NETWORKS AND CRYPTOGRAPHY
PROJECT 2
Cracking a substitution cipher

1 Getting the ciphertext

Once again, we will do these projects on the CS department server, `castor.cs.amherst.edu`, or on the workstations in Seeley Mudd 007. To get started, login to one of these systems and bring yourself to a shell, then follow these steps to get the starting source code:

```
$ cd cs281
$ mkdir project-2
$ cd project-2
$ cp -v ~sfkaplan/public/COSC-281/project-2/<yourusername>.ciphertext .
```

The file that you obtain is encrypted just for you. The original plaintext was stored as an standard, UNIX text file (that is, a sequence of bytes using a common extended ASCII encoding; a detail that actually matters little). Each byte was replaced with a randomly chosen (yet consistent) other byte value.

2 Crack the code

Your job is a simple one: **decrypt the ciphertext**. I strongly suggest that you obtain a sufficiently large, sample cleartext of English textfiles. (I suggest, for example, some items from Project Gutenberg.) Measure the frequencies of the byte values in those, thus including a measurement of spaces, newlines, commas, etc. Then perform frequency analysis on your ciphertext, and thus begin to match up the most frequent values, building a map of ciphertext symbols to likely cleartext symbols.

3 How to submit your work

Follow the directions in the decrypted file once your crack it. Use `cs281-submit`, using the project name `project-2`. Note that must submit a correct decryption of your ciphertext file in order to move onto Project 3.

This assignment is due at **11:59 pm** on **Sunday, April 07.**