Shane Hagan
Lab 1
CMPSC 443

Task 1

Text converted to:
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 JUST 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 QUESTION SURROUNDING THIS YEARS ACADEMY AWARDS IS HOW OR IF THE CEREMONY WILL ADDRESS METOO ESPECIALLY AFTER THE GOLDEN GLOBES WHICH BECAME A JUBILANT 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 INEQUITY AFTER ITS FORMER ANCHOR CATT SADLER QUIT 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 JUST 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 JUDD LAURA DERN AND NICOLE KIDMAN ARE SCHEDULED PRESENTERS

ANOTHER FEATURE OF THIS SEASON NO ONE REALLY KNOWS WHO IS GOING TO WIN BEST

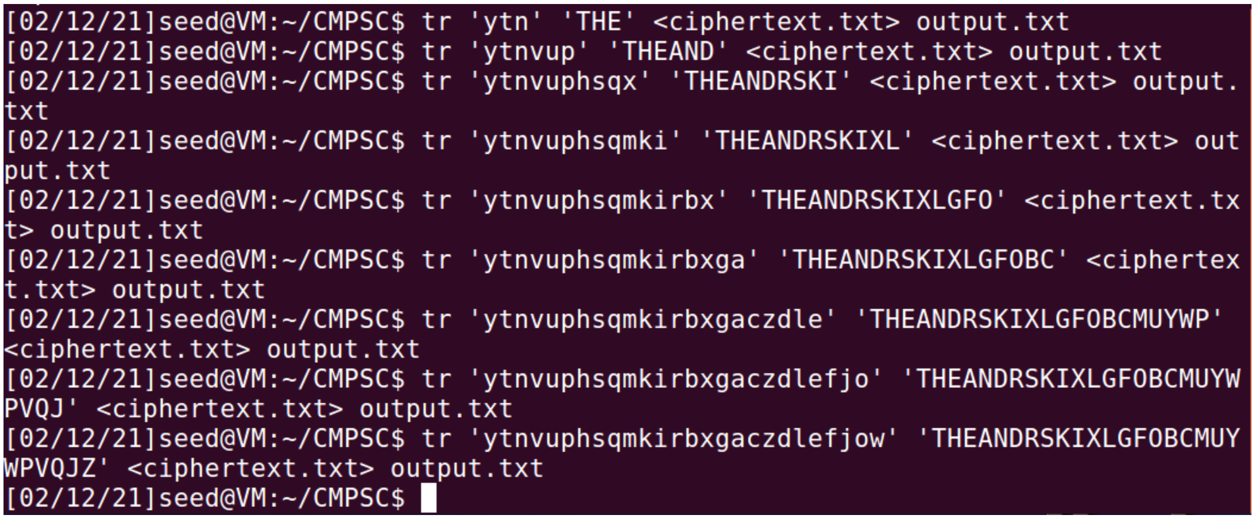
PICTURE ARGUABLY THIS HAPPENS A LOT OF THE TIME INARGUABLY THE NAILBITER NARRATIVE ONLY SERVES THE AWARDS HYPE MACHINE BUT OFTEN THE PEOPLE FORECASTING THE RACE SOCALLED OSCAROLOGISTS CAN MAKE ONLY EDUCATED GUESSES

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 EQUALLY 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 PRIZE 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

