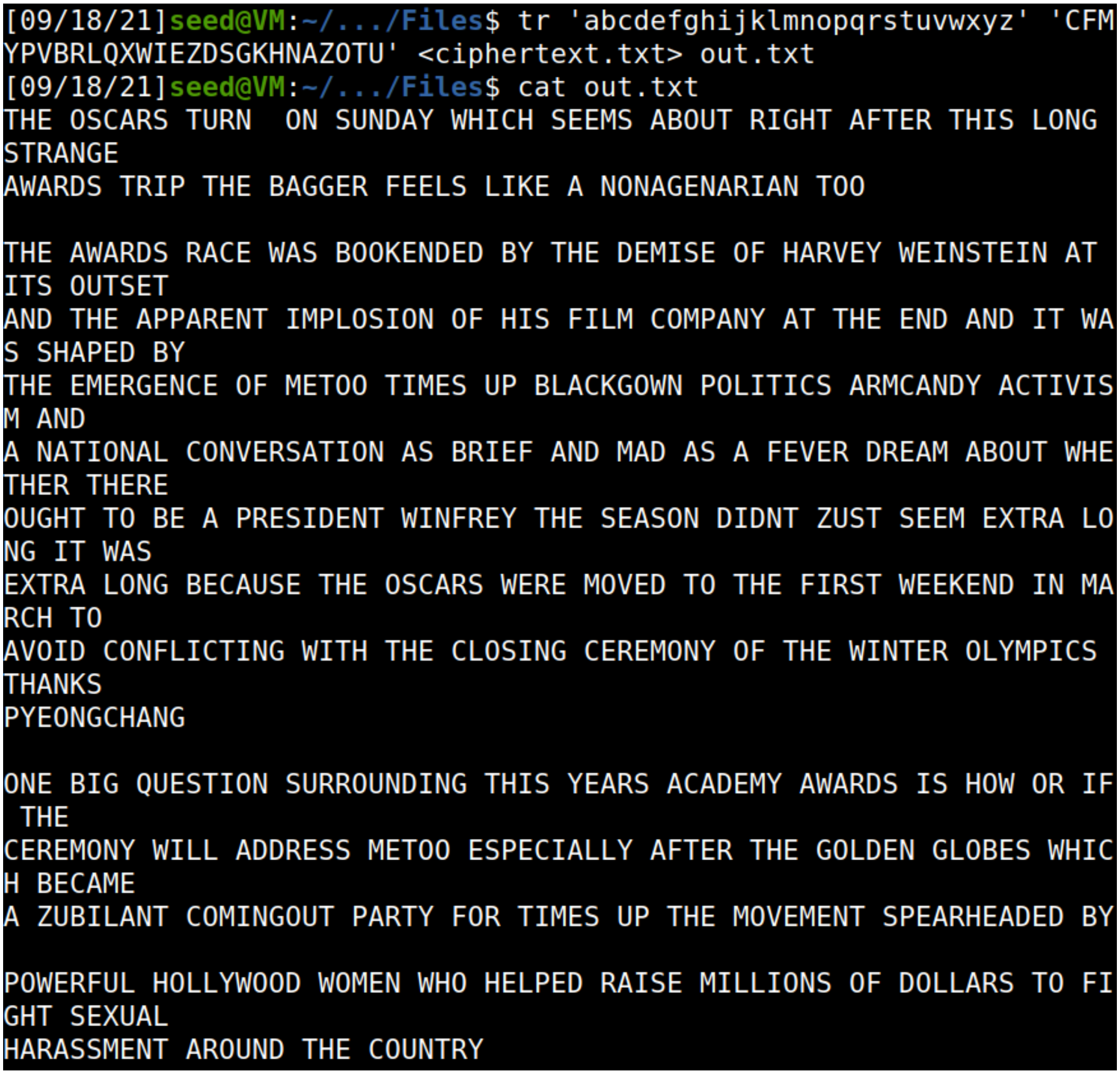
Leonardo Blas

Secret Key Encryption Lab

Task 1



```
[09/18/21]seed@VM:~/.../Files$ tr 'abcdefghijklmnopqrstuvwxyz' 'CFM
YPVBRLQXWIEZDSGKHNAZOTU' <ciphertext.txt> out.txt
[09/18/21]seed@VM:~/.../Files$ cat out.txt
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 WA
S SHAPED BY
THE EMERGENCE OF METOO TIMES UP BLACKGOWN POLITICS ARMCANDY ACTIVIS
M AND
A NATIONAL CONVERSATION AS BRIEF AND MAD AS A FEVER DREAM ABOUT WHE
THER THERE
OUGHT TO BE A PRESIDENT WINFREY THE SEASON DIDNT ZUST SEEM EXTRA LO
NG IT WAS
EXTRA LONG BECAUSE THE OSCARS WERE MOVED TO THE FIRST WEEKEND IN MA
RCH 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 WHIC
H BECAME
A ZUBILANT COMINGOUT PARTY FOR TIMES UP THE MOVEMENT SPEARHEADED BY

POWERFUL HOLLYWOOD WOMEN WHO HELPED RAISE MILLIONS OF DOLLARS TO FI
GHT SEXUAL
