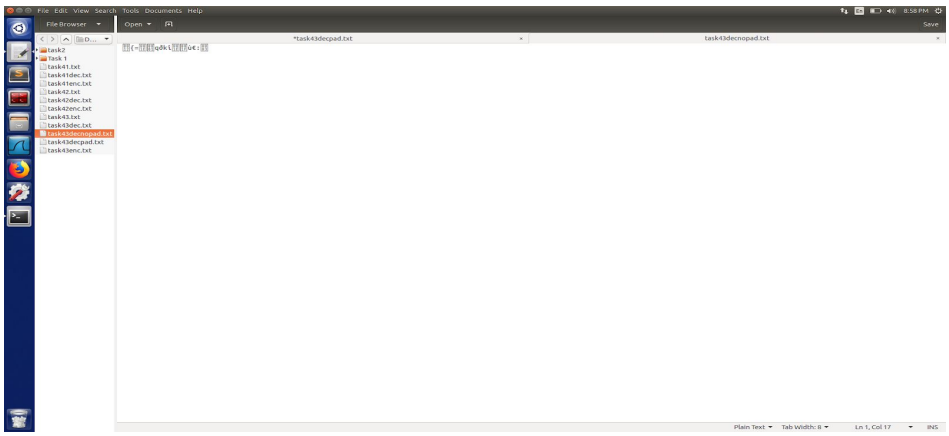
- Doing CBC seems like providing more secure tools because it uses XOR in every other encryption of each ciphertext block.

Task 4: Padding

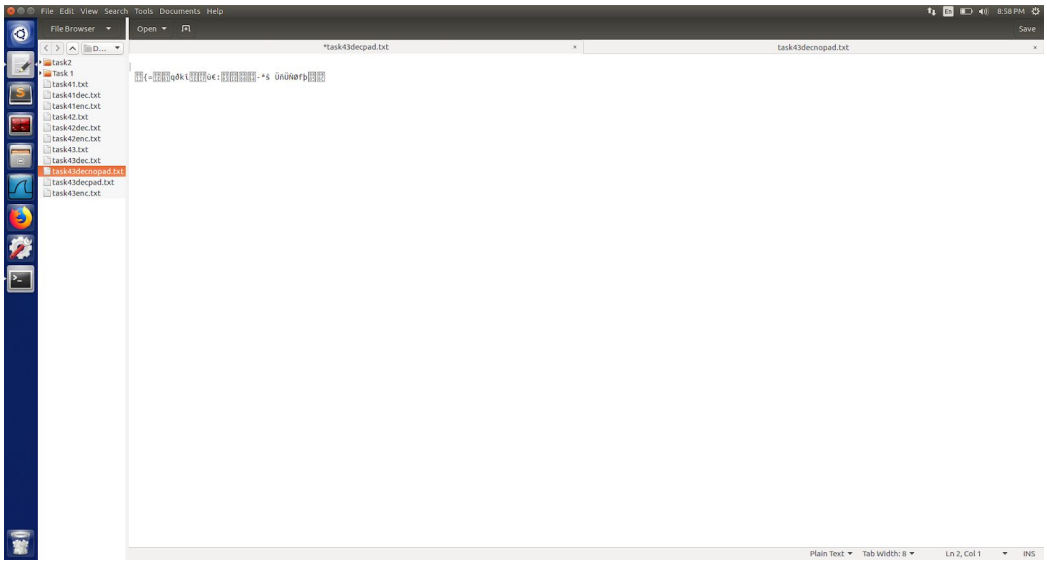
- From the instructions, I created 3 text files with sizes 5, 10, 16 bytes.

