Lab 1 Analysis
Gunnar Yonker

1.

LetterFreqKey.java – Program to obtain frequency of each letter and put it into a txt file called LetterFreq.txt and then create a text file called CipherKey.txt with the monoalphabetic substitutions based on the English frequency patterns.

2.

KeyDecrypt.java – Program to use the CipherKey.txt file as the key to decrypt the ciphertext into the plaintext for further analysis.

3.

For my analysis of this monoalphabetic cipher, using the above stated java programs the initial key that is printed out based solely on the English letter frequencies is:

```
Cipher Key:
A = O
B = M
C = V
D = I
E = X
F = R
G = T
H = L
I = Y
J = A
K = W
L = K
M = J
N = E
O = F
P = C
Q = B
R = G
S = H
T = Q
U = U
V = N
W = Z
X = S
Y = P
Z = D
```

As an example, the first line of the plaintext after the key is used is as follows:

AEHOP'H UABLEH TRANHLATED BY GEORGE UYLER TOFNHEND

This is now a good starting point for me to adjust the key based on what I can assume from this first line after the English letter frequencies substitutions. One adjustment to make is so that the 3rd word becomes TRANSLATED.

Lab 1 Analysis
Gunnar Yonker

After some adjustments the key becomes:

```
Cipher Key:
A = O
B = M
C = V
D = H
E = X
F = R
G = T
H = L
I = Y
J = A
K = U
L = K
M = J
N = E
O = W
P = C
Q = B
R = G
S = S
T = Q
U = F
V = N
W = Z
X = I
Y = P
Z = D
```

This results in the first sentence and paragraph becoming:

AESOP'S FABLES TRANSLATED BY GEORGE FYLER TOWNSEND

THE WOLF AND THE LAMB

WOLF, MEETING WITH A LAMB ASTRAY FROM THE FOLD, RESOLVED NOT TO

LAY VIOLENT HANDS ON HIM, BCT TO FIND SOME PLEA TO XCSTIFY TO THE

LAMB THE WOLF'S RIGHT TO EAT HIM. HE THCS ADDRESSED HIM:

"SIRRAH, LAST YEAR YOC GROSSLY INSCLTED ME." "INDEED," BLEATED

THE LAMB IN A MOCRNFCL TONE OF VOIUE, "I WAS NOT THEN BORN." THEN

SAID THE WOLF, "YOC FEED IN MY PASTCRE." "NO, GOOD SIR," REPLIED

THE LAMB, "I HAVE NOT YET TASTED GRASS." AGAIN SAID THE WOLF,

"YOC DRINK OF MY WELL." "NO," EJULAIMED THE LAMB, "I NEVER YET

DRANK WATER, FOR AS YET MY MOTHER'S MILK IS BOTH FOOD AND DRINK

Lab 1 Analysis
Gunnar Yonker

TO ME." CPON WHIUH THE WOLF SEIZED HIM AND ATE HIM CP, SAYING,

"WELL! I WON'T REMAIN SCPPERLESS, EVEN THOCGH YOC REFCTE EVERY

ONE OF MY IMPCTATIONS." THE TYRANT WILL ALWAYS FIND A PRETEJT FOR

HIS TYRANNY.

Most of the text has now become decrypted and can easily be read, but there are still a few more substitutions to be fixed in the key.

The final key that results in a full decryption of the Gunnar.txt file is:

Cipher: “ABCDEFGHIJKLMNOPQRSTUVWXYZ”

Key: “OMVHJRTLYACKXEWUBGSQFNZIPD”

```
Cipher Key:
A = O
B = M
C = V
D = H
E = J
F = R
G = T
H = L
I = Y
J = A
K = C
L = K
M = X
N = E
O = W
P = U
Q = B
R = G
S = S
T = Q
U = F
V = N
W = Z
X = I
Y = P
Z = D
```

Lab 1 Analysis
Gunnar Yonker

Using this key the first paragraph becomes:

AESOP'S FABLES TRANSLATED BY GEORGE FYLER TOWNSEND

THE WOLF AND THE LAMB

WOLF, MEETING WITH A LAMB ASTRAY FROM THE FOLD, RESOLVED NOT TO
LAY VIOLENT HANDS ON HIM, BUT TO FIND SOME PLEA TO JUSTIFY TO THE
LAMB THE WOLF'S RIGHT TO EAT HIM. HE THUS ADDRESSED HIM:
"SIRRAH, LAST YEAR YOU GROSSLY INSULTED ME." "INDEED," BLEATED
THE LAMB IN A MOURNFUL TONE OF VOICE, "I WAS NOT THEN BORN." THEN
SAID THE WOLF, "YOU FEED IN MY PASTURE." "NO, GOOD SIR," REPLIED
THE LAMB, "I HAVE NOT YET TASTED GRASS." AGAIN SAID THE WOLF,
"YOU DRINK OF MY WELL." "NO," EXCLAIMED THE LAMB, "I NEVER YET
DRANK WATER, FOR AS YET MY MOTHER'S MILK IS BOTH FOOD AND DRINK
TO ME." UPON WHICH THE WOLF SEIZED HIM AND ATE HIM UP, SAYING,
"WELL! I WON'T REMAIN SUPPERLESS, EVEN THOUGH YOU REFUTE EVERY
ONE OF MY IMPUTATIONS." THE TYRANT WILL ALWAYS FIND A PRETEXT FOR
HIS TYRANNY.

