System Security

EECS 121

HW1

Kyle Zyler Cayanan

80576955

01/31/2024

# 1 - Frequency Analysis

When starting this task I started analyzing the most frequent trigrams and then moving onto bigrams. I began with translating the top 2 ranking bigrams and trigrams. From there it took some tedious work to translate the rest of the consonants. My thought process started with trigrams → bigrams → vowels → consonants based on guess work. The screenshots above show the commands that I tried to decipher the plaintext. Eventually the plaintext came out to the following:

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

PRIrE 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

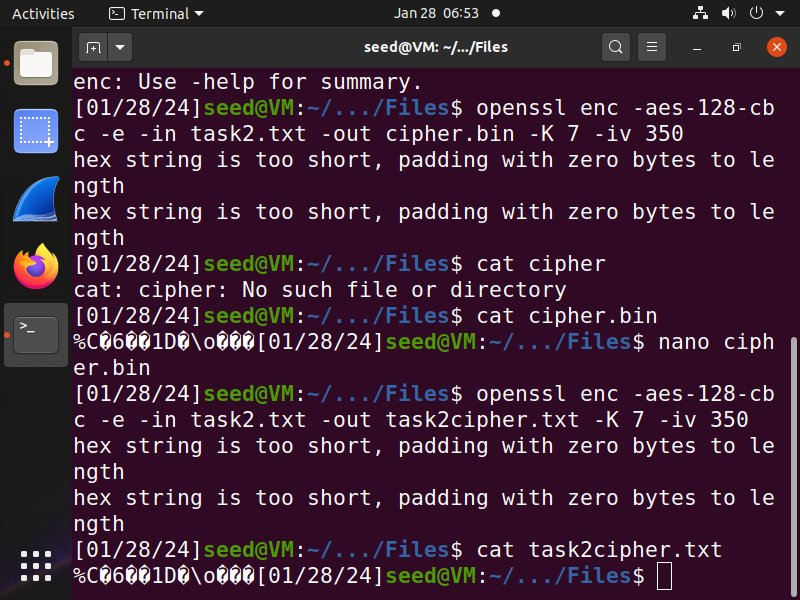
AND THE BAFTA BUT ITS FILMMAKER MARTIN MCDONAGH WAS NOT NOMINATED FOR BEST

DIRECTOR AND APART FROM ARGO MOVIES THAT LAND BEST PICTURE WITHOUT ALSO

EARNING BEST DIRECTOR NOMINATIONS ARE FEW AND FAR BETWEEN

# 2 - Encryption using Different Ciphers and Modes

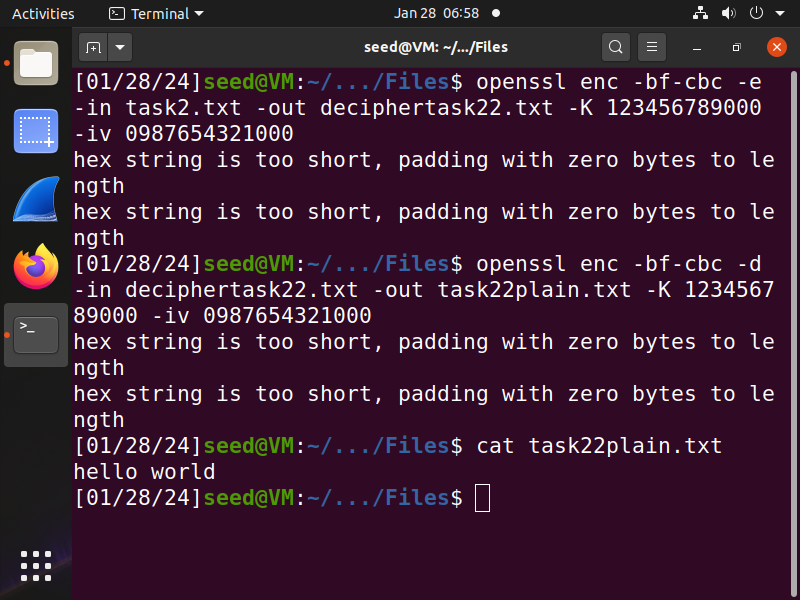
In this task, I simply tried different ciphers, I tried encrypting with the cbc and cgb modes. Through this task I started to get pretty familiar with the openssl command.



In this screenshot I am using the cbc encryption mode with AES. I am using the cat command to confirm that my encryption command was functioning properly.



In this screenshot I am performing a similar task as the previous screenshot but this time around I am deciphering the file.



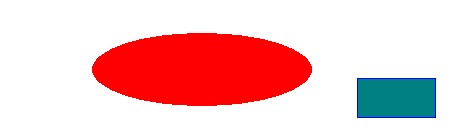
In this screenshot I am trying out the -bf-cbc encryption mode and deciphering it.

