

Name:\_\_\_\_\_

Introduction to Cryptography  
Vigenere Cipher

- (1) If a one-time pad is shorter than the message, one can simply repeat the pad until the message is complete. The method is called a Vigenere cipher. For example, we can encrypt the plain text message ILOVEMATHEMATICS using the Vigenere key CAT by computing “ILOVEMATHEMATICS”+“CATCATCATCATCATC” to obtain “KLHXEFCTAGMTVIVU”.

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 an appropriate key and implements the Vigenere cipher if the key is shorter than the message and implements the one-time pad if the key is longer than the message;
- (d) skips over punctuation and spaces whenever performing the encryption/decryption;
- (e) prints the encrypted or decrypted message as a string.