HARASSMENT AROUND THE COUNTRY
```

In this snippet, we perform a frequency analysis to replace abc… by CFM… in ciphertext.txt. This is a simplified demonstration, not displaying the trial-and-error efforts performed throughout this operation. And we obtain the deciphered text:

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 ZUST 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 ZUBILANT 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 ZUST 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 ZUDD 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

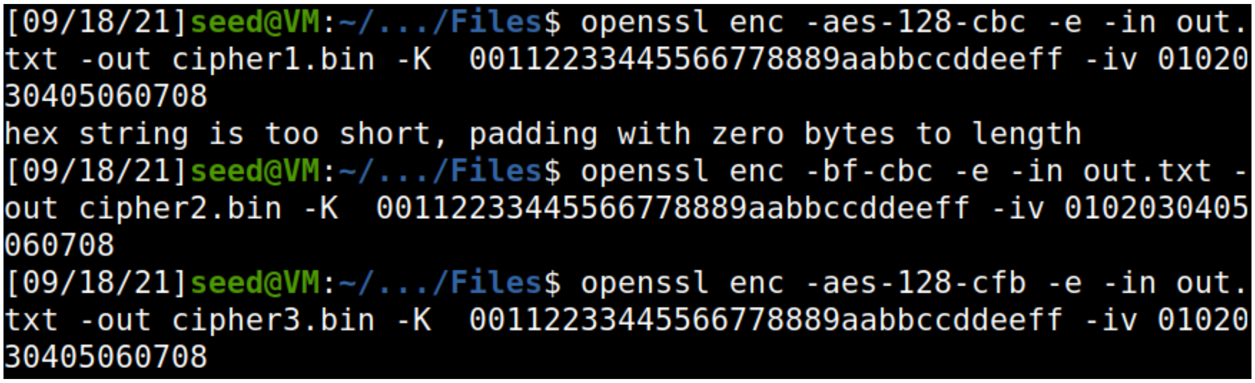
IN IT WAS A TOSSUP BETWEEN BOYHOOD AND THE EVENTUAL WINNER BIRDMAN

IN WITH LOTS OF EXPERTS BETTING ON THE REVENANT OR THE BIG SHORT THE 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 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

