(Spring 2014) CSC 555 Programming Project 1: Frequency Analysis

Due date: //2014, 11:59pm

Set up turnin command

1. Log in Putty.
2. Type in the following command to set up turnin

```
/export/home/public/zhang/turnin.pl    555
```

3. To submit a file to me, use the following two commands

```
source   .alias
turnin425   yourfile.cpp
```

File needed

Copy the following file to your own directory

```
cp  /export/home/public/zhang/crypto/cipher.dat   cipher.dat
```

Tasks

The file **cipher.dat** contains the ciphertext you want to decrypt. You know that the plaintext is encrypted using a monoalphabetic cipher. You need to write two programs **frequency.cpp** and **decrypt.cpp** in order to do the decryption.

The first program **frequency.cpp** will produce frequency information (in percentage) of the 26 English letters in the ciphertext as follows.

```
> ./a.out
Enter the filename: cipher.dat
Frequency analysis for cipher.dat
==============================
(a, 0.0490)
(b, 0.0070)
(c, 0.0909)
(d, 0.0000)
(e, 0.1259)
… …
```

Use the letter frequencies to decide the mappings for the two most frequent letters e and t. Then use the second program to decrypt the message. The **decrypt.cpp** program allows the user to enter a partial

key (a partially completed mapping) to decrypt the ciphertext. The user enters "*" for currently unknown mappings.

```
> ./a.out
Enter the file name: cipher.dat
Enter key:
ABCDEFGHIJKLMNOPQRSTUVWXYZ  (this line is printed out by program)
***m***e***t***vu********s

sTMN vXTNE CFA vEuEF KECNv CJT TMN sCWSENv ONTMJSW sTNWS TF WSVv
XTFWVFEFW, C FEB FCWVTF, XTFXEVuEA VF GVOENWK, CFA AEAVXCWEA WT
WSE RNTRTvVWVTF WSCW CGG tEF CNE XNECWEA EYMCG
```

Based on the partial mapping, the program prints out the substituted letters in lowercase and un-substituted letters in uppercase. To decrypt the message you need to run the program multiple times and use trial-and-error. Use two-letter and three-letter words in the ciphertext to help recover the mapping.

You need to submit the following three files

- **frequency.cpp**
- **decrypt.cpp**
- **analysis.txt** In this text file you need to describe how you use the two programs to decrypt the message.

Grading guide

- (3 pts) Successful implementation of **frequency.cpp**
- (3 pts) Successful implementation of **decrypt.cpp**
- (4 pts) Detailed description of the cryptanalysis process