Math 139 Problem Set #4 Due 13 March 2003

Reading: Singh, Chapter 2; Barr, §§ 2.3, 2.5.

Exercises: Write your solutions clearly, remembering that they will be graded for presentation as well as correctness.

A1. Consider using a computer to decrypt a general mixed-alphabet cryptogram by brute force. Suppose the computer can check 10^9 decryption alphabets per second (including the time required to decide whether the result is sensible or not).

(a) How long will it take for the computer to check all 26! possible alphabets? Give your answer in the most appropriate time units.

(b) Suppose that we are able to guess (correctly) the ciphertext equivalents of the letters `t`, `h`, and `e`. Once these letters are fixed, how many decryption alphabets will we have to check? How long will it take?

(c) Now suppose we know the ciphertext equivalents of `t`, `h`, and `e`, and we are quite confident that the four least common letters in the cryptogram are the cipertext equivalents of `q`, `j`, `x`, and `z` (but we don't know which of these four is which). How many decryption alphabets will we have to check? How long will it take?

(d) Finally, suppose that we do frequency counts on a great deal of text and find the following:

- There is one letter that is clearly the ciphertext equivalent of `e`;
- There are seven other high-frequency letters, which must correspond (in some order) to `t`, `a`, `i`, `n`, `o`, `s`, and `r`;
- There are four medium-frequency letters, which must correspond (in some order) to `h`, `l`, `d`, and `c`;
- There are five very low-frequency letters, which must correspond (in some order) to `k`, `j`, `q`, `z`, and `x`.

How many decryption alphabets will we have to check? How long will it take?

B1. Pick one of the cryptograms on the handout Cryptograms #6 and cryptanalyze it. Provide a short explanation of how you reconstructed the encryption or decryption alphabet. You don't need to decrypt the entire message (unless you want to); the first hundred letters will do.

B2. Pick one of the cryptograms on the handout Cryptograms #7 and cryptanalyze it. Provide a short explanation of how you determined the keyword. Give a decryption of at least the first hundred letters of the cryptogram.