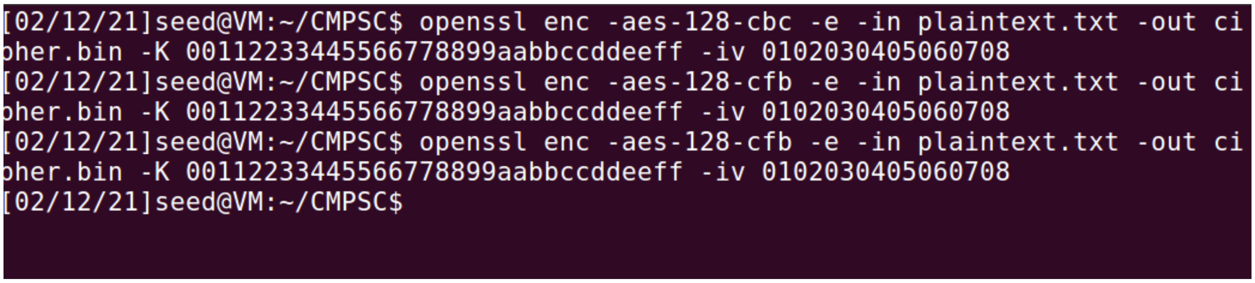
THIS YEAR AWARDS WATCHERS ARE UNEQUALLY DIVIDED BETWEEN THREE BILLBOARDS OUTSIDE EBBING MISSOURI THE FAVORITE AND THE SHAPE OF WATER WHICH IS THE BAGGERS PREDICTION WITH A FEW FORECASTING A HAIL MARY WIN FOR GET OUT BUT ALL OF THOSE FILMS HAVE HISTORICAL OSCARVOTING PATTERNS AGAINST THEM THE SHAPE OF 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



```
[02/12/21]seed@VM:~/CMPSC$ tr 'ytn' 'THE' <ciphertext.txt> output.txt
[02/12/21]seed@VM:~/CMPSC$ tr 'ytnvup' 'THEAND' <ciphertext.txt> output.txt
[02/12/21]seed@VM:~/CMPSC$ tr 'ytnvuphsqx' 'THEANDRSKI' <ciphertext.txt> output.
txt
[02/12/21]seed@VM:~/CMPSC$ tr 'ytnvuphsqmki' 'THEANDRSKIXL' <ciphertext.txt> out
put.txt
[02/12/21]seed@VM:~/CMPSC$ tr 'ytnvuphsqmkirbx' 'THEANDRSKIXLGFO' <ciphertext.tx
t> output.txt
[02/12/21]seed@VM:~/CMPSC$ tr 'ytnvuphsqmkirbxga' 'THEANDRSKIXLGFOBC' <ciphertex
t.txt> output.txt
[02/12/21]seed@VM:~/CMPSC$ tr 'ytnvuphsqmkirbxgaczdle' 'THEANDRSKIXLGFOBCMUYWP'
<ciphertext.txt> output.txt
[02/12/21]seed@VM:~/CMPSC$ tr 'ytnvuphsqmkirbxgaczdlefjo' 'THEANDRSKIXLGFOBCMUYW
PVQJ' <ciphertext.txt> output.txt
[02/12/21]seed@VM:~/CMPSC$ tr 'ytnvuphsqmkirbxgaczdlefjow' 'THEANDRSKIXLGFOBCMUY
WPVQJZ' <ciphertext.txt> output.txt
[02/12/21]seed@VM:~/CMPSC$ 
```

Using the Wikipedia and frequency sites, I was able to start plugging in random swaps. For example, the "ytn" was the highest frequency three letter word, making me guess it would be replaced with "THE". From there I just looked at more letter frequencies, and as the text started becoming decrypted, I would plug in letters that would complete a word. Just taking our time, checking output.txt, we are able to see what needs to be changed, what words could make sense.