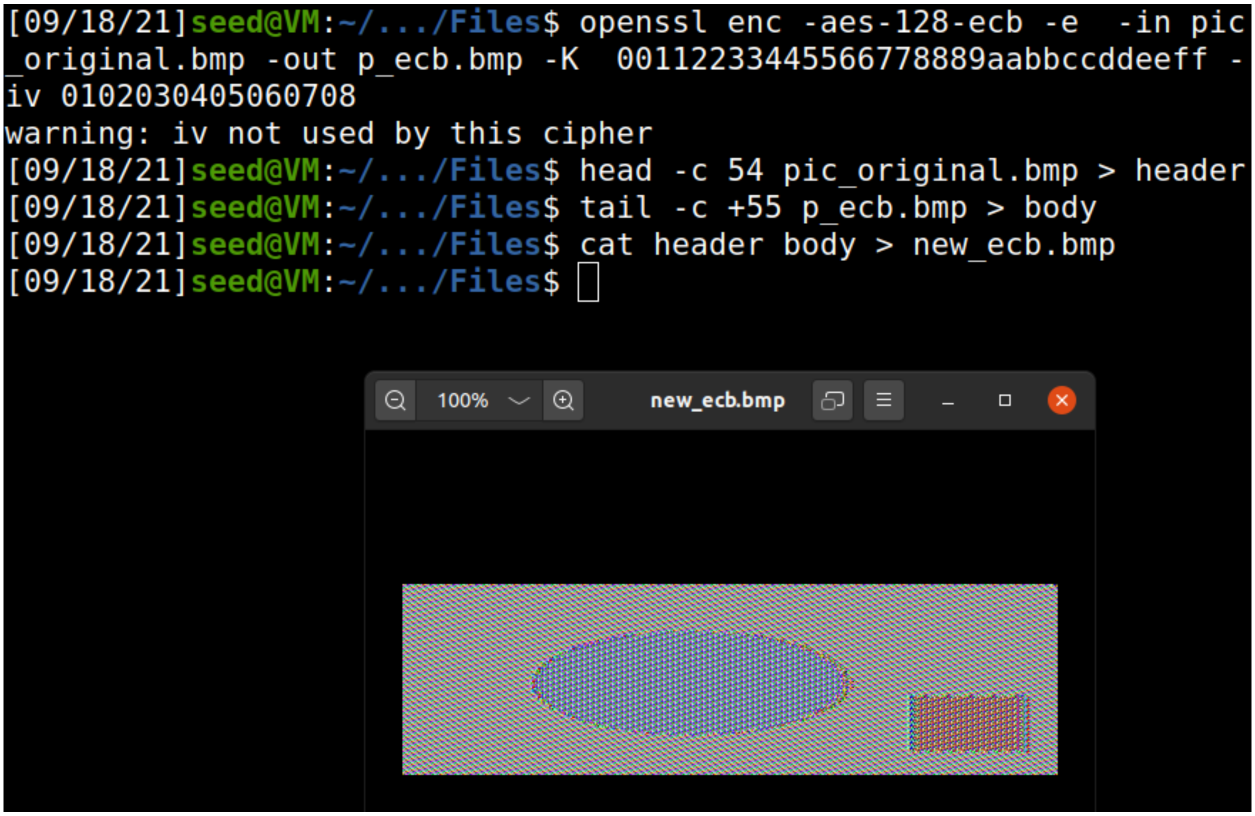
Task 2



```
[09/18/21]seed@VM:~/.../Files$ openssl enc -aes-128-cbc -e -in out.
txt -out cipher1.bin -K  00112233445566778889aabbccddeeff -iv 01020
30405060708
hex string is too short, padding with zero bytes to length
[09/18/21]seed@VM:~/.../Files$ openssl enc -bf-cbc -e -in out.txt -
out cipher2.bin -K  00112233445566778889aabbccddeeff -iv 0102030405
060708
[09/18/21]seed@VM:~/.../Files$ openssl enc -aes-128-cfb -e -in out.
txt -out cipher3.bin -K  00112233445566778889aabbccddeeff -iv 01020
30405060708
```