- Then, I've encrypted the files using cbc mode, compared the file size with the original file, then decrypted the previously encrypted file in order to observe how much padding has been implemented to block sizes of each files.
  Openssl enc -aes-128-cbc -d in task43enc.txt out task43decpad.txt \-k 00112233445566778889aabbccddeeff \-iv 0102030405060708

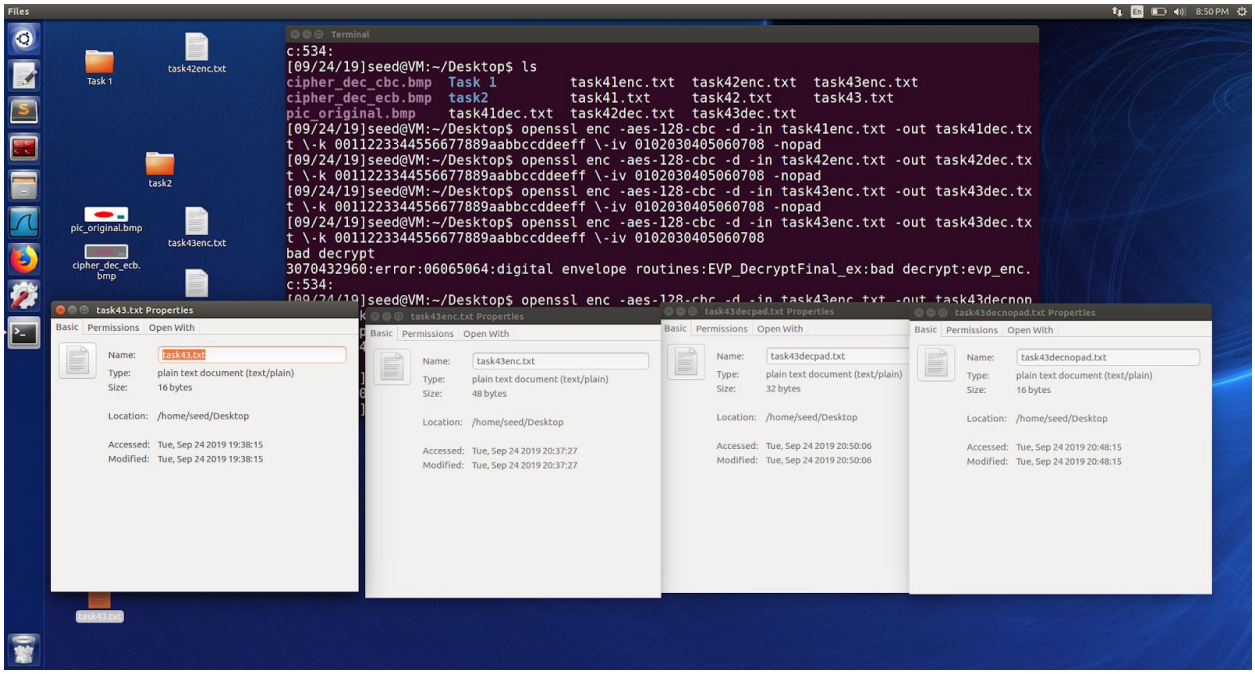
  File with no padding



File with padding



I’ve observed the file sizes of them



The original file*: task43.txt*

Encrypted file*: task4enc.txt*

Decryption with pad*: task43decpad.txt*

Decryption with no pad*: task43decnopad.txt*

- The original file contained 16 bytes however with the encryption it added 2 more blocks of 16 bytes and made the file 48 bytes.