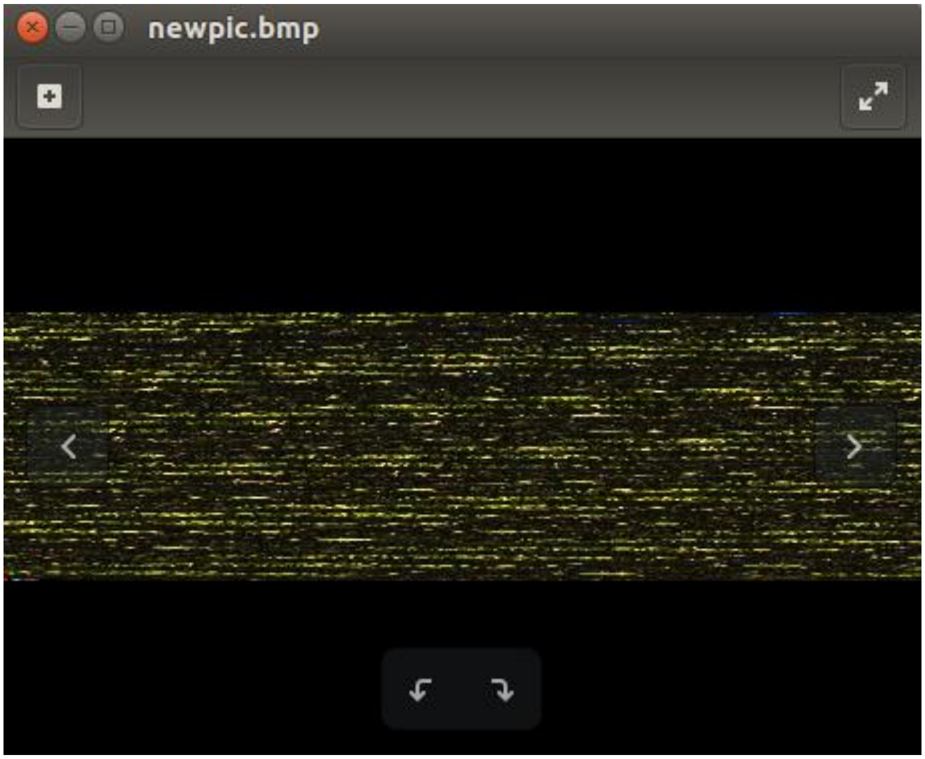
Task 2



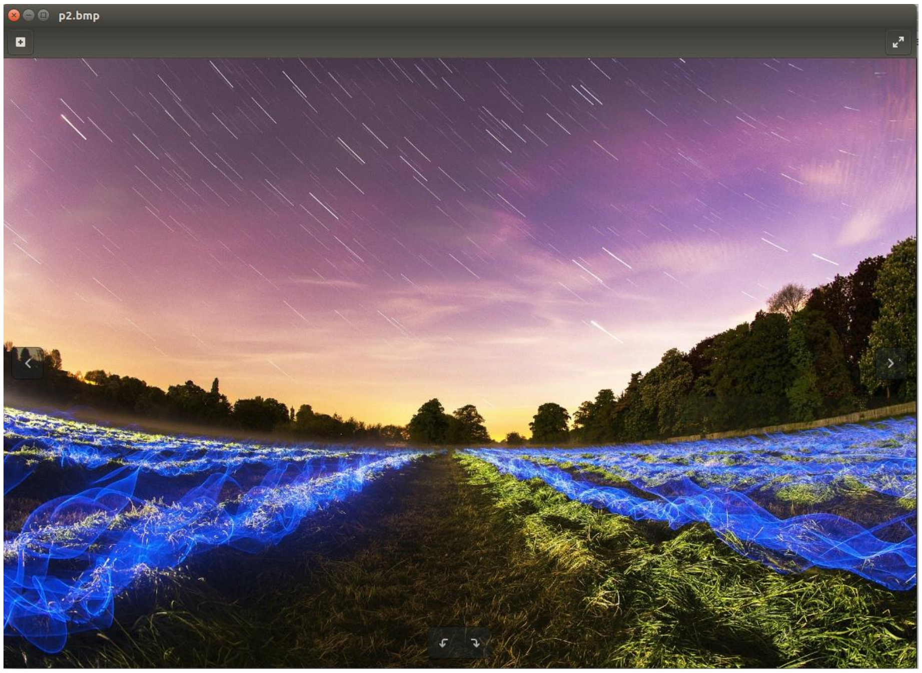
```
[02/12/21]seed@VM:~/CMPSC$ openssl enc -aes-128-cbc -e -in plaintext.txt -out ci
pher.bin -K 00112233445566778899aabbccddeeff -iv 0102030405060708
[02/12/21]seed@VM:~/CMPSC$ openssl enc -aes-128-cfb -e -in plaintext.txt -out ci
pher.bin -K 00112233445566778899aabbccddeeff -iv 0102030405060708
[02/12/21]seed@VM:~/CMPSC$ openssl enc -aes-128-cfb -e -in plaintext.txt -out ci
pher.bin -K 00112233445566778899aabbccddeeff -iv 0102030405060708
[02/12/21]seed@VM:~/CMPSC$
```