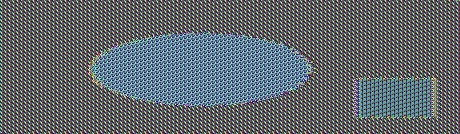
# 

# 3 - Encryption Mode – ECB vs. CBC

Upon encrypting the bmp images using ECB and CBC encryption modes, I noticed when viewing the encrypted files that CBC fully scrambled the pixel values and there was no clear shape within the image. When it came to using the ECB encryption mode, I was able to derive useful information from the images and make out the shapes of the original image. For my own personal image I chose a random map of greenland. I could not see any outline in the CBC encryption for the image but I could definitely make out an outline of the map using the ECB encryption.

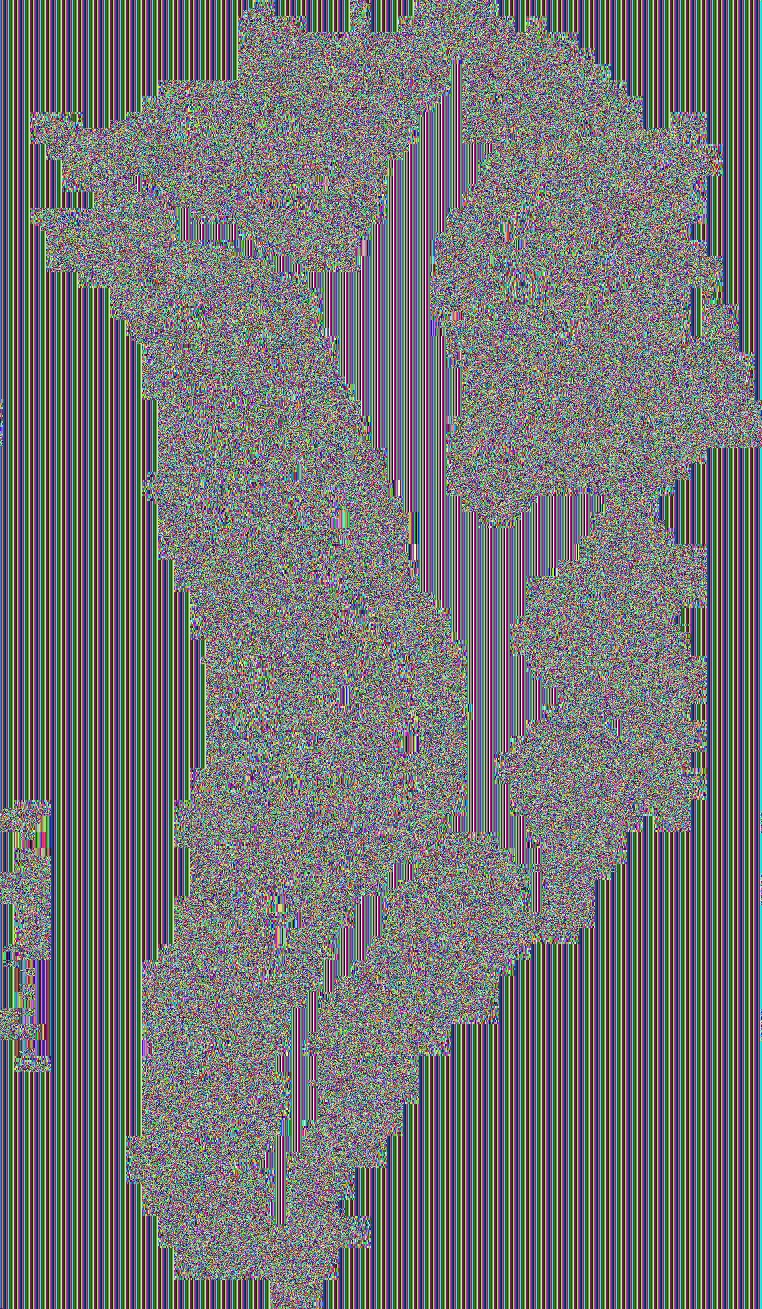
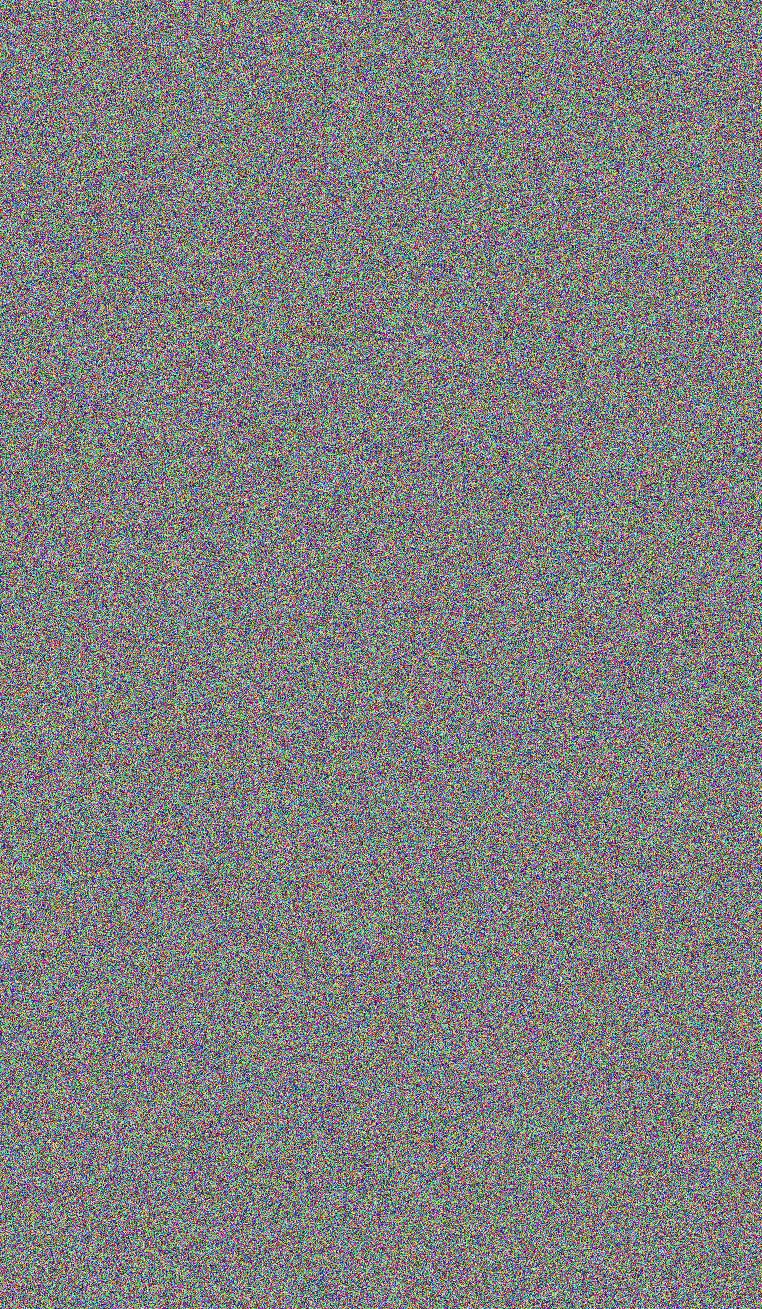
Images provided by the lab:





