Comp 424 w/Prof. Vahab

Written By: Jared Fowler

February 19, 2015

Homework 1

Encrypted Message:

KUHPVIBQKVOSHWHXBPOFUXHRPVLLDDWVOSKWPREDDVVIDWQRBHBGLLBBPKQUNRVOHQEIRLWOKKRDD

Decrypted Message:

BE HAPPY FOR THE MOMENT THIS MOMENT IS YOUR LIFE BY KHAYYAM OH AND ALSO THIS CLASS IS REALLY FUN

Technique:

I started off by writing a program that would read a file and calculate the frequencies of each letter used. I was able to acquire an English dictionary in ASCII .txt format off the internet, which I ran through the program. I then ran the cipher-text through the same program and compared results. Based upon the letters with the lowest and highest frequencies, there was strong evidence that the simple-shift was based off a -3 shift. Upon arriving at the solution, this observation was validated!

The program I wrote began to be ever more expansive as I found a need for more functionality for preforming tests. I wrote a function which outputs all the different possibilities that could result from a simple-shift. (26 possibilities) I next wrote a function that would take this output, along with a maximum key length value, and output to a file all the different permutations based upon columnar transposition. To make my life easier, I assumed, and greatly hoped, that the key would be of length 8 or less. This greatly reduced the amount of time needed to iterate all the possibilities. (This step took longer than it should of due to an error in code.)

Great, I have a long list and just one of them is the correct plaintext message. Now what?

I developed a function which would go through the large list and attempt to match up words (short words 2-7 chars). To prepare, I first had to write a function which would read a dictionary (list of words) and separate them into 26 different files which represented 26 single dictionaries by letter. These words were output in a way to be then easily hard-coded into the program.

With the proper tools I began to shorten the large permutated list:

-Original List Size:	1202058
-Ciphers with a valid 2+ letter start word:	145406
-Ciphers with a 4 letter word:	58479
-Ciphers with a 5 letter word:	5218
-Ciphers with a 6 letter word:	195

At this point, I used the pattern recognizing ability of a human mind to determine the correct line from the list. I somewhat feel lucky that the above operations each proved true for the message. To improve the above technique, I would once again modify my function which compares words to do more comparisons and somehow keep track of ciphers which are more close to plain text than others. I don't question the ability to make the functions more efficient, rather, I question the much needed time necessary to spend on doing such.

All the used programs were written by myself. I did utilize and slightly modify a permutation algorithm from: http://www.cs.utexas.edu/users/djimenez/utsa/cs3343/lecture25.html

Dictionary: http://www.winedt.org/Dict/