Evan Smith

Internet Security CSE 644

Lab 5

**Task 1 – Frequency Analysis:**

I made a first pass at the translation using the single-letter frequencies as shown here:

A picture containing table

Description automatically generated

This suggests that N maps to E, based on the top frequency. To confirm other assumptions made from this, I used the tool from <https://www.guballa.de/substitution-solver> to obtain the full translation:

*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*

**Observations –** This exercise points out the weakness of a monoalphabetic cypher. By simply looking at the frequency of the cyphertext, is it fairly easy to deduce the cypher itself, provided that the text is sufficiently long. It is conceivable to have a short enough, unusual enough wording that it would be difficult to crack using frequency analysis. For most use cases though, this seems to be a poor choice for encryption.

**Task 2 – Encryption using Different Ciphers and Modes:**

Using the openssl command, I used three different cipher modes, and displayed the output, as shown:

Text, letter

Description automatically generated

**Observations –** By changing the cipher mode, even while using the same key, we can produce ciphertext from the same plain text that is totally different. Not only is the content different, but the length is also varied. It is clear to see that varying any other variables would produce even more varied in the output.

**Task 3- Encryption Mode – ECB vs. CBC**

We start with the original image: Icon

Description automatically generated

We save off the header, encrypt the rest, and then reinsert the header:

Text, letter

Description automatically generated

This produces the following result:

Graphical user interface, background pattern

Description automatically generated

We then do the same with the CBC encryption:

Text

Description automatically generated

This produces a much more encrypted version:

Background pattern

Description automatically generated

We repeat with a different image, with the original shown here:

Graphical user interface, application, Teams

Description automatically generated

After executing the same steps above…

Text, letter

Description automatically generated

We get the ECB version:

Graphical user interface, application

Description automatically generated

And the CBC version:

A screenshot of a computer

Description automatically generated with medium confidence

**Observations:** We see that the ECB encoding is not nearly as successful as the CBC encoding in disguising the overall structure of the images. We can see that the CBC encoding is basically static, even when the secret key is the same between the two. ECB maintains artifacts, especially around strong borders in the images.

**Task 5 – Corrupted Cypher Text:**

For this task, we use a sample text file that is the first page or so of The Hobbit.

We encrypt it using AES-128 encoding for ECB, CBC, CFB, and OFB:

Text

Description automatically generated

These encryptions are then each corrupted in the 55th byte with the byte 00:

ECB before:

Graphical user interface, text, application, table, email

Description automatically generated

After:

Graphical user interface, text, application, table, email

Description automatically generated

CBC before:

Graphical user interface, text, application, table, email

Description automatically generated

After:

Graphical user interface, text, application, email

Description automatically generated

CFB before:

Graphical user interface, text, application, table

Description automatically generated

After:

Graphical user interface, text, application, table, email

Description automatically generated

OFB before:

Graphical user interface, text, application, table, email

Description automatically generated

After:

Graphical user interface, text, application, table, email

Description automatically generated

My predictions about the feasibility of changing the bytes is that ECB will be able to decode the majority of the file, and the corruption will be less impactful. The others will have more of an issue, and may be unable to be decoded at all. CBC will likely be unable to decode anything after the 55th byte, since the encoding of the later bytes is dependent on the previous ones, so a corrupted byte would destroy the final result. Similarly, I expect CFB to be unreadable after the block containing the 55th byte, since it also chains blocks. OFB encodes each block separately, so it should be okay to decode apart from the corrupted block.

We now decode each corrupted file into an output:

Text, letter

Description automatically generated

The ECB file decoded:

Text, letter

Description automatically generated

CBC decoded:

Text, letter

Description automatically generated

CFB decoded:

Text, letter

Description automatically generated

OFB decoded:

A close-up of a document

Description automatically generated with low confidence

**Observations:** My predictions were mostly correct, as shown by the screenshots. We see that for ECB encoding, only the block of data that was corrupted was unable to be properly decoded, which makes sense since each block is encoded separately and without context. For CBC and CFB, the entire file has issues, although CBC has more consistent and larger errors, while CFB is more readable. OFB is completely fine, which was contradictory to my prediction, where I thought the corrupted block wouldn’t come out properly. This suggests that there is error-correction within the encoding process of OFB.