I used the 3 different ones that were given to us in the lab pdf. It made it pretty easy to see and reflect on which encryptions did what.

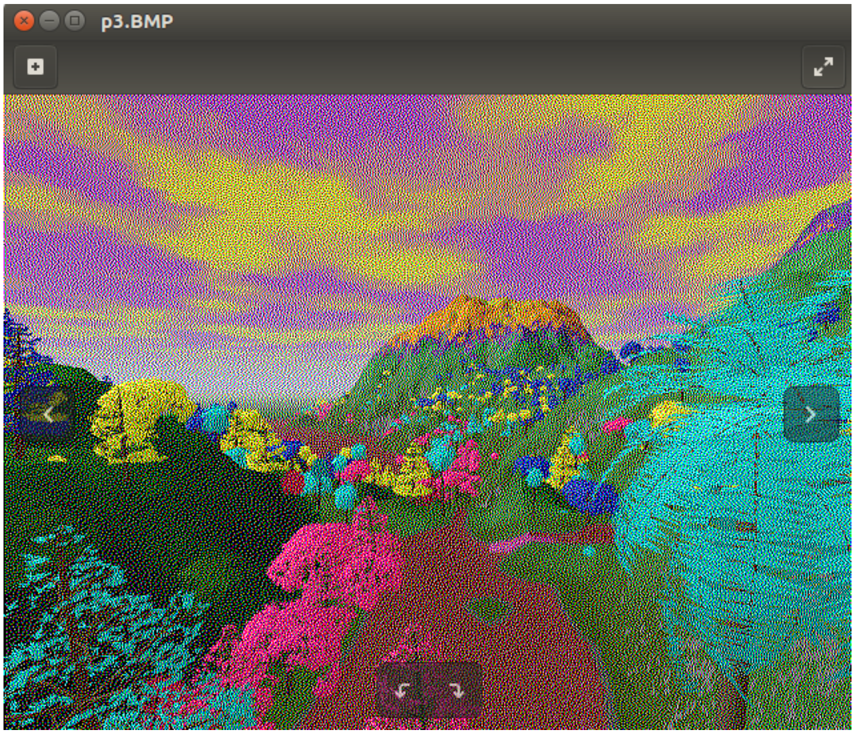
Task 3



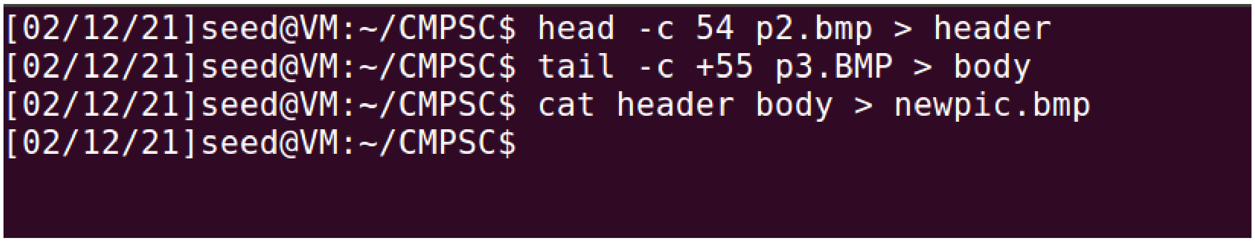
This was the new picture (for p2 I used a picture off the internet, which I will use for my example as well). As we can see, there is not much we can make out from this picture. It seems really well encrypted and not able to be used in any wrong way. It doesn't seem easy to crack or solve.