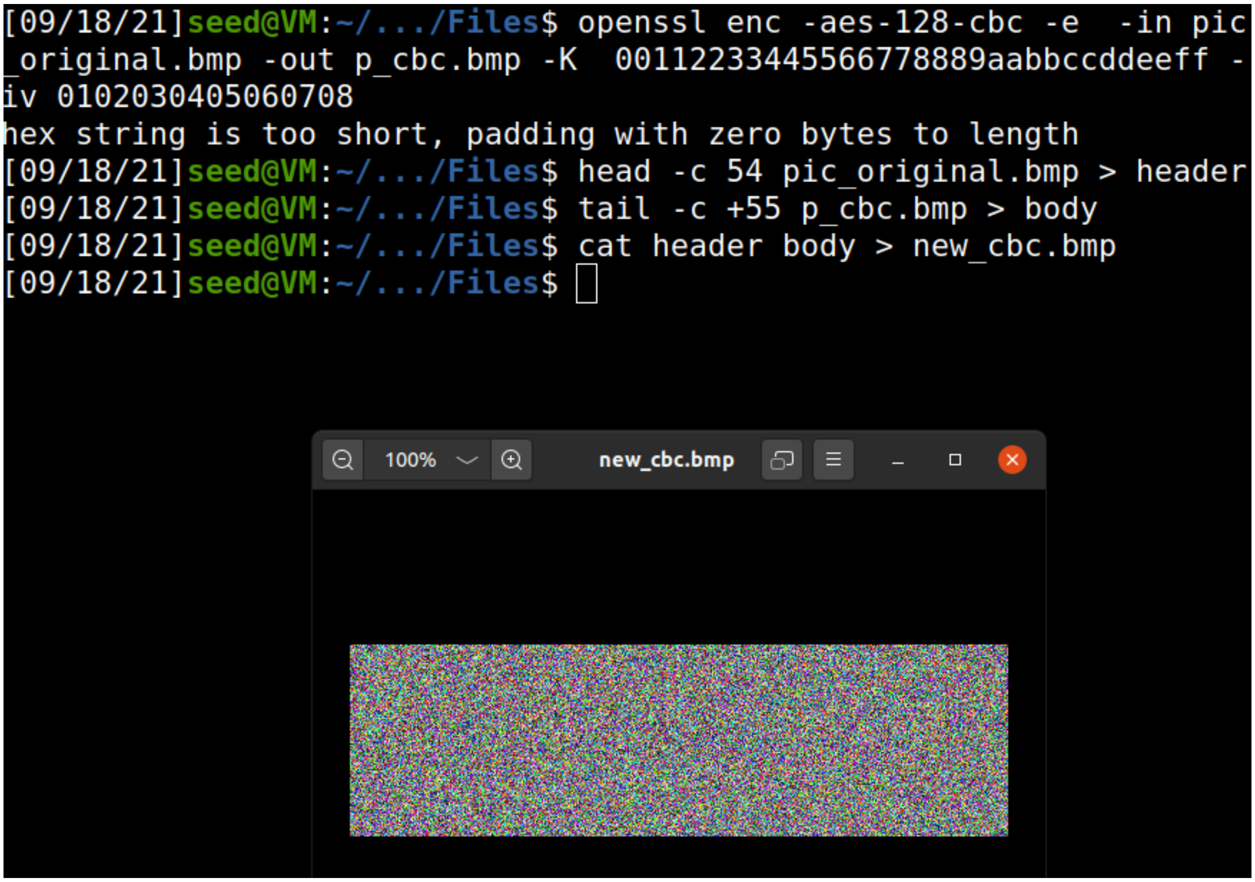
In this snippet, we encrypt our recently decrypted ciphertext using different three cipher types, -aes-128-cbc, -bf-cbc, and -aes-128-cfb

Task 3



```
[09/18/21]seed@VM:~/.../Files$ openssl enc -aes-128-ecb -e  -in pic
_original.bmp -out p_ecb.bmp -K  00112233445566778889aabbccddeeff -
iv 0102030405060708
warning: iv not used by this cipher
[09/18/21]seed@VM:~/.../Files$ head -c 54 pic_original.bmp > header
[09/18/21]seed@VM:~/.../Files$ tail -c +55 p_ecb.bmp > body
[09/18/21]seed@VM:~/.../Files$ cat header body > new_ecb.bmp
[09/18/21]seed@VM:~/.../Files$ 
```

In this snippet, we encrypt original.bmp using ECB encryption. Note how, since we are using ECB, the encryption does not use the provided IV.