Images chosen by me:

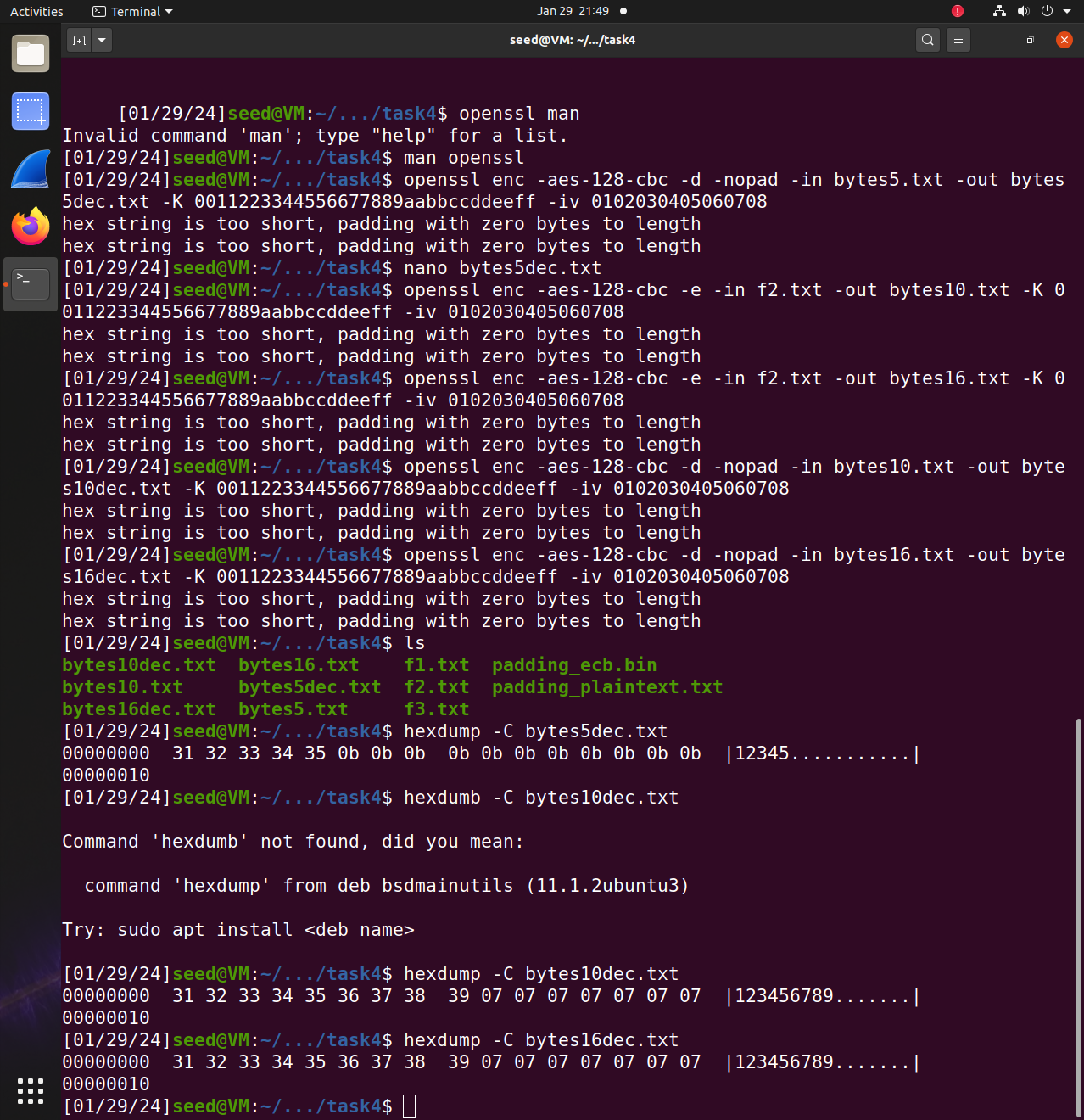




In each of the images above, I show the original image, the CBC encryption, and the ECB encryption respectively.

# 

# 4 - Padding

’

In the screenshot above I am using the hexdump -C command to reveal the changes in the bytes with padding. I use the command on 3 different files of 5 bytes, 10 bytes, and 16 bytes respectively. For the encryptions of each file I had used the CBC mode as specified by the lab