CS166 Section-04
Mikhail Sumawan
Homework 1 - SEED Lab: Secret-Key Encryption

Task 1: Frequency Analysis on Monoalphabetic Substitution Cipher

1.) Given a ciphertext, find out the key and the original plain text file using the help of a frequency analysis program and then guess the ciphertext with the help of a decryption program.
2.) My first step was to do a frequency analysis on the given ciphertext, this is my frequency analysis program coded in Java to determine how many occurrences of each letter within the given ciphertext.
3.) Here are the screenshots of my frequency analysis program in Java:

You can also check the code in my GitHub repo (https://github.com/mikh97/SEEDLabCypherText)

```java
import java.io.IOException;
import java.io.BufferedReader;
import java.util.HashMap;
import java.io.FileReader;
    public class Main {
        public static void main(String[] args) throws IOException {
            HashMap<Integer, Integer> hash = new HashMap<>();

            // File path to the cipher text file
            // I'm using Buffer Reader used to read each of the line in the cipher text file
            BufferedReader reader = new BufferedReader(new FileReader( fileName: "/Users/mikhailsumawan/Desktop/ciphertext.txt"));

            // For loop to read the line
            while (true) {
                String line = reader.readLine();
                // If statement to end the loop if no strings or integers are present in the given line
                if (line == null) {
                    break;
                }
                for (int i = 0; i < line.length(); i++) {
                    char frequency = line.charAt(i);
                    if (frequency != ' ') {
                        // Count the value of each letter on each line
                        int value = hash.getOrDefault((int) frequency,  defaultValue: 0);
                        hash.put((int) frequency, value + 1);
                    }
                }
            }
            reader.close();

            // For loop to print the frequency analysis given on the cipher text
            for (int key : hash.keySet()) {
                System.out.println((char) key + ": " + hash.get(key));
            }
        }
    }
```

4.) And here's the output I get from running the frequency analysis to the **ciphertext.txt**:

```
/Library/Java/JavaVirtualMachines/jdk-14.0.2.jdk
a: 116
b: 83
c: 104
d: 59
e: 76
f: 49
g: 83
h: 235
i: 166
j: 5
k: 5
l: 90
m: 264
n: 488
o: 4
p: 156
q: 276
r: 82
s: 19
t: 183
u: 280
v: 348
w: 1
x: 291
y: 373
z: 95

Process finished with exit code 0
```

5.) I use this output shown in the frequency analysis to replace the most common letters with the most frequent letter in the English alphabet and guess my way through the plain text. Here's the program that I wrote in Java to replace all the common letters in the ciphertext while running it multiple times until the ciphertext is readable:

```java
import java.io.FileReader;
import java.io.FileWriter;
import java.io.File;
import java.io.IOException;
import java.io.BufferedReader;

    public class Decryption
    {
        static void decryptor(String filePath, String oldString, String newString)
        {
            // Initializing the file path for the ciphertext
            File fileToBeModified = new File(filePath);
            String oldContent = "";
            BufferedReader reader = null;
            FileWriter writer = null;
            try
            {
                // Using BufferReader to read all the lines in the given file
                reader = new BufferedReader(new FileReader(fileToBeModified));
                String line = reader.readLine();

                while (line != null)
                {
                    oldContent = oldContent + line + System.lineSeparator();
                    line = reader.readLine();
                }

                // Method to replace the old encrypted alphabet with the given key
                String newContent = oldContent.replaceAll(oldString, newString);
                writer = new FileWriter(fileToBeModified);
                writer.write(newContent);
            }
            catch (IOException e)
            {
                e.printStackTrace();
            }
```

```java
        finally
        {
            try
            {
                reader.close();
                writer.close();
            }
            catch (IOException e)
            {
                e.printStackTrace();
            }
        }
    }
```

```java
    public static void main(String[] args)
    {
        // Filepath to the given ciphertext
        //
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "n",  newString: "E");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "y",  newString: "T");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "v",  newString: "A");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "x",  newString: "O");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "q",  newString: "S");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "u",  newString: "N");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "m",  newString: "I");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "h",  newString: "R");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "t",  newString: "H");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "i",  newString: "L");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "p",  newString: "D");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "a",  newString: "C");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "c",  newString: "M");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "z",  newString: "U");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "l",  newString: "W");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "b",  newString: "F");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "d",  newString: "Y");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "e",  newString: "P");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "g",  newString: "B");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "r",  newString: "G");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "s",  newString: "K");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "f",  newString: "V");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "j",  newString: "Q");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "k",  newString: "X");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "o",  newString: "J");
        decryptor( filePath: "/Users/mikhailsumawan/Desktop/cpt.txt",  oldString: "w",  newString: "Z");


        System.out.println("done");
    }
}
```

6.) For the **ciphertext.txt** file given from SEED Lab for Task 1, the **output** that I got is below: **(This is the original text from ciphertext.txt)**

cpt.txt

ciphertext.txt | cpt.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 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
```

Line 36, Column 1 Tab Size: 4

