Yun, Chris

Comp424

Assignment #1

Method 1:

The ciphertext can be decrypted using columnar transposition and a simple shift substitution, so I decided to create a string that has the ciphertext and put it through a simplified columnar transposition decryption method to see if I could get lucky finding the message. I chose to use columns of 1, 7 and 11 for my columnar transposition because they are divisible from 77.

Results\_01:

I had a feeling the assignment wasn’t going to be that easy, but I thought it was worth a shot. The results were complete gibberish and I could not find a single word when I skimmed through the output.

Method 2:

I wanted to focus on using a 7 column transposition because of my previous reasoning. I decided to skip columns of 11 because the directions state that the key is less than or equal to 10 characters. I don’t know I could go through every permutation for 7 columns, but I thought to just go for it and see what I could find.

I decided to make a key of “abcdefg” and create an arrayList of every permutation, then run that through a variation of the first program while outputting strings that contain the word “THE.”

Results\_02:

There were a very large amount of results (640), so I just looked at the first 5 letters of the string to see if there was a word there. After going halfway through the list, I found a lot of strings that started with “APPY,” so I searched for the word “HAPPY.” I was able to find the following string:

24: String used: HREMSFYNHSLPETEUYMLCRUEOMSIIAATSLPHTMOBAASSFATNOYEYDIIYYMHNRKOSLENBFOITLHHOAA

Key used: gcaedbf

Possible Decryption Text:BEHAPPYFORTHEMOMENTTHISMOMENTISYOURLIFEBYKHAYYAMOHANDALSOTHISCLASSISREALLYFUN

It looks like it says “Be happy for the moment this moment is your life by khayyam oh and also this class is really fun.” So the string was shifted by +23 and the key for the columnar transposition was gcaedbf.

Sources:

caesar shift:

https://stackoverflow.com/questions/19108737/java-how-to-implement-a-shift-cipher-caesar-cipher

https://beginnersbook.com/2015/04/convert-stringbuffer-to-string/

columnar transposition:

https://programmingcode4life.blogspot.com/2015/10/columnar-transposition-cipher-without.html

https://programmingcode4life.blogspot.com/2015/09/columnar-transposition-cipher.html

https://www.geeksforgeeks.org/columnar-transposition-cipher/

permutations:

https://www.geeksforgeeks.org/print-all-permutations-of-a-string-in-java/

https://stackoverflow.com/questions/4240080/generating-all-permutations-of-a-given-string