Dr. R. Beezer
Practicum #2
Monoalphabetic Substitution Cipher

Math 133
Fall 2003

A *monoalphabetic substitution cipher* is a process for obscuring a message by replacing each letter of the alphabet with a different letter. This is the "substitution" part of the name, the "monoalphabetic" means just one set of substitutions is used, and remains the same throughout the encoding of the message. Frequency analysis is the most common method used to break a code like this.

**Procedure**

1. You will receive an email message from me with a message encoded by a monoalphabetic substitution cipher. The text is about 1000 characters long.
2. The "Mono" program by Stumpel is a useful tool for testing different keys progessively (link on course page). Save your ciphertext into a file of its own (cut-and-paste into Notepad, for example). Fire up `mono.exe` and have it read the file with the ciphertext. Use the space bar to see different ways of arranging the two alphabets (cipher frequency is the best). Use the right/left arrow keys in concert with the letter keys to test out substitutions.
3. The "Cryptogram Helper Applet" might be also useful, except the frequency graph seems to be overwhelmed by a larger file. Drag and drop letters to create a test key.
4. Tables of frequencies of single English letters, and pairs of English letters can be helpful. Single letter tables are common, and there is a table of letter pairs and triples in the Army Field Manual link.
5. `letcount.exe` is a simple program that will give you counts of letter frequencies and digraph frequencies. I will email everyone a copy of this program.
6. Once decoded, an Internet search should reveal the author of your text.
7. You will reply to me with the name of the author of the text.

**Grading**

1. Sending me the correct author's name will earn you full credit.

**Notes**

1. My encryption program for this exercise is a bit rusty, punctuation is stripped out on purpose, but right now numbers also get stripped out, so any dates will be missing.
2. Plaintext is the first few paragraphs of a classic piece of literature. As such, some of the usage of the English language is a bit convoluted.
3. Frequency analysis is always presented as being very easy and routine. With this exercise, you should discover that there is a bit of "art" in doing it quickly.