```
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

Line 36, Column 1                                          Tab Size: 4
```

Thus, the key to the **ciphertext.txt** by deductive analysis is:

Plain text Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Key Encryption	c	f	m	y	p	v	b	r	l	q	x	w	i	e	j	d	s	g	k	h	n	a	z	o	t	u

Task 1: Frequency Analysis on the ciphertext-o2.txt

1.) I used the same method I did for the first ciphertext.txt, I ran the same frequency analysis code on the ciphertext-o2.txt and got this result:

```
/Library/Java/JavaVirtualMachines/jdk-14.0
a: 495
b: 184
c: 5
d: 10
e: 212
f: 1174
g: 104
h: 241
i: 861
j: 636
k: 141
l: 288
m: 433
n: 825
o: 295
p: 3
q: 860
r: 126
s: 753
t: 10
u: 339
v: 751
w: 179
x: 75
y: 723
z: 589

Process finished with exit code 0
```

2.) Next, I ran the alphabet swapping code to match the ciphertext-o2.txt with the most frequent English alphabets and did a deductive analysis until I found the exact key for this encryption. This is the result that I got after running multiple times to find the right key: **(Original text of ciphertext-o2.txt)**

cpt2.txt

THE FELLOWSHIP OF THE RING
MAIN ARTICLE THE LORD OF THE RINGS THE FELLOWSHIP OF THE RING

IN THE SECOND AGE OF MIDDLEEARTH THE LORDS OF ELDES DWARDES AND MEN ARE GIDEN RINGS OF POWER UNBEKNOWNST TO THEM THE DARK LORD SAURON FORGES THE ONE RING IN MOUNT DOOM INFUSING INTO IT A GREAT PART OF HIS POWER TO DOMINATE THROUGH IT AND AT A DISTANCE THE OTHER RINGS SO HE MIGHT CONQUER MIDDLEEARTH A FINAL ALLIANCE OF MEN AND ELDES BATTLES SAURONS FORCES IN MORDOR WHERE PRINCE ISILDUR OF GONDOR SEDERS SAURONS FINGER AND THE RING WITH IT THEREBY DESTROYING HIS PHYSICAL FORM WITH SAURONS FIRST DEFEAT THE THIRD AGE OF MIDDLEEARTH BEGINS UNFORTUNATELY THE RINGS INFLUENCE CORRUPTS ISILDUR AND RATHER THAN DESTROY THE RING ISILDUR TAKES IT FOR HIMSELF ISILDUR IS LATER KILLED BY ORCS AND THE RING IS LOST FOR YEARS UNTIL IT IS FOUND BY GOLLUM WHO OWNS IT FOR FIDE CENTURIES THE RING IS THEN FOUND BY A HOBBIT NAMED BILBO BAGGINS WHO TURNS INDISIBLE WHEN HE PUTS IT ON BUT IS UNAWARE OF ITS HISTORY

SIXTY YEARS LATER BILBO CELEBRATES HIS TH BIRTHDAY IN THE SHIRE REUNITING WITH HIS OLD FRIEND GANDALF THE GREY BILBO REDEALS THAT HE INTENDS TO LEADE THE SHIRE FOR ONE LAST ADDENTURE AND HE LEADES HIS INHERITANCE INCLUDING THE RING TO HIS NEPHEW FRODO ALTHOUGH BILBO HAS BEGUN TO BECOME CORRUPTED BY THE RING AND TRIES TO KEEP IT FOR HIMSELF GANDALF INTERDENES GANDALF SUSPICIOUS OF THE RING TELLS FRODO TO KEEP IT SECRET AND TO KEEP IT SAFE GANDALF THEN INDESTIGATES THE RING DISCODERS ITS TRUE NATURE AND RETURNS TO WARN FRODO GANDALF ALSO LEARNS THAT GOLLUM WAS TORTURED BY ORCS AND THAT GOLLUM UTTERED TWO WORDS DURING HIS TORTURE SHIRE AND BAGGINS GANDALF INSTRUCTS FRODO TO LEADE THE SHIRE ACCOMPANIED BY HIS FRIEND