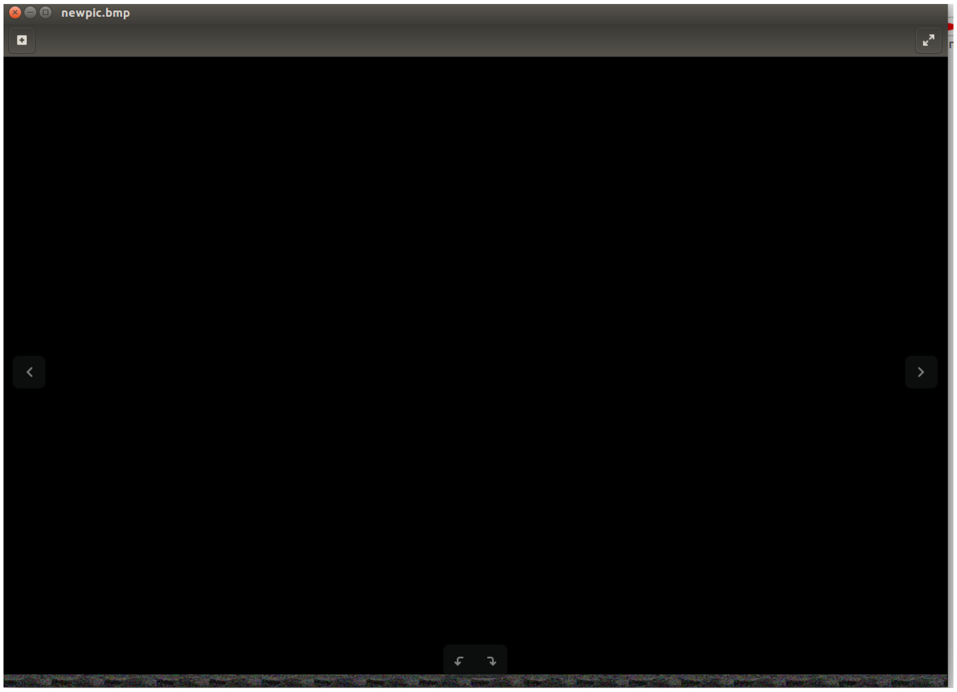
This is our p2.bmp



This is our p3.bmp. When we do the same procedure, our output is below.