that we can use any cipher we want. It seems like each file needed padding due to the Key or Initialization vector being too long or short for the data. Padding would be necessary in this scenario so that the key scheduling of AES would work properly.

We can see what paddings are applied to each file in the screenshot above.

The 5 byte file had paddings of 0b 0b 0b… and so on.

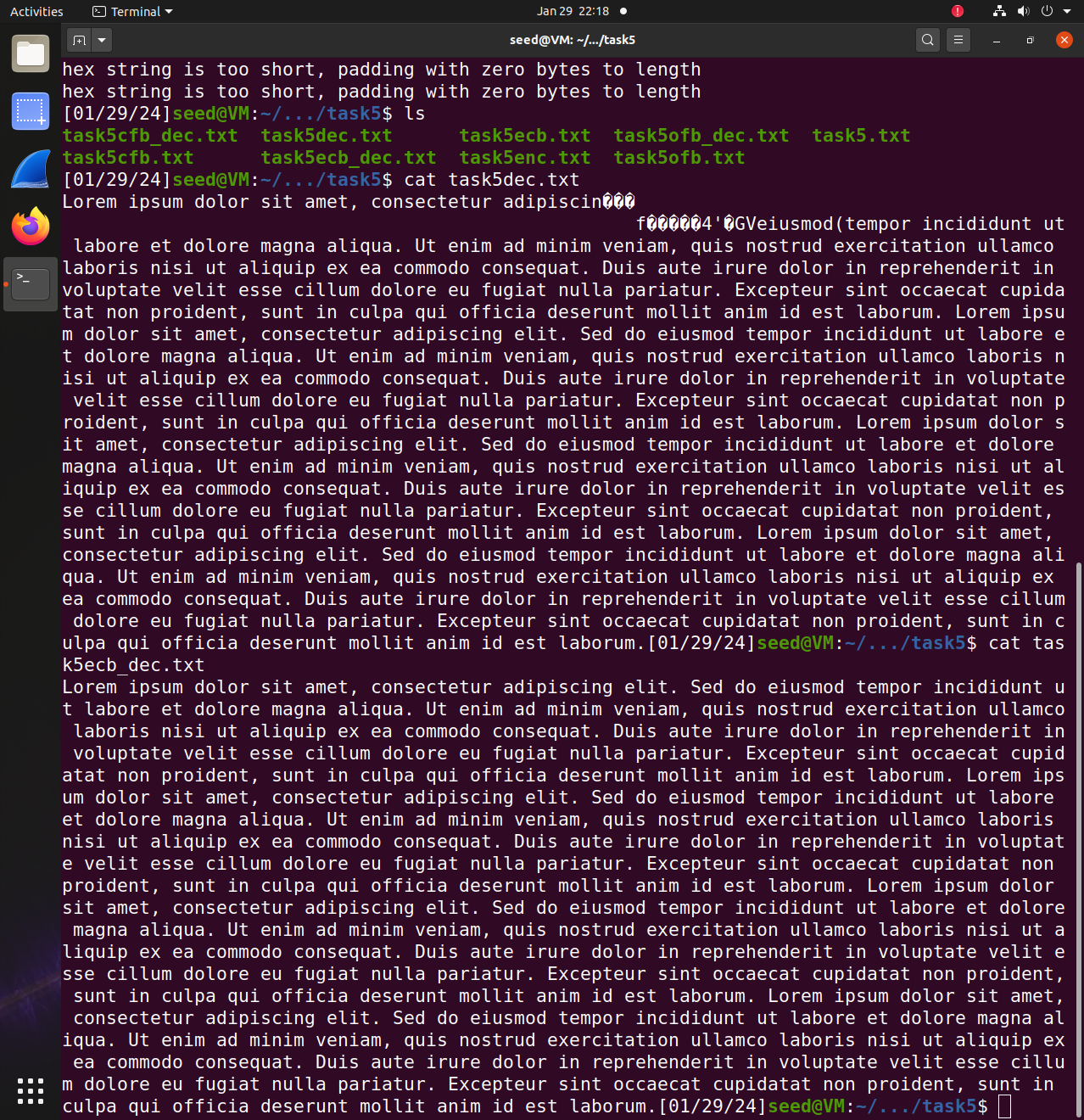
The 10 byte file had padding of 07 07 07… and so on.