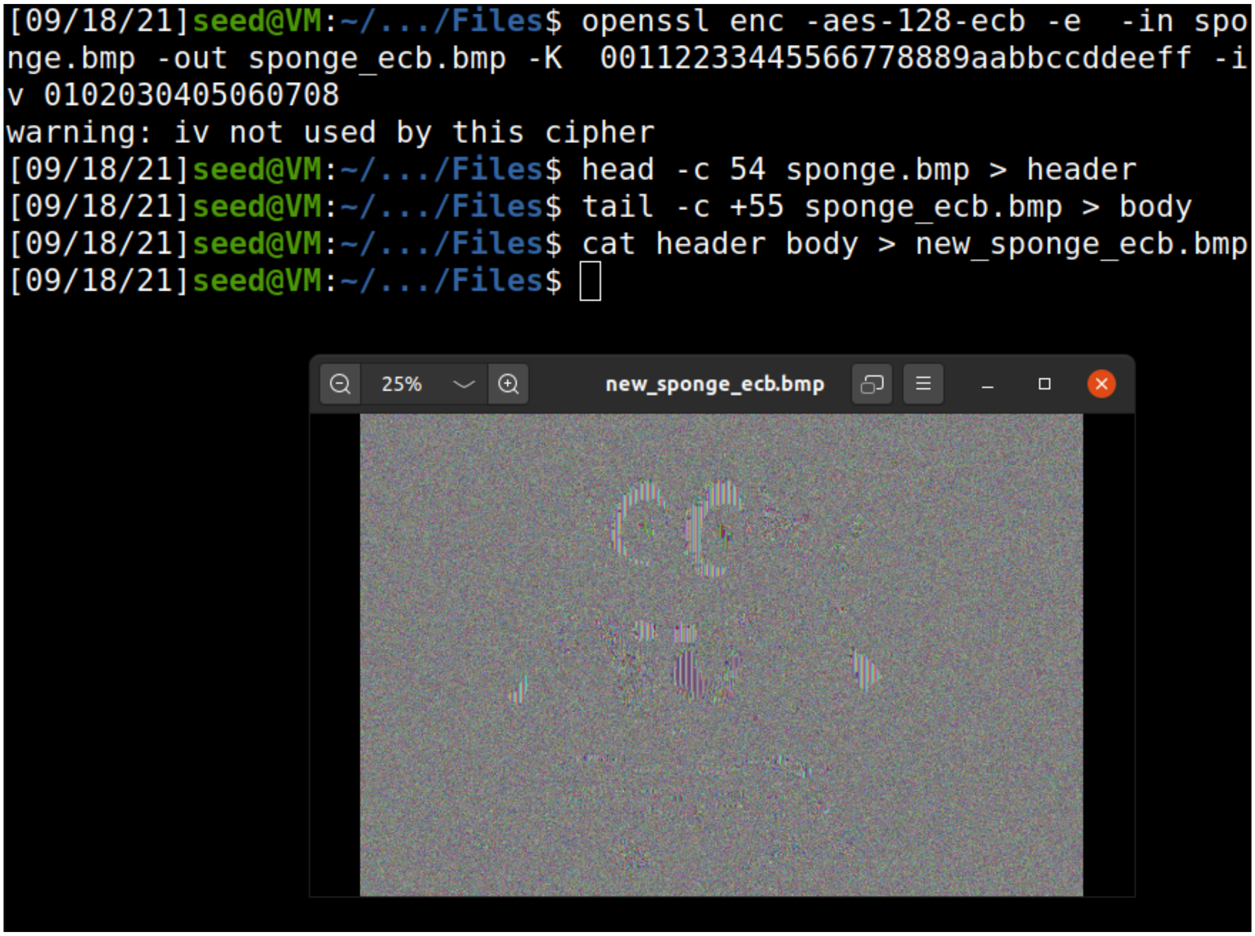
```
[09/18/21]seed@VM:~/.../Files$ openssl enc -aes-128-cbc -e  -in pic
_original.bmp -out p_cbc.bmp -K  00112233445566778889aabbccddeeff -
iv 0102030405060708
hex string is too short, padding with zero bytes to length
[09/18/21]seed@VM:~/.../Files$ head -c 54 pic_original.bmp > header
[09/18/21]seed@VM:~/.../Files$ tail -c +55 p_cbc.bmp > body
[09/18/21]seed@VM:~/.../Files$ cat header body > new_cbc.bmp
[09/18/21]seed@VM:~/.../Files$ 
```

In this snippet, we encrypt original.bmp using CBC encryption.

As we can see, we can extract useful information from simply observing an ECB encrypted image. This is because the encrypted information is simply substituted, and while the substitutions mask the information, they don't mask the information patterns. These patterns could give us clues about the message, as we see in the ECB encrypted image.