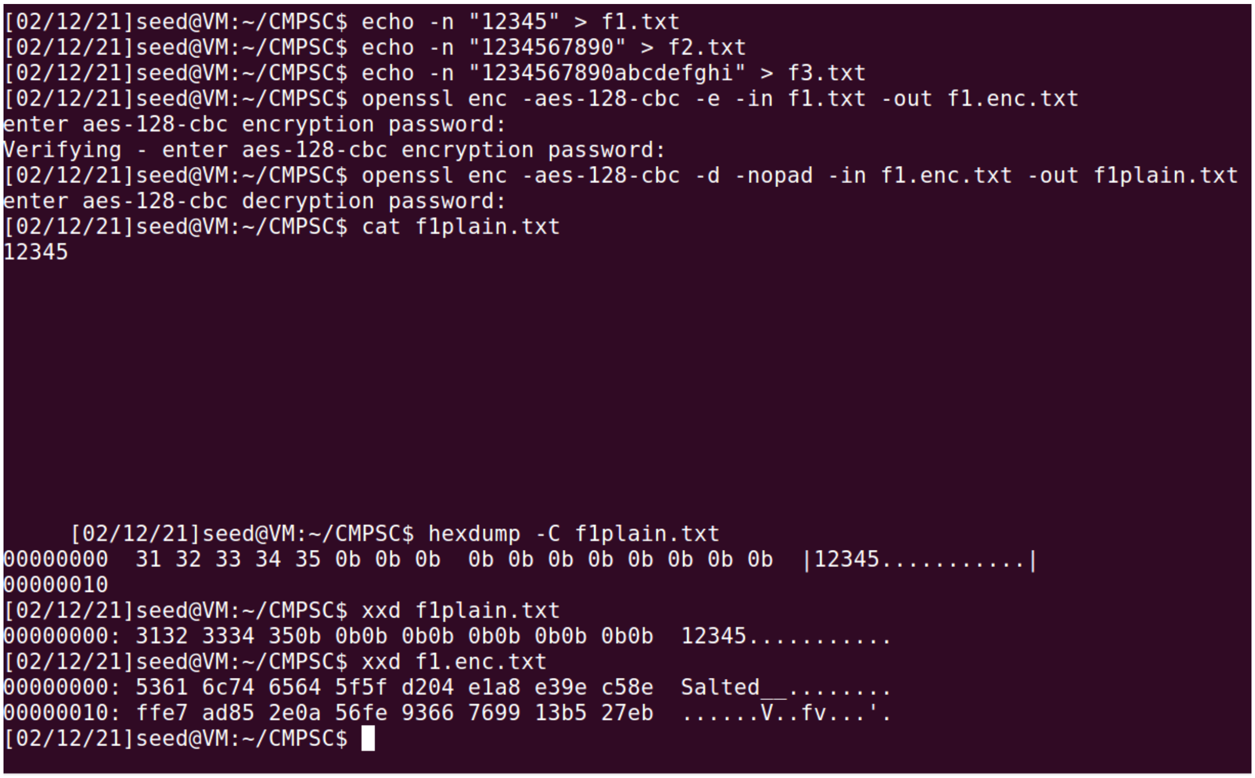
```
[02/12/21]seed@VM:~/CMPSC$ head -c 54 p2.bmp > header
[02/12/21]seed@VM:~/CMPSC$ tail -c +55 p3.BMP > body
[02/12/21]seed@VM:~/CMPSC$ cat header body > newpic.bmp
[02/12/21]seed@VM:~/CMPSC$
```



Our output does not come out ideal at all. We see an all-black screen, with some fuzzy at the bottom. Not sure what occurred, but still we cannot tell the pictures we combined.

