Comp 424: Security
Assignment #1

Juan Navarrete
10/18/16

Introduction

The assignment was to decipher an encrypted text and the given information was two encryption methods were implemented, Caesar shift and column transposition. My methodology in deciphering the text was to create an algorithm that produced all possible combination of plaintext. Next, each plaintext was crossed referenced with a dictionary. And finally, the plaintext with the most words would result being the decipher string. In my software I found the decipher string to be, *'BE HAPPY FOR THE MOMENT THIS MOMENT IS YOUR LIFE BY KHAYY AMOHANDAL SO THIS CLASS IS REALLY FUN'*.

Analysis on cipher text

The first step I used towards decrypting the ciphertext was to annotate the frequency of each character. The most frequent character in the ciphertext would let me know the appropriate shift to use in the Caesar Cypher. The reason this information is valuable is because in English the most frequent letter is '*E*' ("Letter Frequency"). By analogy the most frequent character in the ciphertext would represent the character '*E*' after it has been encrypted.

Figure 1, displays the frequency of each character in the ciphertext. The histogram displays two characters, '*D*' & '*V*', as the most frequent characters in the ciphertext. From the analysis I can infer that each of these letters can represent the character '*E*' in the plaintext and provide the appropriate shift.

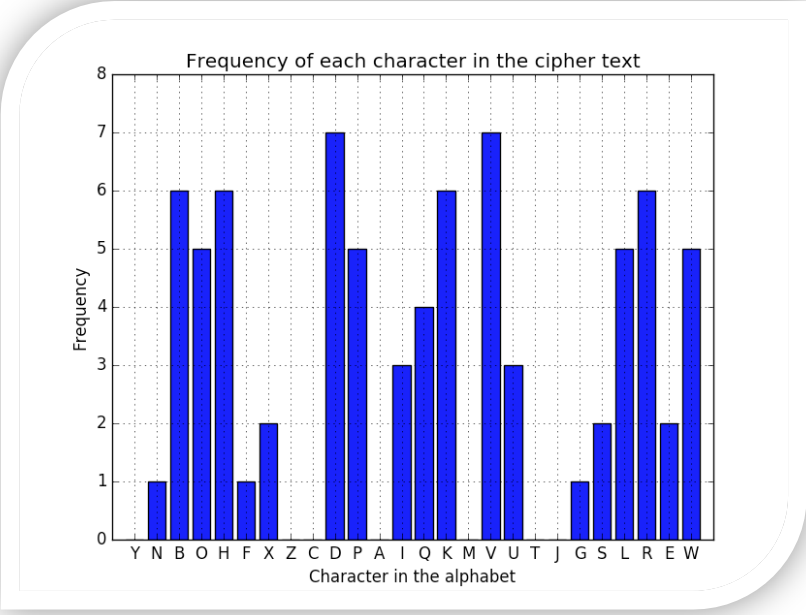

Figure 1. Frequency of each character in the cipher text.
The result analysis from count.py

First Attempt to decrypting the cyphertext

In my first attempt in decrypting the cyphertext I assume the most parsimonious condition. That is I assume:

1: Character '*D*' or '*V*' would represent the letter '*E*' in the plaintext.

2: The key length would be size 7 because the cyphertext is divisible by 7 and would not require any padding when decrypting the text.

3: The decrypted plaintext would contain the most words, from a dictionary.

The results from these assumptions yield only unreadable text. Figure 2 displays the plaintext with the highest common word count along with the column sequence. This methodology was not enough to break the code; the scope of my investigation was too narrow. For my second attempt I will widen my scope of investigation to all other key lengths and Caesar shifts.

```
COMMON WORD COUNT            PERMUTATION              TEXT
Shift: 3
              23             (7, 3, 5, 1, 2, 6, 4)  HFAAHHMLHUOALHIMPMRIMSDRTYSSETOMHELFLTTFFYESOUEEYYLIENYAHBRASHSEPBONESITYAOIS
              23             (5, 1, 3, 2, 7, 6, 4)  AAFHHHMUOHALLHPMMRIIMRTDYSSSOMTHEELTTLFFFYOUSEEEYIELNYYARABSHHSBOPNEESYATOIIS
              23             (6, 3, 5, 1, 2, 7, 4)  HFAAHHMLHUOALHIMPMRIMSDRTYSSETOMHELFLTTFFYESOUEEYYLIENYAHBRASHSEPBONESITYAOIS
              23             (5, 1, 3, 2, 6, 7, 4)  AAFHHHMUOHALLHPMMRIIMRTDYSSSOMTHEELTTLFFFYOUSEEEYIELNYYARABSHHSBOPNEESYATOIIS
              22             (5, 6, 3, 2, 7, 1, 4)  AHFHHAMULHALOHPIMRIMMRSDYSTSOETHEMLTFLFFTYOESEEUYIYLNYEARHBSHASBEPNEOSYITOIAS
```