The 16 byte file had padding of 07 07 07… and so on as well.

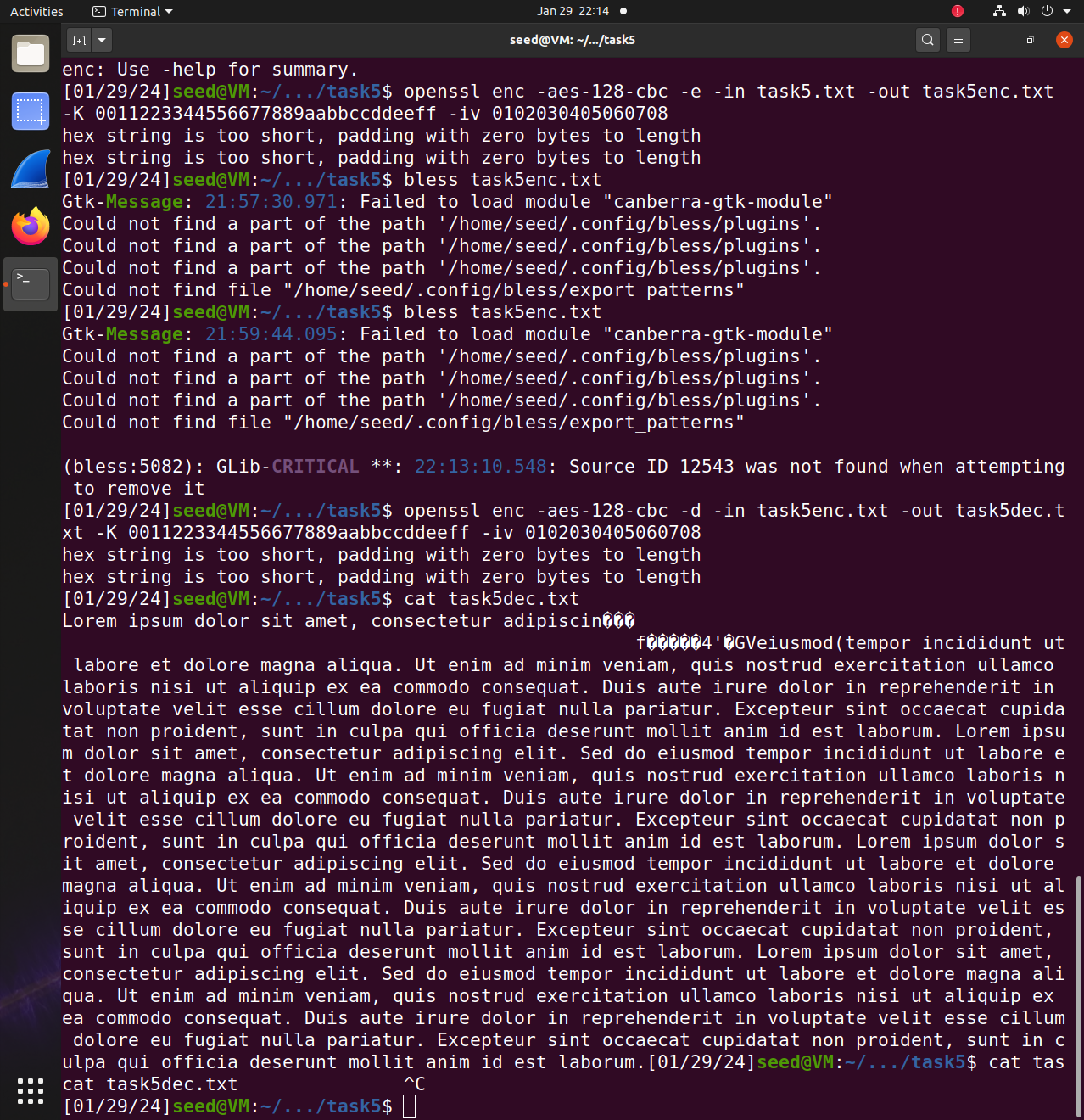
# 

# 5 - Error Propagation – Corrupted Cipher Text

ECB: As we saw from Task 3, ECB is not a very effective cipher so I would have to guess that even if the data is corrupted it would be easily recoverable. Below is the screenshot after answering the original question. It seems that