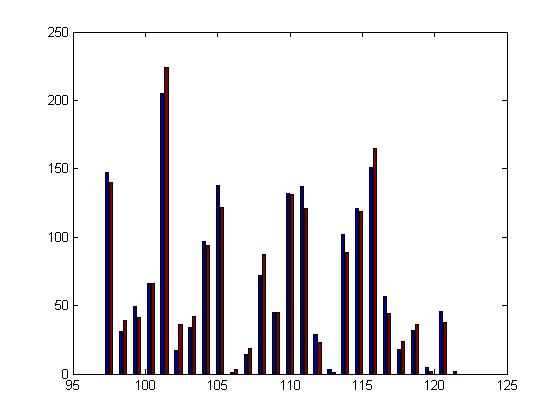
Matthew Krause

Math 056 H

Prof. Karl Petersen

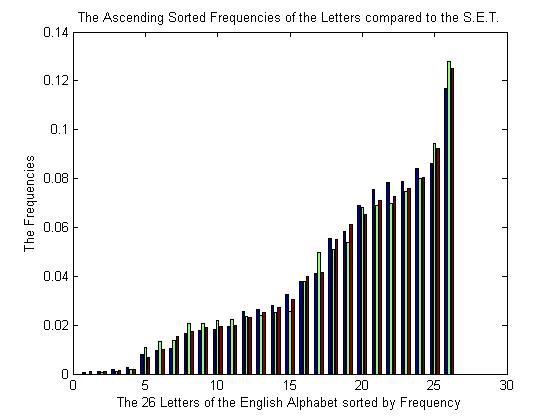
The index of coincidence for the text, which tests to see if the ciphered text contains frequencies similar to that of Standard English Text, is 0.0648. This is very close to 0.065, meaning that the cyphered text very closely resembles a simple monoalphabetic substitution. Now that we know that the cyphered text closely resembles a simple monoalphabetic substitution, we look for the frequency of each letter, and compare it to that of standard English text. This is given by Figure 1.

Figure 1



Now we are to assume that the keylength of the cypertext is of length 2. We run the command “initPASCC(2)” which cracks the ciphered text of a polyalphabetic substitution ciphered text with a keylength of 2. One of our output is the L1Distance (which is the distance between the frequency of characters), 0.0591. Since this is close to 0, it is close to the frequency of standard English text. When graphed (Figure 2), it is easy to see that the frequency in standard English text (far right bar) is similar to that of the ciphered text.

Figure 2



From here, we can view and analyze the candidate Plain Text. Through various swapping in the substitution of the matrix, we can finally break the cypher to reveal it’s message, which is a continuous string of text that can be broken up into words and sentences.