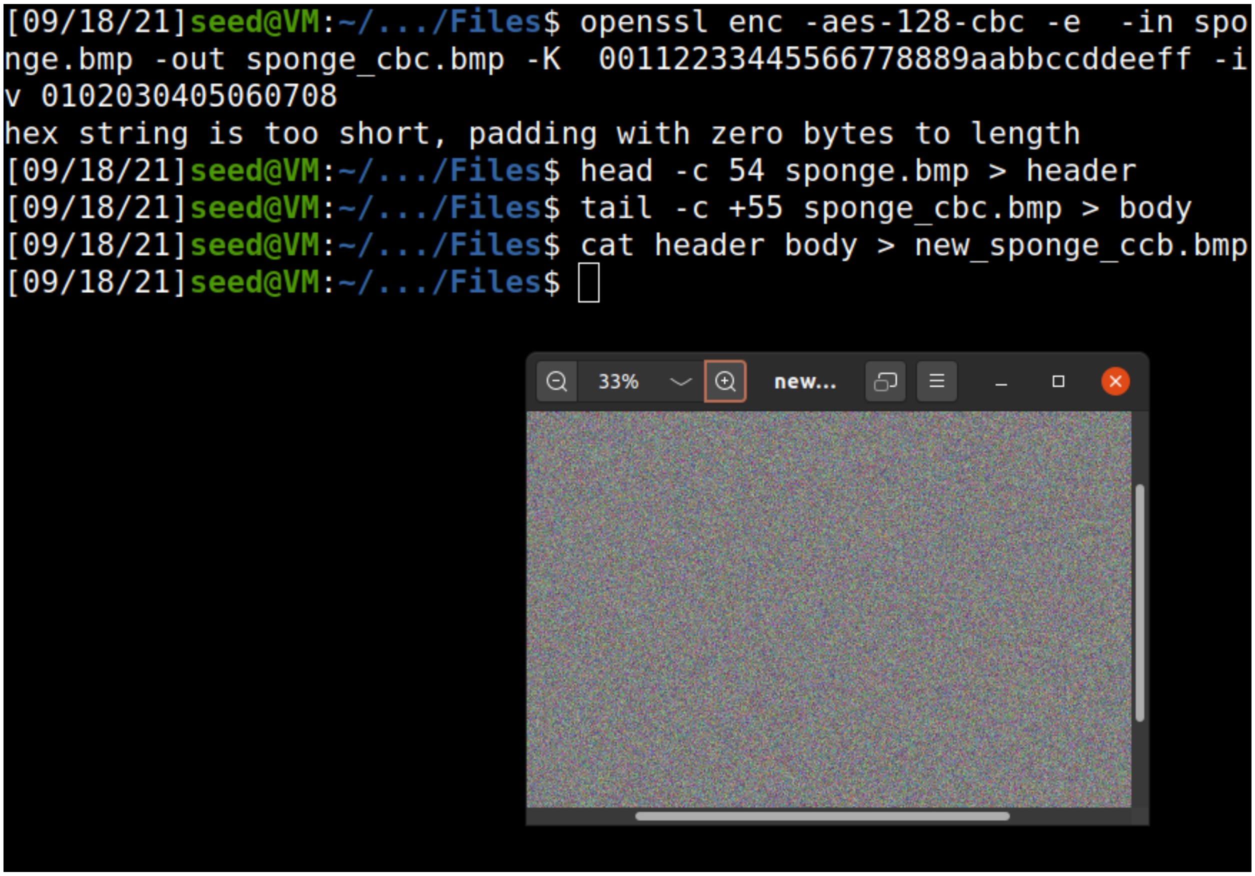
On the other hand, we cannot extract useful information from simply observing a CBC encrypted image. This is because of the extra steps the CBC method takes to increase safety, using an IV and chaining to mask both the information and the information patterns.

This is another image to encrypt, sponge.bmp.



```
[09/18/21]seed@VM:~/.../Files$ openssl enc -aes-128-ecb -e  -in spo
nge.bmp -out sponge_ecb.bmp -K  00112233445566778889aabbccddeeff -i
v 0102030405060708
warning: iv not used by this cipher
[09/18/21]seed@VM:~/.../Files$ head -c 54 sponge.bmp > header
[09/18/21]seed@VM:~/.../Files$ tail -c +55 sponge_ecb.bmp > body
[09/18/21]seed@VM:~/.../Files$ cat header body > new_sponge_ecb.bmp
[09/18/21]seed@VM:~/.../Files$ 
```

In this snippet, we encrypt sponge.bmp using ECB encryption. Note how, since we are using ECB, the encryption does not use the provided IV.



```
[09/18/21]seed@VM:~/.../Files$ openssl enc -aes-128-cbc -e  -in spo
nge.bmp -out sponge_cbc.bmp -K  00112233445566778889aabbccddeeff -i
v 0102030405060708
hex string is too short, padding with zero bytes to length
[09/18/21]seed@VM:~/.../Files$ head -c 54 sponge.bmp > header
[09/18/21]seed@VM:~/.../Files$ tail -c +55 sponge_cbc.bmp > body
[09/18/21]seed@VM:~/.../Files$ cat header body > new_sponge_ccb.bmp
[09/18/21]seed@VM:~/.../Files$ 
```

In this snippet, we encrypt sponge.bmp using ECB encryption.

Once more, we notice how the ECB encryption method partially reveals useful information to the naked eye. On the other hand, we cannot extract useful information from simply observing the CBC encrypted image.