

CSc 3320 - Assignment 6

Caesar Cipher

Andrew Rosen

Due **6AM**, April 16th

Abstract

This assignment focuses on File IO and basic cryptography, the Caesar cipher.

1 The Assignment

The task in this assignment is to solve a very simple cipher. Ceaser ciphers, named after the emperor Julius, consist of replacing each letter in a message with the letter n places down ($\bmod 26$ for English). For example, with the key of 10, all instances of ‘a’ would be replaced by the letter ‘j’. Each key has an inverse which is simply $26 - key$, so that applying the Ceaser cipher with that inverse will result in the plain text.

$$((a + key) \bmod 26 + 26 - key) \bmod 26 = (a + key - key) \bmod 26 = a$$

While tedious to solve with paper and pencil these ciphers are very easy to solve by machines. Since we know that ‘e’ is the most common English letter, we can find the most common letter in the Ceaser cipher and work out what was added to ‘e’ to get that letter. Once you have the key, you can figure out the needed inverse of the key which, when applied to each character of the ciphertext, produces the original character.

Your task is to write a program that finds the key needed to decrypt text encrypted with a Caesar cipher and prints out original plaintext. To help you in your task, I’ve provided `caesar.c`, a program that will encrypt text using the Caesar cipher. Test your program on `text.one.encrypt`. If your program can decrypt it, it works.

2 Hints

- Examine `ceasar.c` and figure out how it works before writing code.
- Be sure to initialize any arrays you create.

3 Submission Directions

Submit your homework to Brightspace/D2L. Please submit only the `.c` file, but remember, **if the code doesn't compile, you get a zero.**