Gabriel Sturtevant

Comp 424

Dr. Vahab Pournaghshband

10/17/2016

Assignment 1

When approaching this assignment, I initially looked into how Caesar Ciphers and columnar transposition ciphers were performed. I ended up drawing out the steps on paper and coming up with my own encrypted phrases. These initial tests were limited to sentence lengths that allowed for a result of zero when taking the modulus against the column key size.

With that information in hand, I designed a program that exactly mimicked the method in which a human would go about loading the sentence into a grid, and rearranging it based on the column keys attempted. After a few trials, my program was able to decrypt the messages that I had already come up with, so I moved on to trying the message from the homework assignment. Since that message was 77 characters long, I focused my attention on key lengths of 7. In order to sift through the results, I compiled a dictionary of around 300,000 words from various places on the internet, then I ran each permutation against my dictionary and counted and recorded the hits I got. In addition, I analyzed the letter frequency of the message and calculated the shift needed to get the most frequent letter to be ‘e’, which left me a shift of -3 or 23. When that didn’t produce anything, I realized I had to broaden my search. This meant rewriting my algorithm to fill empty space left by the dimension mismatch.

This realization also led me to realize that the program would take much, much longer to run and so I decided to take advantage of my multiple cores and used wrote my algorithm in a manner that no logger required 2 dimensional lists, and I began using the built in dictionaries in Linux. At that point, I decided to run the program testing columns 2-6, with a shift of -3, since that would take much less time than running all possibilities. Luckily, when I checked the results from that run, the top permutation in my organized list was entirely English, so I stopped pending confirmation with you that my result was correct.

Result: “*BE HAPPY FOR THE MOMENT THIS MOMENT IS YOUR LIFE BY KHAYYAM OH AND ALSO THIS CLASS IS REALLY FUN*”