SAMWISE GAMGEE GANDALF RIDES TO ISENGARD TO MEET WITH FELLOW WIZARD SARUMAN THE WHITE BUT LEARNS THAT HE HAS JOINED FORCES WITH SAURON WHO HAS DISPATCHED HIS NINE UNDEAD NAZGL SERDANTS TO FIND FRODO AFTER A BRIEF BATTLE SARUMAN IMPRISONS GANDALF FRODO AND SAM ARE JOINED BY FELLOW HOBBITS MERRY AND PIPPIN AND THEY EDADE THE NAZGL ARRIDING IN BREE WHERE THEY ARE MEANT TO MEET GANDALF HOWEDER GANDALF NEDER ARRIDES AND THEY ARE INSTEAD AIDED BY A RANGER NAMED STRIDER A FRIEND OF GANDALFS WHO PROMISES TO ESCORT THEM TO RIDENDELL THE HOBBITS ARE AMBUSHED BY THE NAZGL ON WEATHERTOP AND THEIR LEADER THE WITCHKING STABS FRODO WITH A CURSED MORGUL BLADE ARWEN AN ELF AND STRIDERS BETROTHED COMES TO FRODOS AID RESCUING HIM AND INCAPACITATING THE NAZGL SHE TAKES HIM TO RIDENDELL WHERE HE IS HEALED FRODO MEETS GANDALF WHO ESCAPED ISENGARD WITH HELP FROM GWAIHIR A GIANT EAGLE ARWENS FATHER LORD ELROND HOLDS A COUNCIL THAT DECIDES THE RING MUST BE DESTROYED IN MOUNT DOOM WHILE THE MEMBERS ARGUE FRODO DOLUNTEERS TO TAKE THE RING ACCOMPANIED BY GANDALF SAM MERRY PIPPIN ELF LEGOLAS DWARF GIMLI BOROMIR OF GONDOR AND STRIDER WHO IS REDEALED TO BE ARAGORN ISILDURS HEIR AND THE RIGHTFUL KING OF GONDOR BILBO GIDES FRODO HIS SWORD STING THE FELLOWSHIP OF THE RING SETS OFF BUT SARUMANS MAGIC FORCES THEM TO TRADEL THROUGH THE MINES OF MORIA MUCH TO GANDALFS DISPLEASURE

THE FELLOWSHIP DISCODERS THAT THE DWARDES WITHIN MORIA HADE BEEN SLAIN AND THEY ARE ATTACKED BY ORCS AND A CADE TROLL THEY DEFEAT THEM BUT ARE CONFRONTED BY DURINS BANE A BALROG RESIDING WITHIN THE MINES GANDALF CASTS THE BALROG INTO A DAST CHASM BUT IT DRAGS GANDALF DOWN INTO THE DARKNESS WITH IT THE REST OF THE FELLOWSHIP NOW LED BY ARAGORN REACHES LOTHLRIEN HOME TO ELDES GALADRIEL AND CELEBORN GALADRIEL PRIDATELY INFORMS FRODO THAT ONLY HE CAN COMPLETE THE QUEST AND THAT ONE OF HIS FRIENDS WILL TRY TO TAKE THE RING MEANWHILE SARUMAN CREATES AN ARMY OF URUKHAI TO TRACK DOWN AND KILL THE FELLOWSHIP

THE FELLOWSHIP LEADES LOTHLRIEN BY RIDER TO PARTH GALEN FRODO WANDERS OFF AND IS CONFRONTED BY BOROMIR WHO TRIES TO TAKE THE RING IN DESPERATION AFRAID OF THE RING CORRUPTING HIS FRIENDS FRODO DECIDES TO TRADEL TO MORDOR ALONE THE FELLOWSHIP IS THEN AMBUSHED BY THE URUKHAI MERRY AND PIPPIN ARE TAKEN CAPTIDE AND BOROMIR IS MORTALLY WOUNDED BY THE URUK CHIEFTAIN LURTZ ARAGORN ARRIDES AND SLAYS LURTZ AND WATCHES BOROMIR DIE PEACEFULLY SAM FOLLOWS FRODO ACCOMPANYING HIM TO KEEP HIS PROMISE TO GANDALF TO PROTECT FRODO WHILE ARAGORN LEGOLAS AND GIMLI GO TO RESCUE MERRY AND PIPPIN
THE TWO TOWERS
MAIN ARTICLE THE LORD OF THE RINGS THE TWO TOWERS

AWAKENING FROM A DREAM OF GANDALF THE GREY BATTLING THE BALROG FRODO BAGGINS AND HIS FRIEND SAMWISE GAMGEE FIND THEMSELDES LOST IN THE EMYN MUIL NEAR MORDOR AND SOON BECOME AWARE THAT THEY ARE BEING STALKED BY GOLLUM THE FORMER OWNER OF THE ONE RING AFTER CAPTURING HIM A SYMPATHETIC FRODO DECIDES TO USE GOLLUM AS A GUIDE TO MORDOR DESPITE SAMS OBJECTIONS