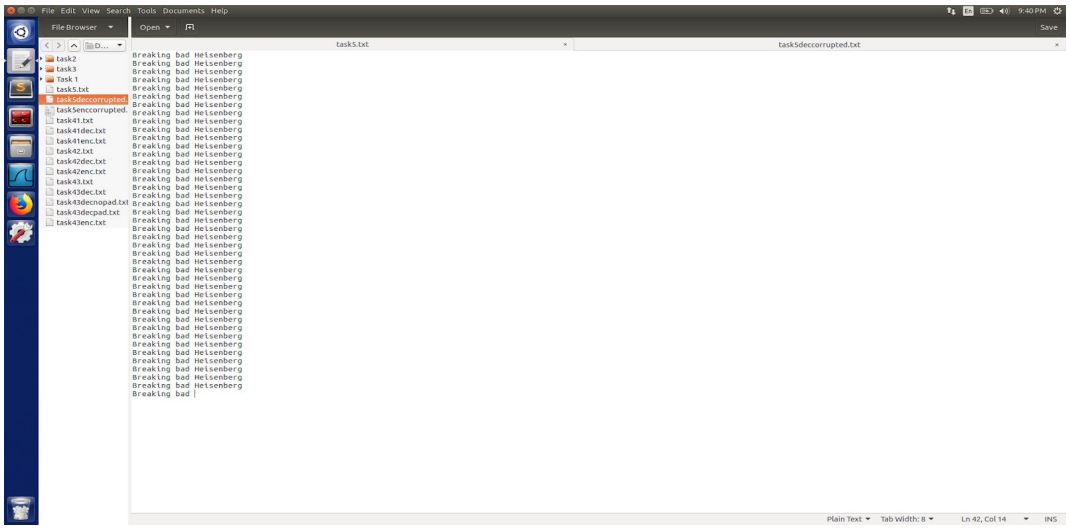
- Decrypting using padding and no padding made differences in the size of the files. As it seems in the image above;

- With the other observations I concluded after trying out different ciphers, padding is needed for ecb and cbc encryption modes because their inputs contain number of blocks which comes with padding.
- For cfb cipher type, the size of the blocks are fixed that is why it does not display any padding. Same rule applies for ofb cipher type;

openssl enc -**aes-128-ofb** -e -in filename -out filename \-k ‘ ‘ \ -iv ‘ ‘

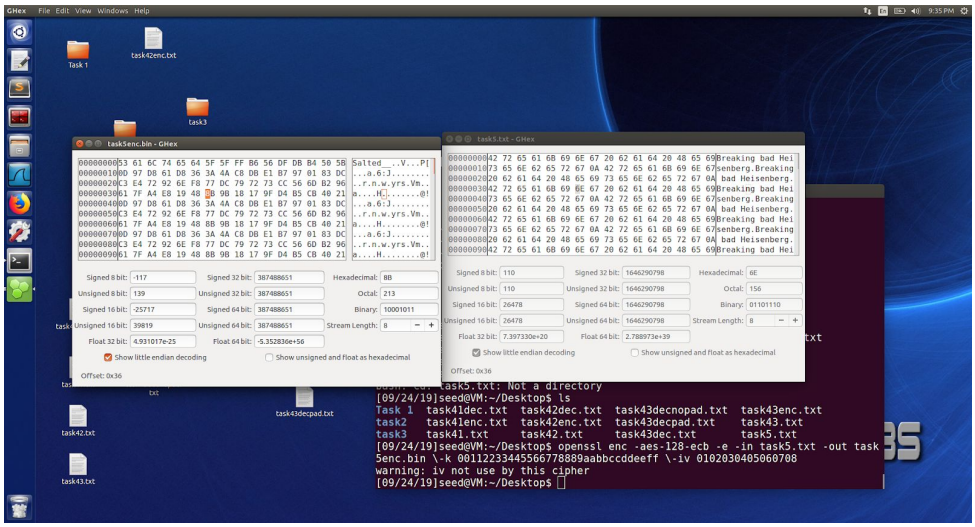
Task 5: Error Propagation – Corrupted Cipher Text