4.

The ciphertext Gunnar.txt can now be fully decrypted by using the above key and the KeyDecrypt.java program when run with the correct key creates the Gunnarplaintext.txt file with the full decrypted message.

Using cryptanalysis along with the English letter frequencies pattern, the key to the cipher was able to be decrypted.

Lab 1 Analysis
Gunnar Yonker

The submitted files are:

LetterFreqKey.java

KeyDecrypt.java

LetterFreq.txt – This will be created and written to by the LetterFreqKey.java program, contains the frequencies of the letters and two letter combinations.

CipherKey.txt – created with LetterFreqKey.java program and contains the key without any analysis only based on the English letter frequencies.

CipherKey-Freq Based.txt – The cipher key from the LetterFreq.txt file with the key that was based solely on the English letter frequencies.

CipherKey-Final.txt – This contains the correct cipher key that was found after my further analysis with additional substitutions. Can be renamed or copied into the CipherKey.txt file and then the KeyDecrypt.java file can be run to display the completed decrypted text.

Gunnarplaintext.txt – This is the decrypted text (plaintext) corresponding to my ciphertext using the correct key.

Gunnar.txt – The original ciphertext used.

Bonus Question:

Using the same programs to decrypt the given ciphertext.

```
Cipher Key:
A = M
C = Y
D = P
E = L
F = W
G = N
H = T
I = G
J = I
K = S
M = H
N = E
Q = A
R = B
S = C
T = F
U = O
V = D
W = U
X = V
```

Lab 1 Analysis
Gunnar Yonker

Z = R

Ciphertext:

NVQ CUGGEHJZ NVUN MG QUGD NH JQAQAIQJ ITN VUJZ NH FJUFR MG FHAIMKUNMHK HW EHJZG NVUN UJQ KHN JQSUNQZ.

M FUK WHSSHE DHT WHJ NVHTGUKZG HW AMSQG UKZ KHN XQN SHGN. M ZH KHN WQUJ FHSZ HJ WMJQ, UKZ M KQMNVQJ QUN KHJ ZJMKR, ITN M ZMGUCCQUJ EVQK NVQ GTK GQNG MK NVQ EQGN. EVH UA M?

Plaintext(Using English letter frequencies):

EDA YONNLTIR EDOE HN AONP ET IAMAMGAI GFE DOIR ET WIOWB HN WTMGHSOEHTS TU LTIRN EDOE OIA STE IACOEAR.

H WOS UTCCTL PTF UTI EDTFNOSRN TU MHCAN OSR STE VAE CTNE. H RT STE UAOI WTCR TI UHIA, OSR H SAHEDAI AOE STI RIHSB, GFE H RHNOYYAOI LDAS EDA NFS NAEN HS EDA LANE. LDT OM H?

Right away comparing this to the large document ciphertext, after the initial substitution using the key based on the English letter frequency patterns it is a lot less discernable to make further adjustments. There are also many letters that were not present which would then throw off the pattern assignment to the counted letters. There are not as many letters used so matching the frequencies is less successful. It would still be possible to figure out this cipher based on trial and error of guessing which letters need to be changed such as it can be assumed that H is most likely I as it fits.

Cipher Key:
A = M
C = P
D = Y
E = W
F = C
G = S
H = O
I = B
J = R
K = N
M = I
N = T
Q = E
R = K
S = L
T = U
U = A
V = H
W = F
X = G
Z = D

Lab 1 Analysis
Gunnar Yonker

This is the correct key that would be used to decrypt the ciphertext given, and it shares very little in common with the original key that was created after using the frequency pattern. There are also letters not used such as the letter B and L in the ciphertext which then makes the frequency assignment not as successful. Through trial and error, I was able to get the above key which would result in this as the plaintext for the given ciphertext.

THE PASSWORD THAT IS EASY TO REMEMBER BUT HARD TO CRACK IS COMBINATION OF WORDS THAT ARE NOT RELATED.

I CAN FOLLOW YOU FOR THOUSANDS OF MILES AND NOT GET LOST. I DO NOT FEAR COLD OR FIRE, AND I NEITHER EAT NOR DRINK, BUT I DISAPPEAR WHEN THE SUN SETS IN THE WEST. WHO AM I?

I also believe that the answer to the above given riddle would be my shadow. It always follows you wherever you go, cannot get cold or hot, doesn't need to eat or drink, and when the sunsets your shadow goes away!

This question gave me a different perspective on monoalphabetic substitution ciphers because I thought that the ability to use the English letter frequency pattern would help to solve any ciphertext using this method. However, it is limited in that the shorter the ciphertext, the more difficult to assign those substitution patterns. With the original ciphertext given for this lab, the frequency pattern worked because there were more letters and more data which made the pattern more evident. Thus, analysis after the initial substitution was more easily done compared to the bonus question ciphertext which required much more trial and error due to less letters and data being available to analyze.