the corruption here is easily detectable and the data is not completely lost.



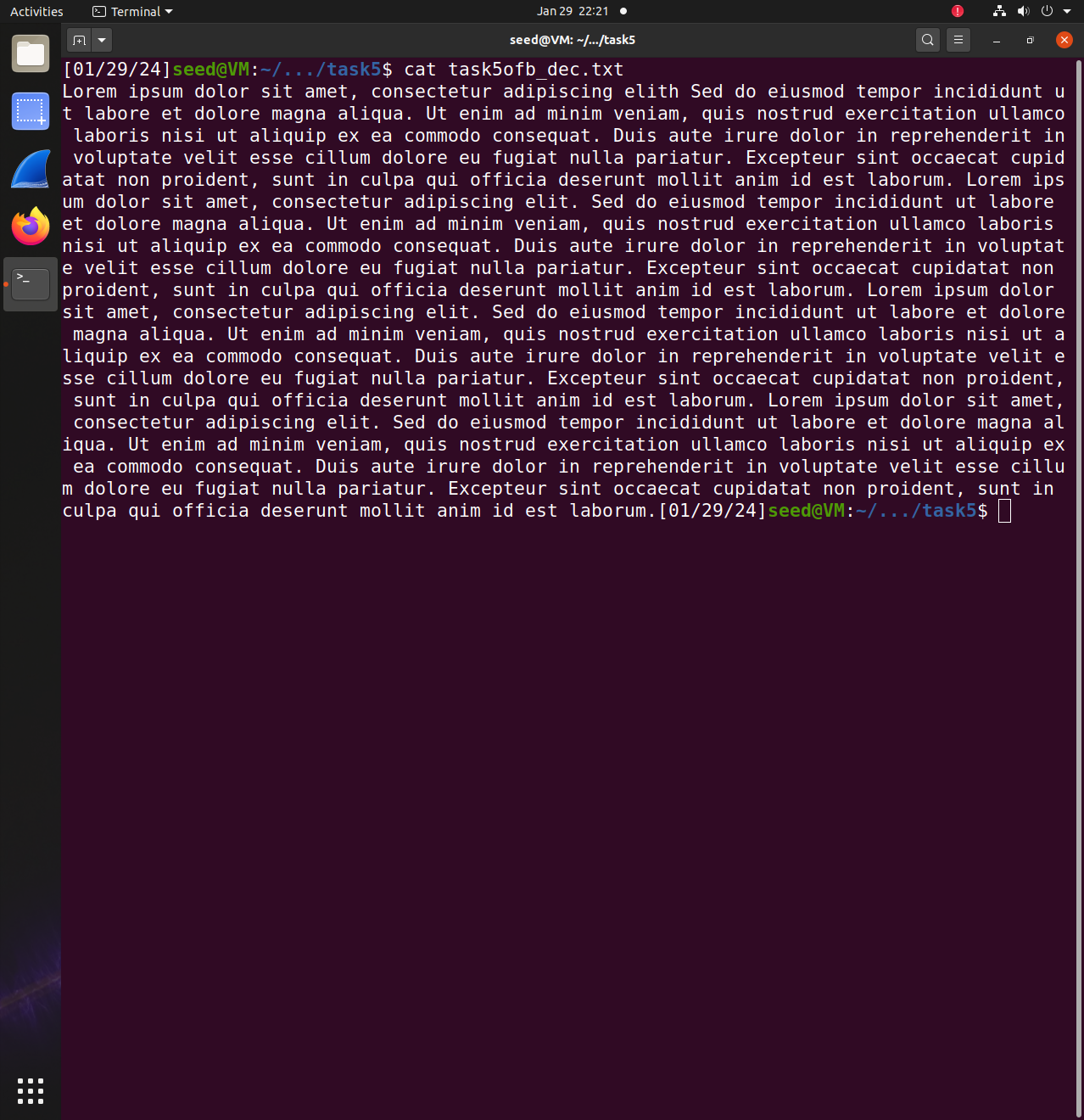
CBC: CBC has proven to be a very efficient cipher so any data that gets corrupted would be difficult to reverse. In the screenshot below I was incorrect in my assumption. We can pinpoint through the corrupted decryption output exactly which byte was affected.