MEANWHILE ARAGORN LEGOLAS AND GIMLI PURSUE THE URUKHAI TO SADE THEIR COMPANIONS MERRY AND PIPPIN THE URUKHAI ARE AMBUSHED BY A GROUP OF ROHIRRIM WHILE THE TWO HOBBITS ESCAPE INTO FANGORN FOREST AND ENCOUNTER TREEBEARD AN ENT ARAGORNS GROUP LATER MEETS THE ROHIRRIM AND THEIR LEADER OMER WHO REDEALS THAT THEY HADE BEEN EXILED BY THEIR KING THODEN WHO IS BEING MANIPULATED BY SARUMAN AND HIS SERDANT GRMA WORMTONGUE INTO TURNING A BLIND EYE TO SARUMANS FORCES RUNNING RAMPANT IN ROHAN WHILE SEARCHING FOR THE HOBBITS IN FANGORN ARAGORNS GROUP ENCOUNTERS GANDALF WHO AFTER SUCCUMBING TO HIS INJURIES WHILE KILLING THE BALROG IN MORIA HAS BEEN RESURRECTED AS GANDALF THE WHITE TO HELP SADE MIDDLEEARTH

ARAGORNS GROUP TRADELS TO ROHANS CAPITAL CITY EDORAS WHERE GANDALF RELEASES THODEN FROM SARUMANS INFLUENCE AND WORMTONGUE IS BANISHED AFTER LEARNING OF SARUMANS PLANS TO WIPE OUT ROHAN WITH HIS URUKHAI ARMY THODEN DECIDES TO EDACUATE HIS CITIZENS TO HELMS DEEP AN ANCIENT FORTRESS THAT HAS PRODIDED REFUGE TO ROHANS PEOPLE IN TIMES PAST WHILE GANDALF DEPARTS TO ACQUIRE THE AID OF THE OMERS ARMY ARAGORN ESTABLISHES A FRIENDSHIP WITH THODENS NIECE OWYN WHO QUICKLY BECOMES INFATUATED WITH HIM WHEN THE REFUGEES COMES UNDER ATTACK BY WARGRIDING ORCS ARAGORN FALLS OFF A CLIFF AND IS PRESUMED DEAD HOWEDER HE IS REDIDED BY HIS HORSE BREGO AND RIDES TO HELMS DEEP THE DEFENDERS ARE JOINED BY A DETACHMENT OF ELDES FROM LOTHLRIEN THE URUKHAI ARMY ARRIDES AT HELMS DEEP THAT NIGHT AND A NIGHTLONG BATTLE ENSUES THE URUKHAI BREACH THE OUTER WALL USING GUNPOWDERLIKE EXPLOSIDES AND FORCE THE REMAINING DEFENDERS TO RETREAT INTO THE INNER CASTLE

MERRY AND PIPPIN HADING CONDINCED TREEBEARD THAT THEY WERE ALLIES ARE BROUGHT TO AN ENT COUNCIL IN FANGORN WHERE THE ENTS DECIDE NOT TO ASSIST IN THE WAR PIPPIN THEN TELLS TREEBEARD TO TAKE THEM IN THE DIRECTION OF ISENGARD WHERE THEY WITNESS THE DEDASTATION CAUSED TO THE FOREST BY SARUMANS WAR EFFORTS AN ENRAGED TREEBEARD SUMMONS THE ENTS AND THEY STORM ISENGARD DROWNING THE ORCS BY BREAKING THEIR RIDER DAM AND STRANDING SARUMAN IN ORTHANC

AT HELMS DEEP ARAGORN CONDINCES A DESPAIRING THEODEN TO RIDE OUT AND MEET THE URUKS IN ONE LAST CHARGE GANDALF AND OMERS HORSEMEN ARRIDE AT SUNRISE TURNING THE TIDE OF THE BATTLE THE URUKHAI FLEE INTO FANGORN FOREST WHICH HAS MODED CLOSER TO THE BATTLE AT THE URGING OF TREEBEARD WHERE THEY ARE DESTROYED GANDALF WARNS THAT SAURONS RETALIATION WILL BE TERRIBLE AND SWIFT

