Group 10: Alinda Heng, Jessica Perez, & James Allen
MATH 354: Analysis of Algorithms, Fall 2016

Assignment 6

Instructions

Decrypt the given ciphered text.

Experiment

For our code, we used brute force by trying all of the possible combinations for an 8-bit binary sequence as the key. There are 256 different combinations, so we inputted the ciphered text and used each possible key on it, outputting the results in another document.

From the resulting document, we can simply browse through the output and look for the one that makes sense. We find that the working key is 01101110 (or 110 in decimal). The deciphered text is the following:

Call me Ishmael. Some years ago--never mind how long precisely--having little or no money in my purse, and nothing particular to interest me on shore, I thought I would sail about a little and see the watery part of the world. It is a way I have of driving off the spleen and regulating the circulation. Whenever I find myself growing grim about the mouth; whenever it is a damp, drizzly November in my soul; whenever I find myself involuntarily pausing before coffin warehouses, and bringing up the rear of every funeral I meet; and especially whenever my hypos get such an upper hand of me, that it requires a strong moral principle to prevent me from deliberately stepping into the street, and methodically knocking people's hats off--then, I account it high time to get to sea as soon as I can. This is my substitute for pistol and ball. With a philosophical flourish Cato throws himself upon his sword; I quietly take to the ship. There is nothing surprising in this. If they but knew it, almost all men in their degree, some time or other, cherish very nearly the same feelings towards the ocean with me.

Analysis

The point of this exercise was to realize that the scheme used to encrypt the plaintext, a recycled one-time pad in which each group of 8-bits were XORd with the same 8-bit key, was highly insecure and trivial to crack. There are only 2^8 = 256 possible 8-bit keys to try out on our ciphertext so it was easy to create a script to cycle through all of the possible combinations until we obtained a result that made sense. A more secure scheme would have involved replacing the key at each step with the new group of 8-bits after XORing with the ciphertext. To brute force this, an attacker would need to cycle through 256 combinations for each individual group of 8-bits, which would become exponentially more difficult as the length of the ciphertext increased.