Basic Cryptography and Decryption

Evan Reynolds

CSCI 101-B

Modern cryptography is an enigma that most people don’t understand or care to understand. For my create project, I will develop a program that can encrypt, decrypt or even break basic encryption (using a specific set of circumstances and a specific encryption algorithm). There will be two inputs to this program. One input will be a txt file containing a message to either decrypt. The second input will be either the operation to either encrypt the file or break it or the key to decrypt it as you would normally. Depending on what operation you’re using, the output will be either a decrypted version of the message or an encrypted version of the message given in both the terminal and as a text file in the same directory of the program.

I will be the only developer of this program, but I will try and get ideas from friends to see what could be beneficial to the program beyond just the basic encryption, decryption and breaking of an encrypted file. I’m going to be collaborating creatively, but beyond that, I’ll be writing everything myself.

As of this moment, my only concern is how difficult my encryption algorithm is to break. While I want it to be breakable by a personal computer, I don’t want it to be broken in a matter of seconds. Since I don’t have the knowledge to build a complex encryption algorithm, I would likely be able to decrypt it extremely easily. I can add more complexity to my program by adding different type of ways to decrypt it.