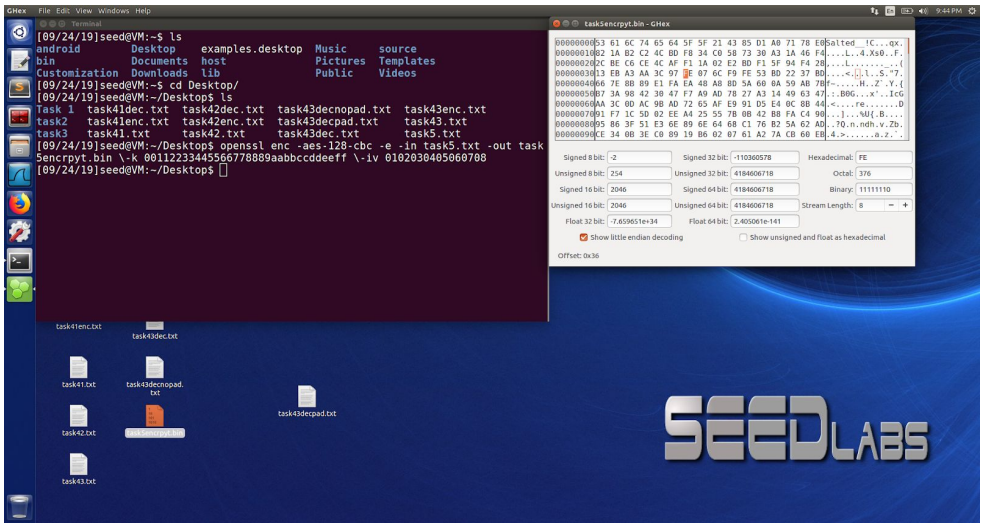
- I created a text file that is more than 1000 bytes, 1001 bytes. Then, i went on encrypting the file using the aes-128 cipher.



CBC mode

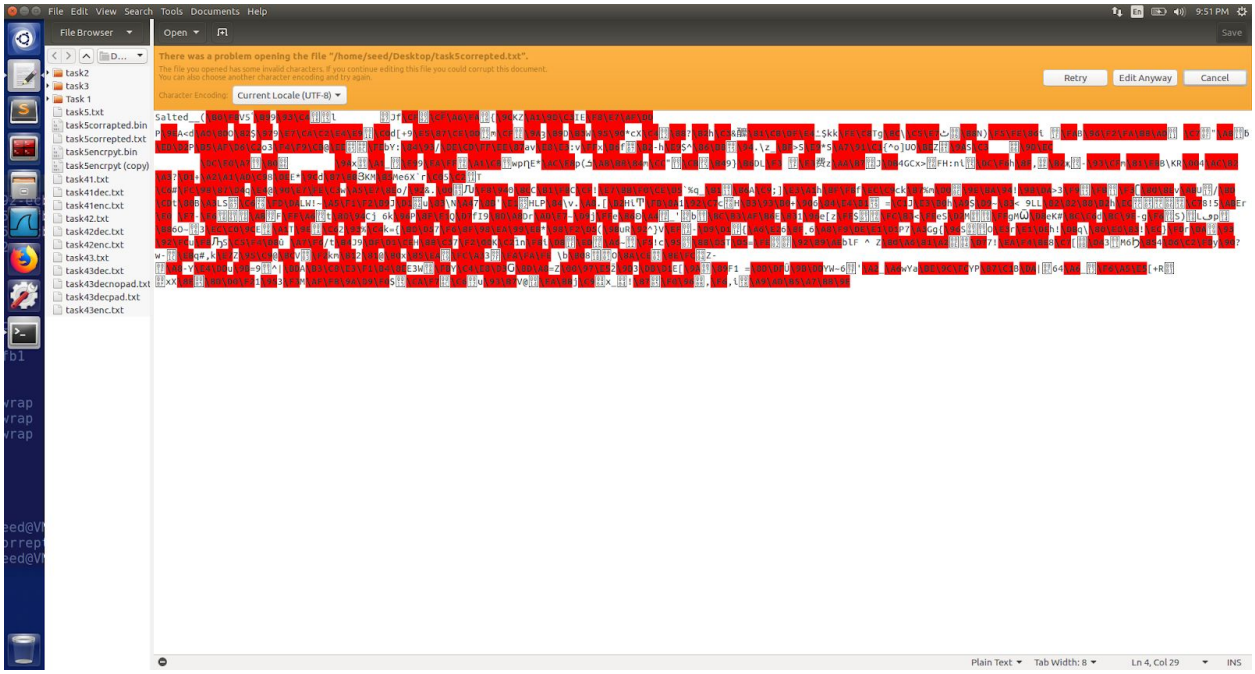
- In the original encrypted file, the position 55th byte is 6E corresponds to the value 8B, I changed the single bit of this value from 6 to F so the value of 55th byte now is FE then I saved the file.