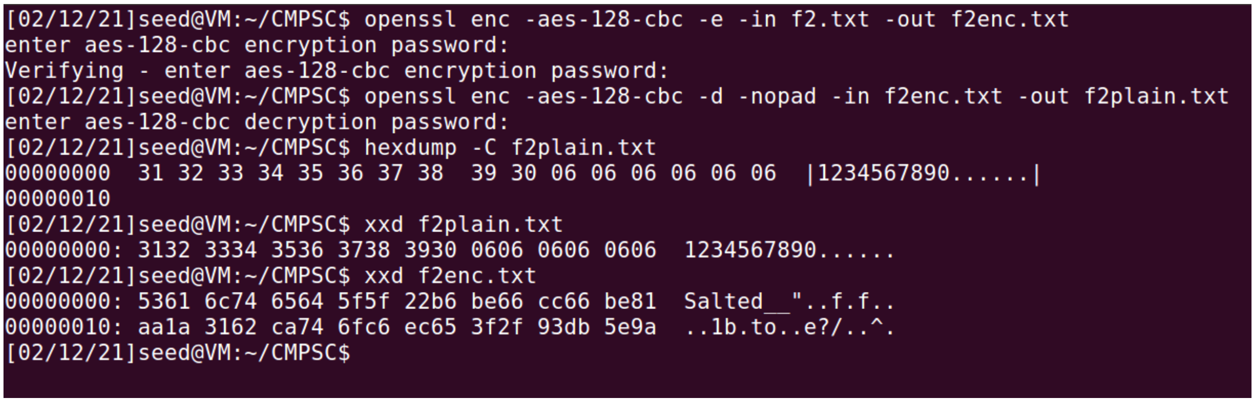
Task 4

F1



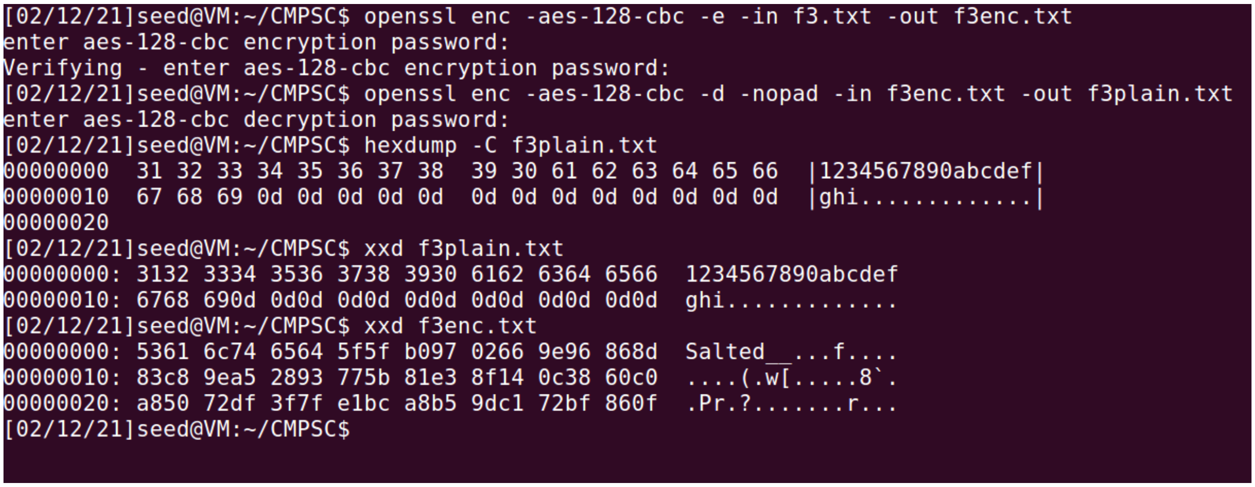
```
[02/12/21]seed@VM:~/CMPSC$ echo -n "12345" > f1.txt
[02/12/21]seed@VM:~/CMPSC$ echo -n "1234567890" > f2.txt
[02/12/21]seed@VM:~/CMPSC$ echo -n "1234567890abcdefghi" > f3.txt
[02/12/21]seed@VM:~/CMPSC$ openssl enc -aes-128-cbc -e -in f1.txt -out f1.enc.txt
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
[02/12/21]seed@VM:~/CMPSC$ openssl enc -aes-128-cbc -d -nopad -in f1.enc.txt -out f1plain.txt
enter aes-128-cbc decryption password:
[02/12/21]seed@VM:~/CMPSC$ cat f1plain.txt
12345









     [02/12/21]seed@VM:~/CMPSC$ hexdump -C f1plain.txt
00000000  31 32 33 34 35 0b 0b 0b  0b 0b 0b 0b 0b 0b 0b 0b  |12345...........|
00000010
[02/12/21]seed@VM:~/CMPSC$ xxd f1plain.txt
00000000: 3132 3334 350b 0b0b 0b0b 0b0b 0b0b 0b0b  12345...........
[02/12/21]seed@VM:~/CMPSC$ xxd f1.enc.txt
00000000: 5361 6c74 6564 5f5f d204 e1a8 e39e c58e  Salted__........
00000010: ffe7 ad85 2e0a 56fe 9366 7699 13b5 27eb  ......V..fv...'.
[02/12/21]seed@VM:~/CMPSC$ 
```

