Specifications Document:

Features of Ceasar Cipher Implementation:

Encryption Mode:

Purpose:

Encryption mode allows user to have a message encrypted of any length when given a single character key. The output gets displayed to the terminal and to a file.

Assumptions:

The message to be encrypted must contain only capital letters and the space character. All other characters are rejected. Lower case letters are converted to capital letters.

Inputs:

Encryption takes a single character string as well as a message of any length as a string.

Outputs:

The message that was taken as input will be encrypted based on the key that was taken. The message is output to the terminal as well as a to a file.

State changes:

The text file that the message was output to will hold the encrypted message.

Cases:

When the Ceasar cipher is selected in the program prompt, the user can choose to encrypt or decrypt a message. For encrypting a message, a key of one letter is taken as input and is checked to make sure that only letters and the space character are accepted, the same is applied for the message.

Expected Behavior:

After running encrypt, the message will be listed in the new file as well as printed to the terminal in all uppercase letters. This file is separate from the decrypt option in order to distinguish the two from each other.

Decryption Mode:

Purpose:

Decryption mode allows the user to decrypt a message and have it displayed on the terminal as well as a new file.

Assumptions:

Decrypt mode must have a message and a key that contains only letters and the space character. The key must only contain one character.

Inputs:

A key and a message are taken as strings by the user.

Outputs:

The message taken as input is decrypted and is output to the terminal and a separate file.

State Changes:

The new file named “Decrypt.txt” will be created and contains the decrypted message after running decrypt mode successfully.

Cases:

When the user chooses to run decrypt with the Ceasar cipher, the message and key are checked to make sure that they are valid to run the decrypt function. This means that only letters and spaces are accepted as inputs.

Expected Behavior:

After running decrypt, the decrypted message will be displayed in all capital letters in both the terminal and the new file that was created. No changes should be made to the encrypt file that was created for encrypting a message.

Features of Main Implementation:

Running The Program:

Purpose:

The main function combines the Ceasar cipher, Vigenère cipher, and one-time pad cipher into one file so that all three can be chosen from by the user to encrypt and decrypt messages. The user can also choose to exit the program after performing some function with a message.

Assumptions:

The user will pick a cipher to encrypt or decrypt a message to be displayed in the terminal and a separate file.

Inputs:

The user will be prompted to choose which cipher they want to run, as well as encrypt or decrypt a message from that specific cipher. From there the user will be prompted to give a valid key and message.

Outputs:

Depending on what the user decides for encrypting or decrypting, the message will be saved into the appropriate file as a string in all uppercase letters and spaces.

State changes:

The message will be converted to all uppercase letters if using lowercase letters and the new file will contain the user's message.

Cases:

When the user enters valid input, the program will take the user into the next section of the cipher and its functions. The result will be the encrypted message or decrypted message in a separate file.

Expected Behavior:

A user is prompted to enter what cipher they would like to use or if they would like to exit program. After choosing a cipher, the user is prompted to select either encrypt or decrypt. Both options will ask for a key and a message, and the result will go into the appropriate file.