Matthew Brown, Gunnar Eastman, Samuel Morse

COS 430

Task A1: Decrypting ciphertext.txt

• (15 Points) Explain the steps you took to decrypt the text in detail and provide the key and the original text.

The first step I took was to examine the most popular letters, bigrams, and trigrams in both the english language and the cipher text. In this case, I noticed that both the encrypted bigrams ok and ko were prevalent, and decided to examine the potential of the letters E and R being mapped to o and k in the cipher text. Given that o was more popular in the encrypted text, I chose to substitute E for o and R for k. From there, I noticed the five letter sequence xEvER appearing multiple times, and figured that it might be a name. I continued replacing popular letters, noticing that y appears alone several times, and tried replacing it with A, and v with T. I then replaced for Y and X in order to get “NEXT DAY.” with the five-gram at xETER now, I substitute x for P. After that, I found the word “NEARmrhHTEe” which I imagined could only be so many words, and chose “NEARSIGHTED.” After that it was just a matter of substituting the remaining letters such that the words would make sense.

• (15 Points) Explain what are the problems with the current encryption method and what you propose to improve it?

The major problem I encountered was the presence of spaces. That was the real difference between this and the cipher text assigned as the in-class participation, as a lack of spaces makes it far more difficult to crack, though as a novice that may just be a testament to my inexperience. After that, the use of a monoalphabetic cipher made the process relatively simple. Making it so that one character of plain text could be represented by multiple symbols of cipher text would make decryption more difficult. This could also be true for replacing uppercase and lowercase letters with different symbols, such that the P's in Peter would be different from the p's in other words.