Assignment 1- Part 3 - Report

Joseph May

Code description

The code runs as 2 for loops, the first loops over every letter in the alphabet to shift by and the other loops over the length of the ciphertext to shift every letter. If statements are used to ensure that both upper and lower case letters are handled correctly. For lower case letters the ascii value of a is subtracted then the shift is added, then the alphabet size is added to account for negative numbers as a precaution, the value is then mod with the alphabet size to handle wrap around and then the ascii value of a is added back to give the correct shifted letter. This is the same for upper case letters with a swapped for A. Each character is then printed after the shift and spaces are also outputted but none of the special characters are.
The makefile is called Part3Makefile. In order to run it, run the command make -f Part3Makefile. This creates the executable file called mc_cipher.

Attack method

I used a brute force attack in order to break this cipher. This tries all 25 possible shifts for the cipher and outputs the plaintext for all of them.

Alternative method

An alternative method for decrypting this cipher would be to use frequency analysis. To do this instead of trying every possible combination, each letter would be tallied to see how often it appears in the ciphertext, the shift would then be done between that letter and E since E is the most common letter in the English language. To achieve this in the code, instead of the first for loop iterating over the alphabet, it would be replaced by iterating through the word separate to the for loop for shifting and tallying the letter. The letter that was the most common would be subtracted from E in order to get the shift and then the other for loop would run through the ciphertext shifting this value for every letter.

Results

Left shift by 22 (V, v) or right shift by 4 (D, d)

Plaintext -> never forget what you are, for surely the world will not