Assignment 1- Part 3 - Report

Eugenio Ribón

Code description

The code first takes ciphertext as an input, then it iterates through all the keys in the dictionary shifting the ciphertext character by that key if it is a letter and ignoring the rest of characters. It then displays the result for every key allowing the user to manually look for the correct one. It can be run by using the ./mc_cipher file and then introducing the text to decipher.

Attack method

This is a brute force attack that decrypts the ciphertext for every key. It makes no distinctions between lower and upper case characters. Also it only affects letters from the english alphabet and ignores all other characters.

Alternative method

Instead of a brute-force attack, you could use Frequency Analysis. This method relies on the statistical fact that certain letters in the English language appear more frequently than others . By calculating the frequency of letters in the ciphertext and comparing them to standard English letter frequencies, the program can programmatically determine the most likely key without human review.

Results

Key = 13 left, 13 right.

Plaintext = “to be, or not t%o be: that is the q@uestion”