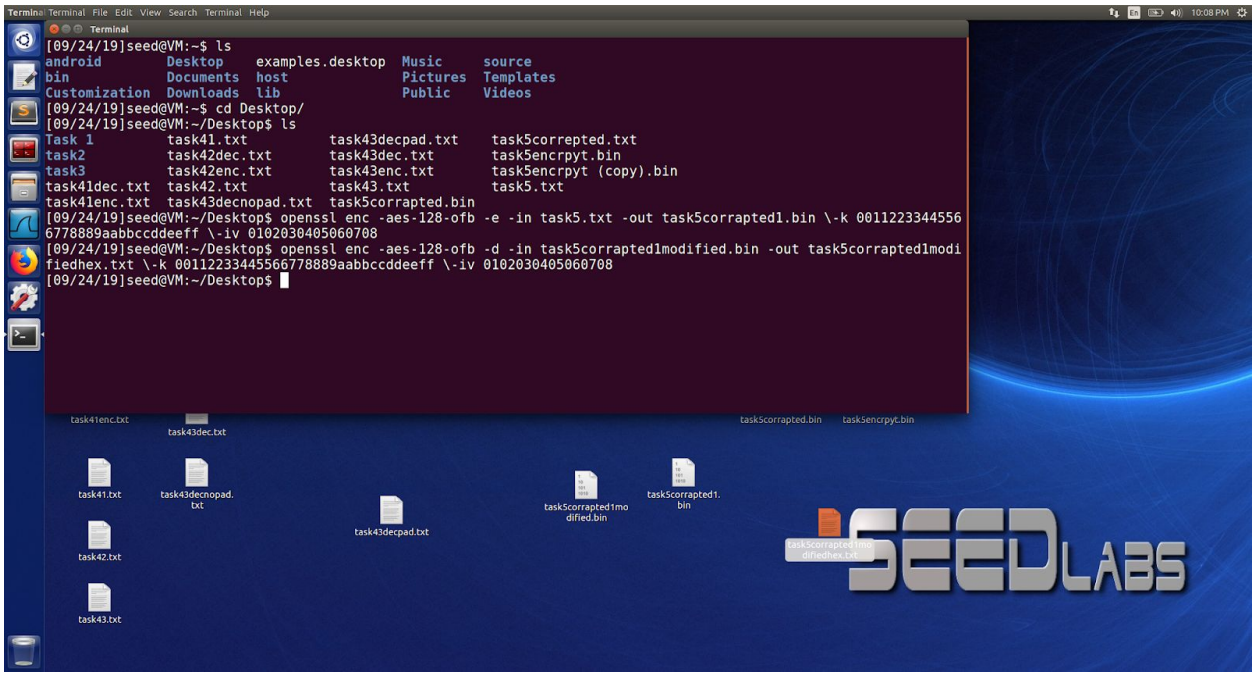
- I got a corrupted encrypted file.