CFB: Since this cipher also uses an Initialization vector and convolutes the data with XOR operations it would be very hard to recover from the corruption. Here I was correct in assuming the recovery from the corruption would prove difficult because we had actually lost data in decrypting the corrupted file.



OFB: Since this cipher also uses an Initialization vector and convolutes the data with XOR operations it would be very hard to recover from the corruption. In this assumption I was incorrect, and all the corrupted data was recovered in the decryption as seen below.

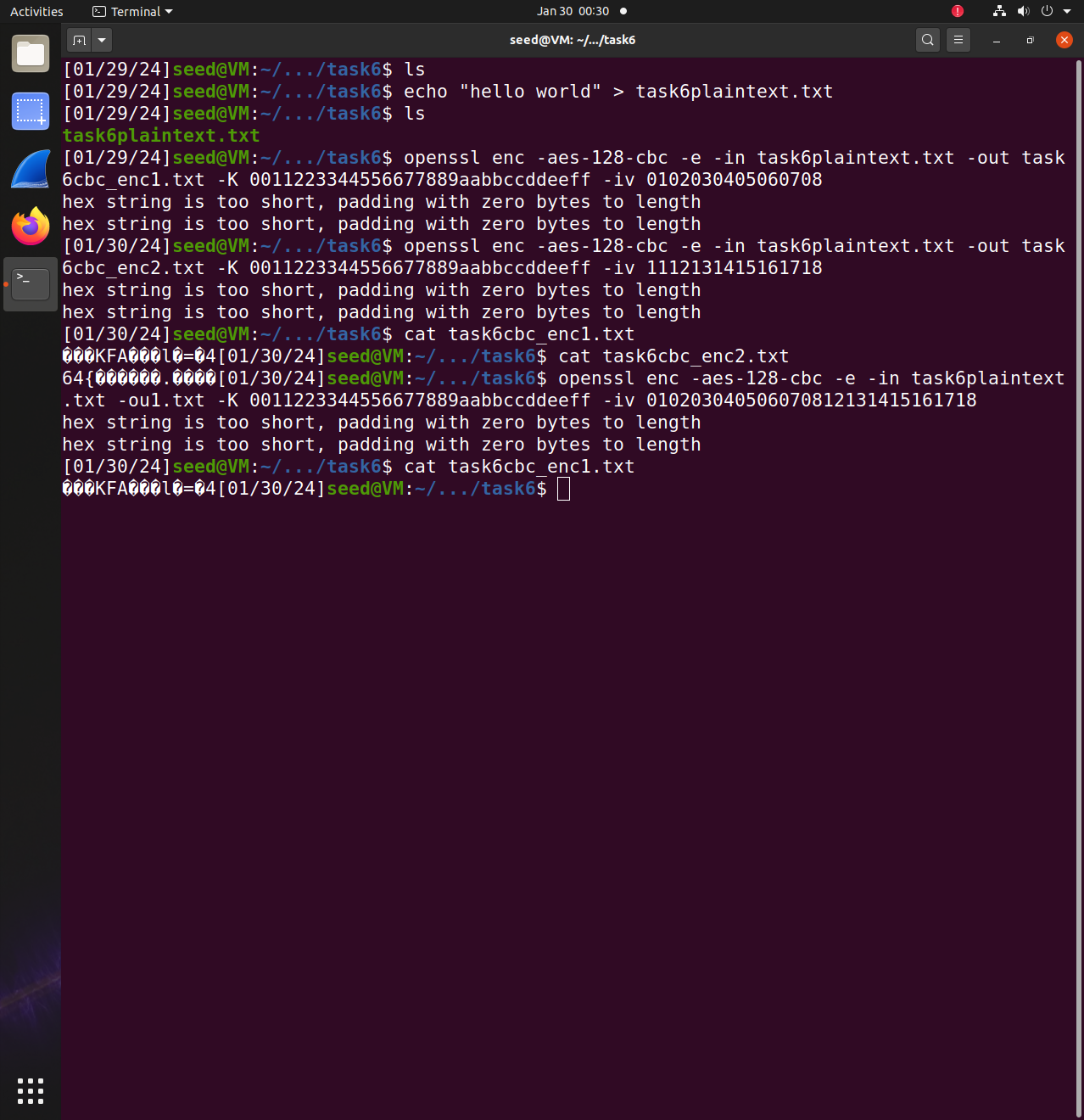


# 

# 6 - Initial Vector (IV) and Common Mistakes

## 6.1: IV Experiment

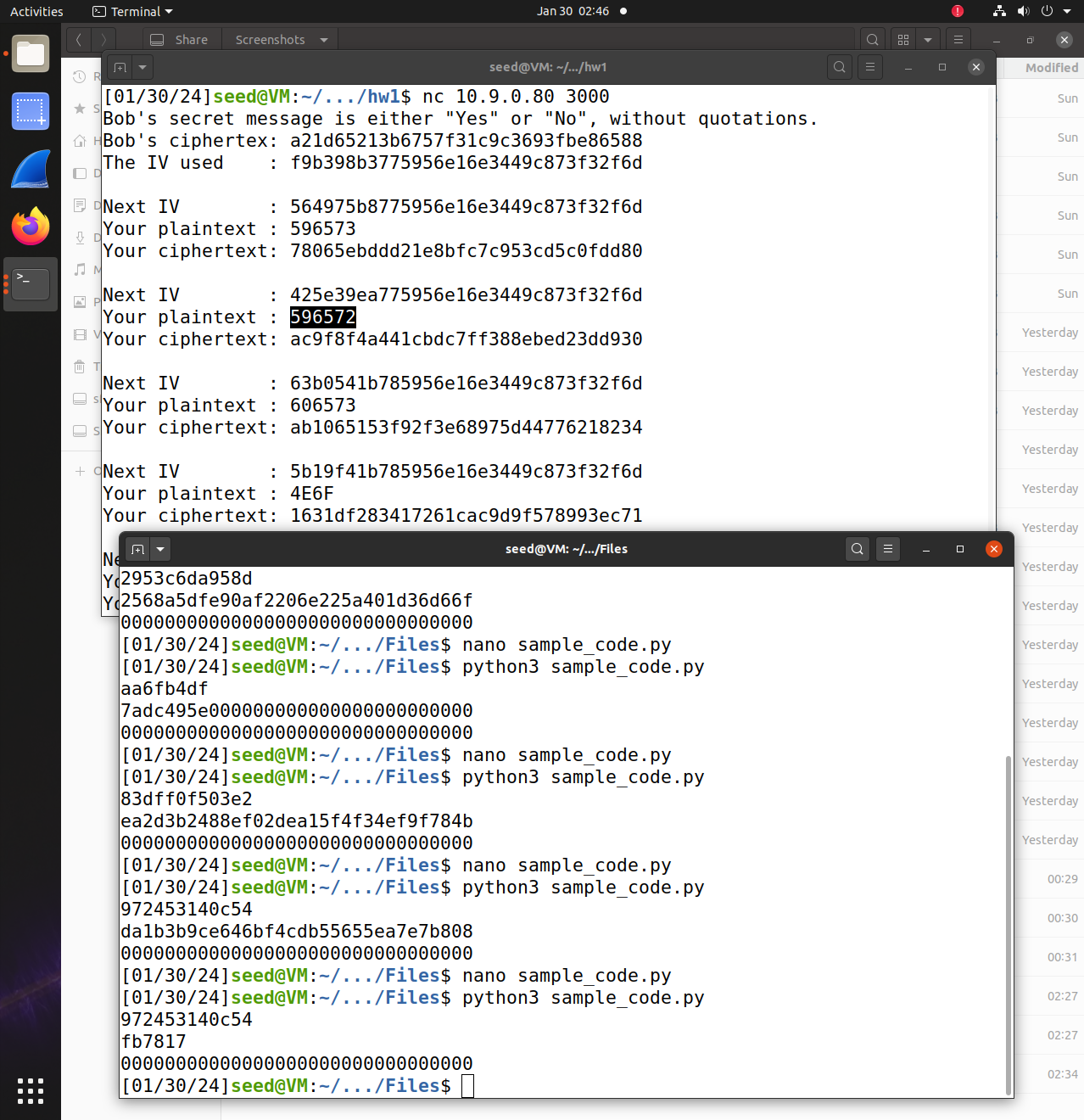
## 

* + 
  + The issue with using the same IV means that you can reproduce the ciphertext by guessing the original plaintext that was used in the encryption. Reproducible encryption leaves vulnerabilities and weakens the strength of the security. In the screenshots above I noticed that the ciphertext would only alter if I changed the IV.

## 6.2: Common Mistake: Use the Same IV

* + Regardless of choice in encryption mode, as long as you know the next IV you can predict also the next ciphertext and use that to work backwards and guess the correct plaintext. For this task, the first few blocks of the plaintext can be revealed so long as the IV is only slightly changed and that the same key is used. If I already know the plaintext that the sender intends to encrypt and I have the next IV, I would be able to use a XOR analysis of their ciphertext and my own to discern whether or not they’re using the same IV. In short, the first few blocks of P2 can be revealed if the encryption mode is changed.

## 6.3: Common Mistake: Use a Predictable IV

* + 
  + In the screenshot above I am interacting with the oracle server and analyzing the similarities and differences of the ciphertext from each interaction. To analyze the ciphertexts I am using XOR analysis with given sample python code given by the lab. With the encryption mode and predictable IVs that Bob is using, it is difficult to discern whether or not Bob’s original message is yes or no. Each the ciphertexts that get produced from each interaction are all unique despite the predictable IVs.