**Project 1 - Documentation**

**Student ID(CWID):** 884976077

**Full Name:** Andreia Shin

The algorithms used for the project was:

**Encryption**

1 - Caesar Cipher (function - caesarCipher)

This algorithm requires 2 inputs. A text (string) and a key(integer). It checks for any alphabetic letter and it shifts forward by the key number. It handles the upper and lower cases. Non-apathetic characters such as spaces, punctuation and numbers, are left alone. So for example if the text is "Hello” and the key is 3 the result we would get would be "Khoor”.

2 - Substitution Cipher (function - substitutionCipher)

Like the previous algorithm, substitutionCipher also requires the same two inputs but in this case we are getting the text that had already been modified by the caesar cipher function which adds another layer of encryption. This algorithm takes any vowels ( a, e, i , o , u) lower or uppercase, transforms them into their ASCII number and adds the key number to it. I did had to add “\*” in between when appending the numbers in order to handle cases that have vowels next to each other. If not, it would be very difficult to decrypt the message. For example, the text "Khoor” would turn to be “Kh\*114\*\*114\*r”. The vowel o is 111 + the key - 3 = 114.

**Decryption**

For the decryption user is asked to input the encrypted file with the key. First the code reverses the substitution cipher with the decryptSubstitution function turning the ASCII numbers into letters again and restoring the original vowels. Then it applies the Caesar one more time but this time it turns the key into a negative number which shifts the vowels to its original position.

**File handling** - both handle if a file cannot be found or if there is an unexpected error.

encrypt\_file(input\_file, output\_file, key) → Reads a file, encrypts it, saves results to encrypted.txt.

decrypt\_file(input\_file, output\_file, key) → Reads an encrypted file, decrypts it, saves results to decrypted.txt.

**User interface**

It requests that the user input a text file with the message they want to encrypt / decrypt and also the key.