

Project #1 [50 points]

Due date is Thursday, July 4th

This project involves some tasks involving historical substitution ciphers, working with decryption and encryption tasks. The idea of this project is to get you comfortable with historic ciphers and the basic concepts of decryptions/encryptions and brute forcing.

Task 1 [30 points] :

Write a function that will take in two strings and encrypt the first string with the second string using the Vigenere cipher. The first string is the plaintext and your function should ignore all non-alphabetic characters (or your code can remove them from the string). All uppercase letters should be treated as lowercase letters (or you can convert the string to all lowercase letters). The second string is the key and it should be able to be from 1 character long to even longer than the plaintext string itself.

Then write a function that, given two strings, decrypts the first string using the second string. Same conditions should apply as before.

Once these functions are completed, have your main body prompt the user for a string to encode, then a key string, then perform the encryption of the plaintext and output the ciphertext.. Then decrypt it and show the resulting plaintext.

Task 2 [20 points] :

In this task, we are wanting to automate the process of decrypting a string using the vignere cipher.

In the main body, prompt the user for a ciphertext string encoded by the vignere cipher with an unknown key. Then prompt the user for a substring that we know has to be in the plaintext and a maximum size of the key (from 1 to 10 let us say). Your code should then brute-force the vignere cipher by decrypting the text using a possible key and then examining the possible plaintext for the substring. If the substring is in the possible plaintext, your code should print it out as a possible result, along with the key found, and then prompt the user if they would like to continue. You should also stop at every increment of keysize and ask them if they wish to continue the brute force.

Submission:

Submit your source files and any associated files, unzipped, through canvas. Do not submit by email. In the notes on canvas, please describe your coding environment and any problems you might have encountered. Also include a document/screenshot demonstrating your code working.

If you did not complete some part of the assignment, please describe what you did complete and what you were not able to finish. Partial credit will be given if work has been done.