Name:______________________

Introduction to Cryptography
Project 1

(1) Implement a program in Python that
  (a) Prompts the user to choose whether to encrypt or decrypt a message;
  (b) prompts the user for a cipher method (additive Caesar or one-time pad);
  (c) prompts the user for an appropriate key depending on the chosen method;
  (d) prompts the user for the plaintext or ciphertext;
  (e) turns all letters to upper case and skips over spaces and punctuation when performing the encryption/decryption;
  (f) prints the encrypted or decrypted message as a string.

(2) Consider the following ciphertext, which was obtained using an additive Caesar shift: "FTQ QZQYK UE AHQD FTQ YAGZFMUZ". Write a program that tries all decryption keys, and then use your program to decrypt the message. Why is such a method intractable for a ciphertext obtained from using a one-time pad?