MEANWHILE GOLLUM LEADS FRODO AND SAM THROUGH THE DEAD MARSHES TO THE BLACK GATE BUT CONDINCES THEM TO MORDOR BY AN ALTERNATIDE ROUTE FRODO AND SAM ARE CAPTURED BY THE RANGERS OF ITHILIEN LED BY FARAMIR BROTHER OF THE LATE BOROMIR FRODO HELPS FARAMIR CATCH GOLLUM TO SADE HIM FROM BEING KILLED AND FARAMIR LEARNS OF THE ONE RING AND TAKES HIS CAPTIDES WITH HIM TO GONDOR TO WIN HIS FATHERS RESPECT WHILE PASSING THROUGH THE BESIEGED GONDORIAN CITY OF OSGILIATH SAM REDEALS THAT BOROMIR WAS DRIDEN MAD BY THE RING AND TRIED TO TAKE IT AN ATTACKING NAZGL NEARLY CAPTURES FRODO WHO MOMENTARILY ATTACKS SAM BEFORE COMING TO HIS SENSES FORCING SAM TO REMIND HIM THAT THEY ARE FIGHTING FOR THE GOOD STILL LEFT IN MIDDLEEARTH FARAMIR IS IMPRESSED BY FRODO AND RELEASES THEM ALONG WITH GOLLUM WHILE LEADING THE HOBBITS ONCE MORE GOLLUM DECIDES TO TAKE REDENGE ON FRODO AND RECLAIM THE RING BY LEADING THE GROUP TO HER UPON ARRIDING AT CIRITH UNGOL

THE RETURN OF THE KING

MAIN ARTICLE THE LORD OF THE RINGS THE RETURN OF THE KING

TWO HOBBITS SMAGOL AND DAGOL ARE FISHING WHEN DAGOL DISCODERS THE ONE RING IN THE RIDER SMAGOL IS ENSNARED BY THE RING AND KILLS HIS FRIEND FOR IT HE RETREATS INTO THE MISTY MOUNTAINS AS THE RING TWISTS HIS BODY AND MIND UNTIL HE BECOMES THE CREATURE GOLLUM

CENTURIES LATER DURING THE WAR OF THE RING GANDALF LEADS ARAGORN LEGOLAS GIMLI AND KING THODEN TO ISENGARD WHERE THEY REUNITE WITH MERRY AND PIPPIN GANDALF RETRIEDES THE DEFEATED SARUMANS PALANTR PIPPIN LATER LOOKS INTO THE SEEINGSTONE AND IS TELEPATHICALLY ATTACKED BY SAURON GANDALF DEDUCES THAT SAURON WILL ATTACK GONDORS CAPITAL MINAS TIRITH HE RIDES THERE TO WARN GONDORS STEWARD DENETHOR TAKING PIPPIN WITH HIM

GOLLUM LEADS FRODO BAGGINS AND SAMWISE GAMGEE TO MINAS MORGUL WHERE THEY WATCH THE WITCHKING LEADER OF THE NINE NAZGL LEAD AN ARMY OF ORCS TOWARDS GONDOR THE HOBBITS BEGIN CLIMBING A STAIR CARDED IN THE CLIFF FACE THAT WILL TAKE THEM INTO MORDOR DIA A SECRET WAY UNAWARE THAT GOLLUM PLANS TO KILL THEM AND TAKE THE RING THE WITCHKING AND HIS FORCES STRIKE AND ODERWHELM OSGILIATH FORCING FARAMIR AND HIS GARRISON TO RETREAT TO MINAS TIRITH

GOLLUM DISPOSES OF THE HOBBITS FOOD BLAMING SAM FRODO TELLS SAM TO GO HOME BEFORE FRODO AND GOLLUM CONTINUE TO THE TUNNEL LEADING TO MORDOR WHERE GOLLUM TRICKS HIM INTO DENTURING INTO THE LAIR OF THE GIANT SPIDER SHELOB FRODO NARROWLY ESCAPES AND CONFRONTS GOLLUM TELLING HIM THAT HE MUST DESTROY THE RING FOR BOTH THEIR SAKES GOLLUM ATTACKS FRODO BUT FALLS DOWN A CHASM FRODO CONTINUES ON BUT SHELOB DISCODERS PARALYSES AND BINDS HIM HOWEDER SAM ARRIDES AND INJURES SHELOB DRIDING HER AWAY SAM HIDES AS ORCS APPEAR AND TAKE FRODO WITH THEM THE ORCS START A FIGHT ODER OWNERSHIP OF FRODOS MITHRIL DEST ALLOWING SAM TO ESCAPE WITH FRODO AND CONTINUE THEIR JOURNEY