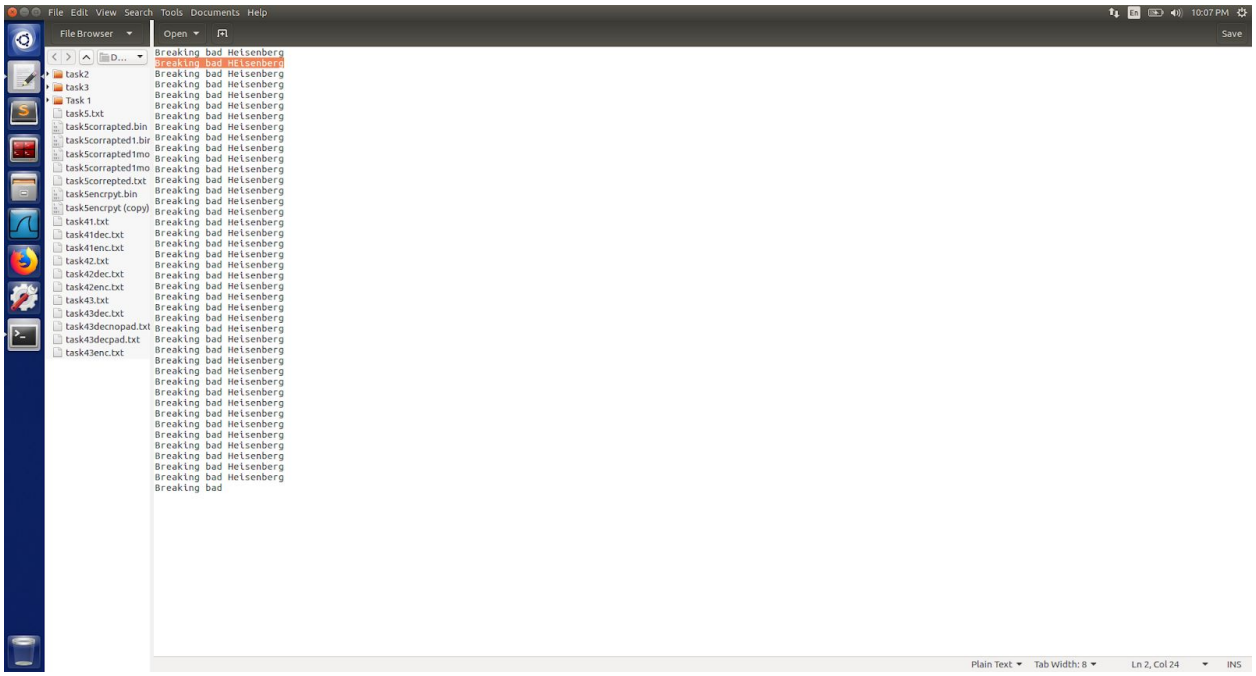
- I decrypted the corrupted encrypted file to see the effects made on the file.



OFB mode

- I went through the same process in order to try different modes and see how much data I will lose with corrupted encryption.
- First, I encrypted the file in my text file task5.txt into a binary file then changed a single bit from the 55th byte in GHex editor, got a corrupted encrypted file.
- Finally, I encrypted the file to see the effects and differences.





- The only significant difference hit was in ‘e’ shown in the image.

Observations

- In CBC mode, there was effect in multiple blocks. Therefore file got into a “weirder” mode.
- I went on and tried different ciphers and specifically on OFB mode, as it seems in the above images, it showed the best results with mostly covering the entire text

- In OFB, feedback is only in the key-generation system. If the single digit of the 55th byte is corrupted, then in plain text that only that byte or character is corrupted.
  “ http://www.crypto-it.net/eng/theory/modes-of-block-ciphers.html”

Works Cited

Ellis, Scott. “Block Ciphers - an Overview | ScienceDirect Topics.” *Sciencedirect.Com*, 2013, www.sciencedirect.com/topics/computer-science/block-ciphers. Accessed 25 Sept. 2019.

“Block Ciphers Modes of Operation | Cryptography | Crypto-IT.” *Crypto-It.Net*, 2013, www.crypto-it.net/eng/theory/modes-of-block-ciphers.html.

“Why Is OCB-AES Mode Not Becoming a Standard for Authenticated Encryption?” *Cryptography Stack Exchange*, 9 Dec. 2012, crypto.stackexchange.com/questions/5639/why-is-ocb-aes-mode-not-becoming-a-standard-for-authenticated-encryption.