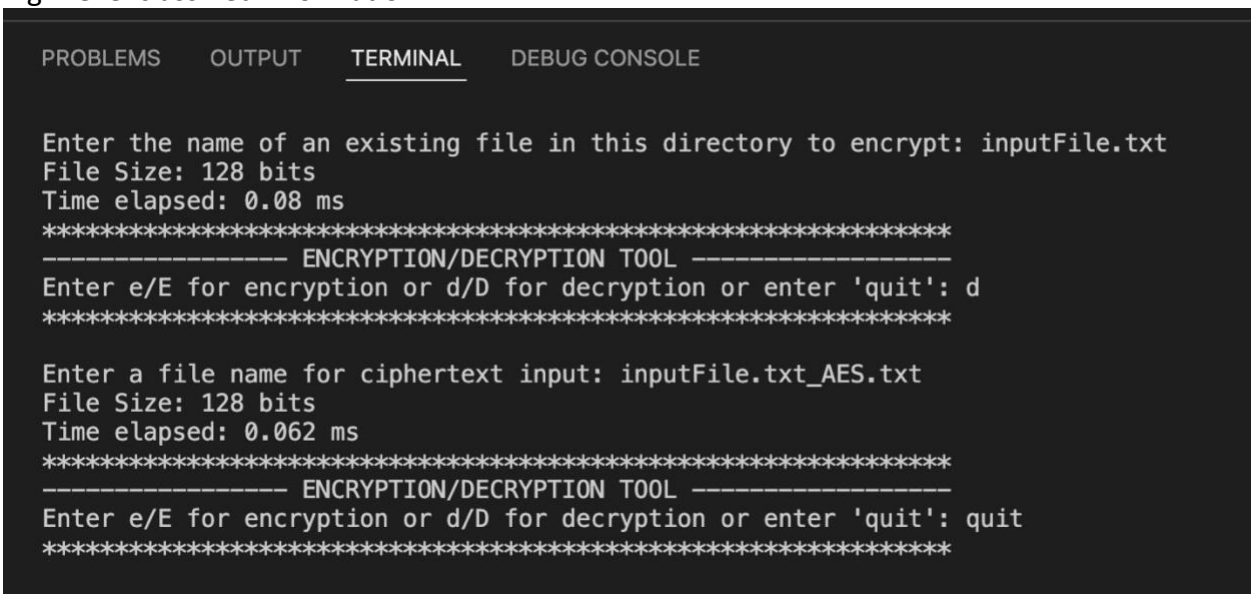
Austin Hale
CSCI 360

Mini Project 1 Report

This project covered the encryption scheme called AES and its implementation using the language Python. In the project I created a Python script with functions for encrypting and decrypting using AES that allowed the user to take file input and write out to files. AES is one of the most popular encryption schemes in the world, especially in America, where it was declared the national standard encryption scheme over a decade ago. AES is a symmetric block cipher and functions by taking a plaintext input and a secret key input of 128, 192, or 256 bits, then passes the ciphertext and plaintext through its cipher and returns the ciphertext of corresponding size to the key. In my program, a menu appears that asks the user to press “e” or “d” to select encryption or decryption. When “e” is pressed, the user is asked to give an input file, then the text from the file is read and sent through the AES encryption scheme, then the resulting ciphertext is outputted into a new text file. This file can then be read when the user presses “d”, and the program asks for an input file for decryption. The plaintext is then outputted into a decryption output file. Both functions also output the file size in bits and the elapsed time in milliseconds. One major example use case of the AES encryption scheme is the United States government. All major US government encryption is done using AES, spare some high-level classified information.



Overall, I learned a great deal about AES encryption through this project, and I also gained a much better working understanding of programming in Python, which will likely be very useful in the future.