Name:______________________

Introduction to Cryptography
Substitution Cipher

A substitution cipher is a method of encryption in which each letter of the alphabet is replaced by another letter of the alphabet. The substituted letter may be the same as the original letter, but two distinct letters may not be substituted with the same letter. As an example, suppose in a message the letter B is always replaced by the letter Q, then no other letter may be replaced by the letter Q. Put another way, if we define the plaintext alphabet in Python by the string ”ABCDEFGHIJKLMNOPQRSTUVWXYZ”, then a valid substitution alphabet may be ”QWERTYUIOPASDFGHJKLZXCVBNM”, while the substitution alphabet ”AAAAAAAAAAAAAAAAAAAAAAAAAA” is not valid.

(1) Implement a program in Python that
   (a) prompts the user whether to encrypt or decrypt a message;
   (b) prompts the user for the plaintext or ciphertext message;
   (c) prompts the user for a substitution alphabet and checks to make sure it is valid for substitution;
   (d) prints the encrypted or decrypted message as a string.

(2) What would go wrong if the restrictions were removed for a substitution alphabet to be considered “valid?” Why is this undesirable?

(3) We have discussed several cipher methods in this course including the additive Caesar, One-Time Pad, and Vigenere. Which of these are also considered substitution ciphers? Explain your answer.