Figure 2. Strings with the most common word count.
Key length of 7 did not produce a successful plaintext. From Mostwordskey.txt

Widen the Scope of investigation

From my unsuccessful initial attempt I learned that the key length is not seven and the Caesar shift is not limited to the common characters in the cyphertext. To widen the scope of investigation I had to cast a catchall net (Figure 3). This system will produce all possible combinations of plaintext. First, the cyphertext will be analyzed through all Caesar cypher shifts. Second, each of those texts will be broken down into columns by all possible key lengths and the columns will be arrange by all combination ($_{\text{key-length}}P_1$) and then concatenate to build the plaintext. And finally, the text is crossed referenced by a dictionary and the plaintext with the most words would be the decrypted text.

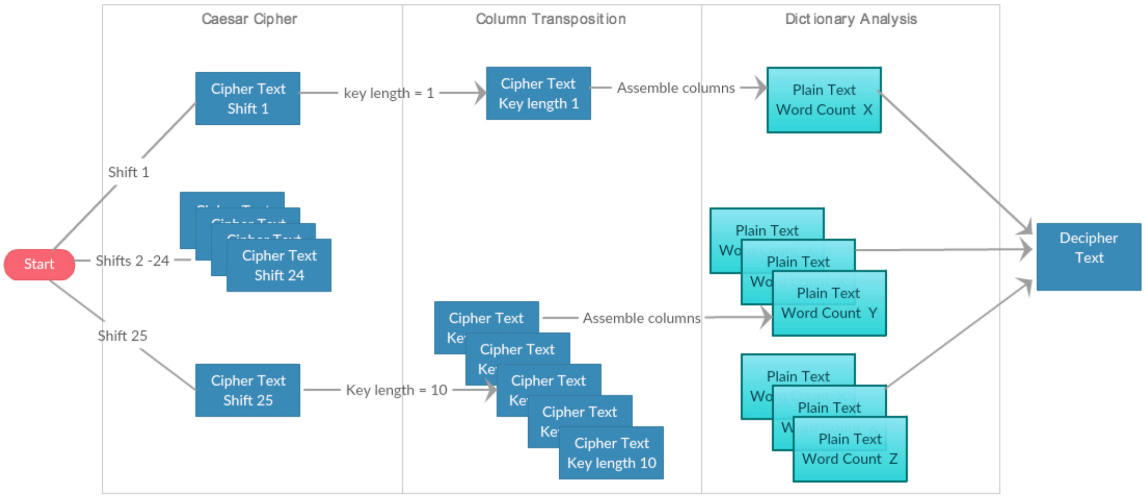

Figure 3. The three stages of deciphering. The figure above displays the three stages of deciphering: Caesar Cipher, Column Transposition, and Dictionary Analysis.

When I concluded with this approach I found the plaintext to be in the Caesar Cipher shift of 3, key length 5, common word count of 47, and column combination of (3, 5, 2, 1, 4) (Figure 4). The decrypted text is 'BE HAPPY FOR THE MOMENT THIS MOMENT IS YOUR LIFE BY KHAYY AMOHANDAL SO THIS CLASS IS REALLY FUN'.

```
Shift: 3
              47            (3, 5, 2, 1, 4)       BEHAPPYFORTHEMOMENTTHISMOMENTISYOURLIFEBYKHAYYAMOHANDALSOTHISCLASSISREALLYFUN
              33            (4, 3, 5, 2, 1)       PBEHARPYFOOTHEMTMENTOHISMIMENTRSYOUBLIFEYYKHAHYAMOLANDAISOTHSSCLAESISRFALLYUN
```

Figure 4. Plaintext results. This figure display part of the results from DictionaryResutls.txt.

Conclusion

The plaintext is was found to be; *'BE HAPPY FOR THE MOMENT THIS MOMENT IS YOUR LIFE BY KHAYY AMOHANDAL SO THIS CLASS IS REALLY FUN'*. The cipher text was not discovered under parsimonious conditions but by brute force where I had to run every possible combination.

What I've learned from this assignment is improving my methodology. In tackling this problem is first create a simple test case and run the software to test its merit. By doing so I found my algorithm works or I found bugs that needs to be fix.

Citation

"Letter Frequency." *Wikepedia*. N.p., n.d. Web.