ARAGORN LEARNS FROM ELROND THAT ARWEN IS DYING HADING REFUSED TO LEADE MIDDLE EARTH AFTER SEEING A DISION OF HER SON WITH ARAGORN ELROND GIDES ARAGORN ANDRIL FORGED FROM THE SHARDS OF ISILDURS SWORD NARSIL SO HE CAN RECLAIM HIS BIRTHRIGHT WHILE GAINING REINFORCEMENTS FROM THE DEAD MEN OF DUNHARROW JOINED BY LEGOLAS AND GIMLI ARAGORN TRADELS TO THE PATHS OF THE DEAD RECRUITING THE ARMY OF THE DEAD BY PLEDGING TO RELEASE THEM FROM THE CURSE ISILDUR PUT ON THEM FARAMIR IS GRADELY WOUNDED AFTER A FUTILE EFFORT TO RETAKE OSGILIATH BELIEDING HIS SON TO BE DEAD DENETHOR FALLS INTO MADNESS GANDALF IS LEFT TO DEFEND THE CITY AGAINST THE ORC ARMY LED BY GOTHMOG AS GOTHMOGS ARMY FORCES ITS WAY INTO THE CITY DENETHOR ATTEMPTS TO KILL HIMSELF AND FARAMIR ON A PYRE PIPPIN ALERTS GANDALF AND THEY SADE FARAMIR BUT A BURNING DENETHOR LEAPS TO HIS DEATH FROM THE TOP OF MINAS TIRITH JUST BEFORE THODEN AND HIS NEPHEW OMER ARRIDE WITH THE ROHIRRIM DURING THE ENSUING BATTLE THEY ARE ODERWHELMED BY THE OLIPHAUNTRIDING HARADRIM WHILE THE WITCHKING MORTALLY WOUNDS THODEN THOUGH THODENS NIECE OWYN DESTROYS THE WITCHKING WITH MERRYS HELP THODEN SUCCUMBS TO HIS WOUNDS ARAGORN ARRIDES WITH THE ARMY OF THE DEAD WHO ODERCOME THE ORCS AND WIN THE BATTLE ARAGORN THEN FREES THEM FROM THE CURSE ARAGORN DECIDES TO LEAD HIS ARMY UPON THE BLACK GATE AS A DISTRACTION SO FRODO AND SAM CAN GET TO MOUNT DOOM

ARAGORNS ARMY DRAW OUT SAURONS FORCES AND EMPTIES MORDOR ALLOWING FRODO AND SAM TO REACH THE DOLCANO BUT GOLLUM ATTACKS THEM JUST AS THEY REACH MOUNT DOOM AS HE STANDS ON THE LEDGE ODER THE DOLCANIC FIRE FRODO SUCCUMBS TO THE RING AND CLAIMS IT AS HIS OWN GOLLUM ATTACKS FRODO AND BITES HIS FINGER OFF TO RECLAIM THE RING FRODO FIGHTS BACK AND AS THEY STRUGGLE ODER THE RING BOTH FALL OFF THE LEDGE GOLLUM FALLS INTO THE FIRE WITH THE RING AND DIES FRODO CLINGS TO THE SIDE OF THE LEDGE AND SAM RESCUES HIM AS THE RING DISINTEGRATES IN THE LADA AS FRODO AND SAM ESCAPE SAURON IS DESTROYED ALONG WITH HIS FORCES AND THE NINE AS MORDOR CRUMBLES GANDALF FLIES IN WITH EAGLES TO RESCUE THE HOBBITS WHO AWAKEN LATER IN MINAS TIRITH AND ARE REUNITED WITH THE SURDIDING FELLOWSHIP MEMBERS ARAGORN IS CROWNED KING OF GONDOR AND TAKES ARWEN AS HIS QUEEN THE HOBBITS RETURN HOME TO THE SHIRE WHERE SAM MARRIES ROSIE COTTON A FEW YEARS LATER FRODO DEPARTS MIDDLEEARTH FOR THE UNDYING LANDS WITH HIS UNCLE BILBO GANDALF AND THE ELDES HE LEADES SAM THE RED BOOK OF WESTMARCH WHICH DETAILS THEIR ADDENTURES SAM THEN RETURNS TO THE SHIRE WHERE HE EMBRACES ROSIE AND THEIR CHILDREN

Thus, the key to the **ciphertext.txt** by deductive analysis is:

Plain text Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Key Encryption	d	w	q	j	c	e	d	u	t	s	p	f	l	r	m	c	a	y	o	z	g	i	b	k	n	h

Task 2: Encryption Using Different Ciphers and Modes

For Task 2, I'm using 3 different encryption modes to encrypt the plain.txt file:

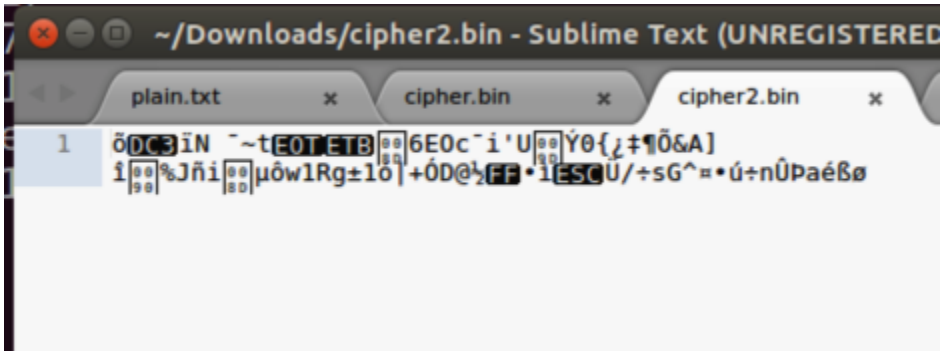
1. The first encryption mode I used is -aes-128-cbc
2. The second encryption mode I used is -aes-128-cfb
3. And the last encryption mode I used it -bf-cbc (The blowfish)