F2



```
[02/12/21]seed@VM:~/CMPSC$ openssl enc -aes-128-cbc -e -in f2.txt -out f2enc.txt
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
[02/12/21]seed@VM:~/CMPSC$ openssl enc -aes-128-cbc -d -nopad -in f2enc.txt -out f2plain.txt
enter aes-128-cbc decryption password:
[02/12/21]seed@VM:~/CMPSC$ hexdump -C f2plain.txt
00000000  31 32 33 34 35 36 37 38  39 30 06 06 06 06 06 06  |1234567890......|
00000010
[02/12/21]seed@VM:~/CMPSC$ xxd f2plain.txt
00000000: 3132 3334 3536 3738 3930 0606 0606 0606  1234567890......
[02/12/21]seed@VM:~/CMPSC$ xxd f2enc.txt
00000000: 5361 6c74 6564 5f5f 22b6 be66 cc66 be81  Salted__"..f.f..
00000010: aa1a 3162 ca74 6fc6 ec65 3f2f 93db 5e9a  ..1b.to..e?/..^.
[02/12/21]seed@VM:~/CMPSC$
```

F3



```
[02/12/21]seed@VM:~/CMPSC$ openssl enc -aes-128-cbc -e -in f3.txt -out f3enc.txt
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
[02/12/21]seed@VM:~/CMPSC$ openssl enc -aes-128-cbc -d -nopad -in f3enc.txt -out f3plain.txt
enter aes-128-cbc decryption password:
[02/12/21]seed@VM:~/CMPSC$ hexdump -C f3plain.txt
00000000  31 32 33 34 35 36 37 38  39 30 61 62 63 64 65 66  |1234567890abcdef|
00000010  67 68 69 0d 0d 0d 0d 0d  0d 0d 0d 0d 0d 0d 0d 0d  |ghi.............|
00000020
[02/12/21]seed@VM:~/CMPSC$ xxd f3plain.txt
00000000: 3132 3334 3536 3738 3930 6162 6364 6566  1234567890abcdef
00000010: 6768 690d 0d0d 0d0d 0d0d 0d0d 0d0d 0d0d  ghi.............
[02/12/21]seed@VM:~/CMPSC$ xxd f3enc.txt
00000000: 5361 6c74 6564 5f5f b097 0266 9e96 868d  Salted__...f....
00000010: 83c8 9ea5 2893 775b 81e3 8f14 0c38 60c0  ....(.w[.....8`.
00000020: a850 72df 3f7f e1bc a8b5 9dc1 72bf 860f  .Pr.?.......r...
[02/12/21]seed@VM:~/CMPSC$
```

The padding appears to be based on the number of bytes as far as the file goes. We can see each of the encoding / decoding is different, it really depends on the size and what we encode.

Task 5

As far as the question being asked (ignoring OFB and swapping it with CTR instead)

- ECB mode, I think only one of the blocks would be affected when the cipher text occurs. Furthermore, each of the blocks would be encrypted / decrypted on their own, not all together. It could have an affect on whatever number of bits in the block, but overall just one block.
  - After carrying it out, this was correct
- For CBC mode, in this case I think that two blocks would be affected, like the situation in ECB, but this time with two separate blocks.
  - After carrying it out, this was correct
- I'm not sure what would happen for CFB, I will guess that there will be another number of blocks affected.
  - After carrying it out, it appears there is a problem for (n/r) blocks. I was somewhat on the right track but did not guess this.
- For CTR I will guess that only a specific bit is affected, instead of a whole block
  - It appears that CTR mode treats each block independently. There doesn't seem to be error from one block to another. Furthermore, the encryption / decryption process are the same operation, this speeds up everything.

Task 7

I am not sure how to implement this. I am hoping if I give a brief understanding, it will be enough for me to receive some credit.

I think for this, I would have to start by breaking down the hex values, integers, and even the ASCII to make it match letters and words within the English words file. From there, we would have to reference the file in some way, allow the program to read the entire text file so we can figure out the key. After settling all the numbers, we could then match it with their respective letters, probably passing our information into an array, searching through the array to see what matches and what does not. From there, we could reference the actual text file, figure out which one matches, and which ones do not. Clearly there would only be one result, hence we would have our key.