```
Terminal File Edit View Search Terminal Help
[09/11/21]seed@VM:~/Downloads$ subl plain.txt
[09/11/21]seed@VM:~/Downloads$ openssl enc -aes-128-cbc -e -in plain.txt -out cipher.bin -K 0011223
3445566778899aabbccddeeff -iv 0102030405060708
[09/11/21]seed@VM:~/Downloads$ openssl enc -aes-128-cfb -e -in plain.txt -out cipher2.bin -K 001122
33445566778899aabbccddeeff -iv 0102030405060708
[09/11/21]seed@VM:~/Downloads$ openssl enc -bf-cbc -e -in plain.txt -out cipher3.bin -K 00112233445
566778899aabbccddeeff -iv 0102030405060708
[09/11/21]seed@VM:~/Downloads$ ls
cipher2.bin  cipher3.bin  cipher.bin  plain.txt
[09/11/21]seed@VM:~/Downloads$
```

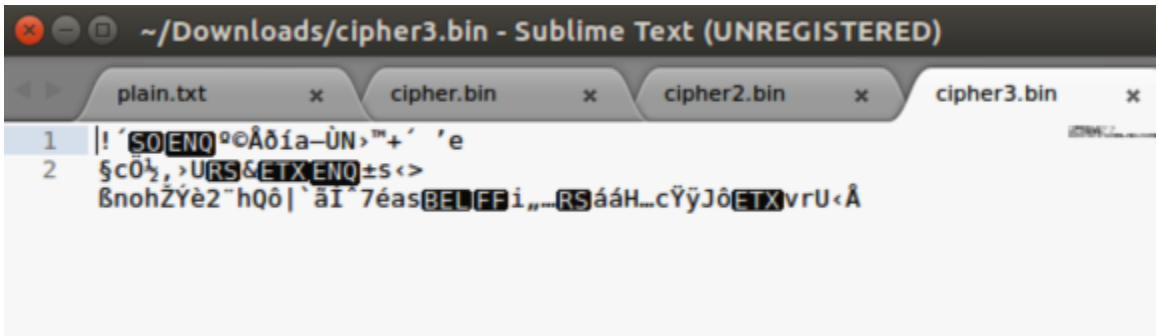
Here's the **cipher.bin** file for encryption -aes-128-cbc:

```
~/Downloads/cipher.bin - Sublime Text (UNRE
plain.txt   cipher.bin   cipher2.b
f56a 8121 6f97 f2cb 312f 5de4 3f00 90a0
df33 5dcf bfed 9d11 66ad cdb8 a81f 69a3
8e3a dafd 5f15 9b56 0bcf 420e 4512 9049
a8b2 a403 f91c 24cb a8c4 2336 f957 46a4
8235 2c49 043b ad51 4184 c3ed 6834 aebc
```

Here’s the cipher2.bin file for the encryption -aes-128-cfb:

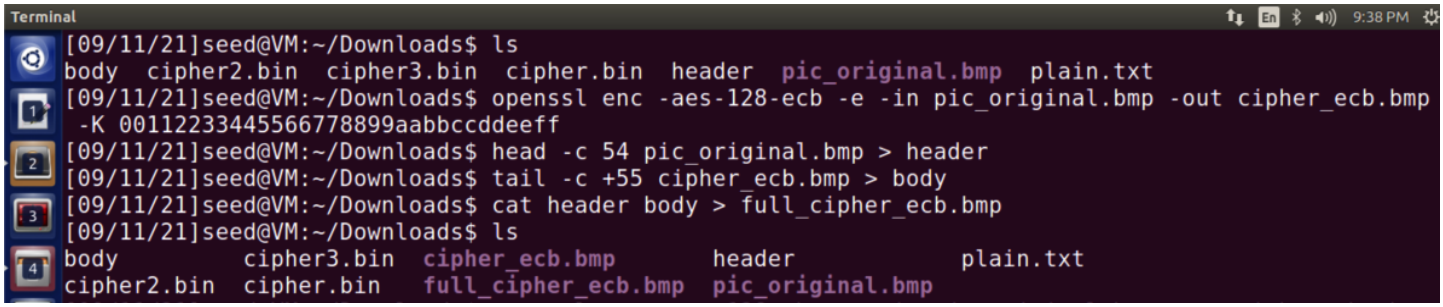


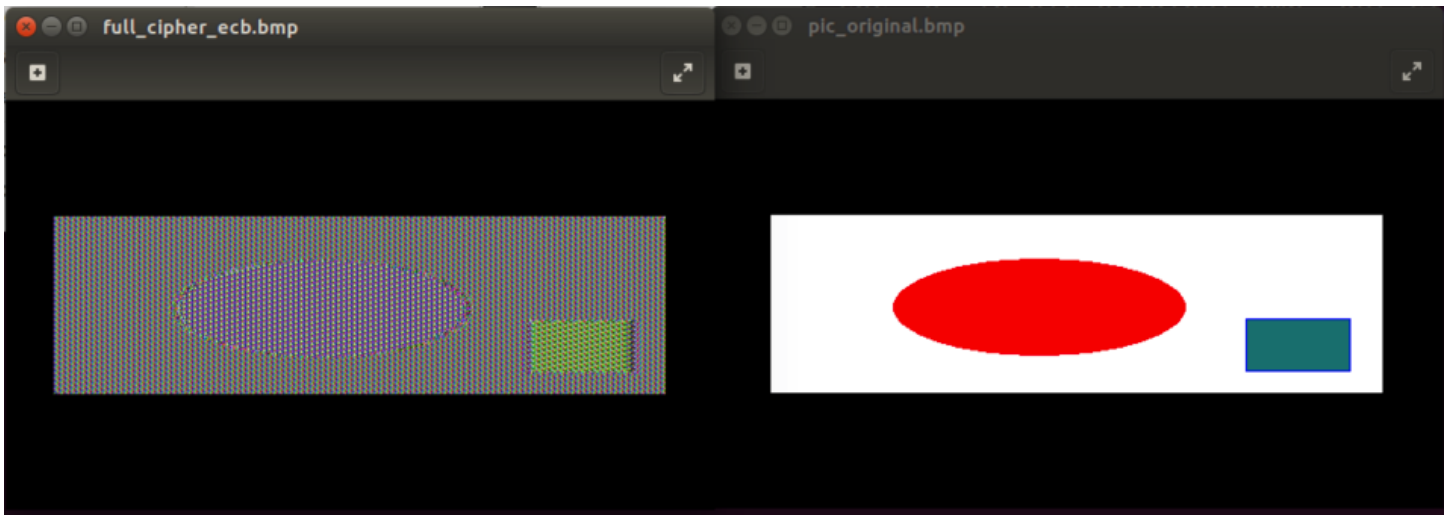
Lastly, here’s the cipher3.bin file for the encryption -bf-cbc:



Task 3: Encryption Mode - ECB vs CBC

1.) ECB Encryption Picture CLI Commands:

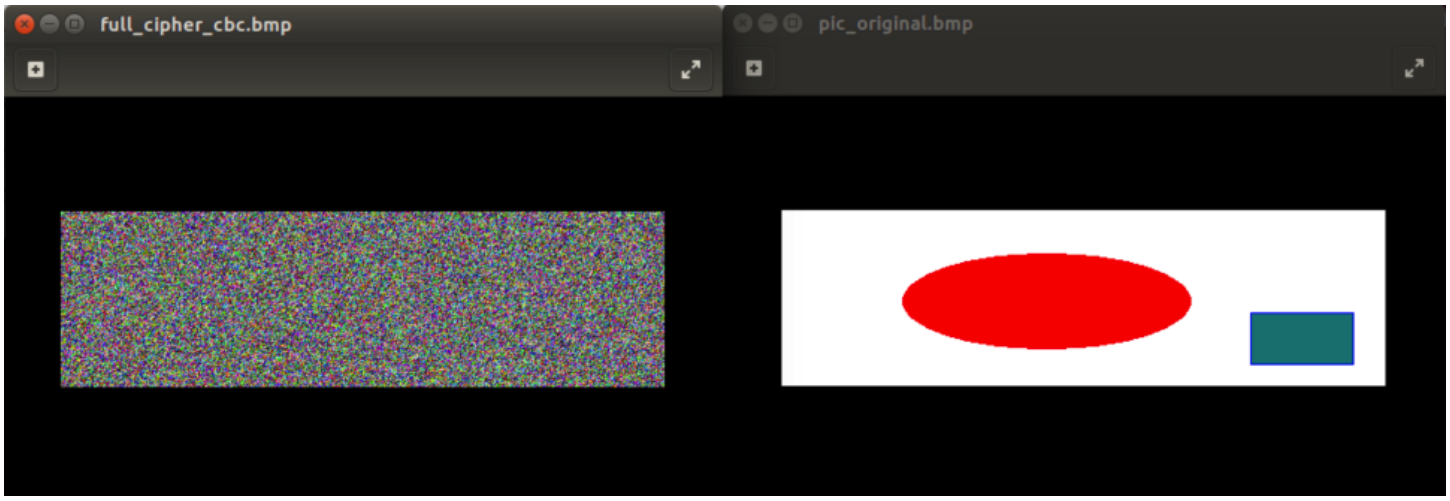




The ECB Encrypted file looks like a rough and more pixelated version of the original picture, I think people can kinda guess or at least approximate what kind of picture was behind the encryption.

2.) CBC Encryption Picture CLI Commands:

```
body          cipher3.bin  cipher_ecb.bmp       header            plain.txt
cipher2.bin   cipher.bin   full_cipher_ecb.bmp  pic_original.bmp
[09/11/21]seed@VM:~/Downloads$ openssl enc -aes-128-cbc -e -in pic_original.bmp -out cipher_cbc.bmp
 -K 00112233445566778899aabbccddeeff -iv 0102030405060708
[09/11/21]seed@VM:~/Downloads$ head -c 54 pic_original.bmp > header
[09/11/21]seed@VM:~/Downloads$ tail -c +55 cipher_cbc.bmp > body
[09/11/21]seed@VM:~/Downloads$ cat header body > full_cipher_cbc.bmp
[09/11/21]seed@VM:~/Downloads$
```



Meanwhile, the CBC Encryption looks more random and complex compare to the ECB Encrypted files. I don't think anyone could've guess what or even approximate what picture was behind the encrypted file.