

# 1 Introduction

## 1.1 Decrypt the ciphertext provided at the end of the section on monoalphabetic substitution ciphers.

JGRMQOYGHMVB BJRWQFPWHGFFDQGFPFZRKBEEBJIZQQOCIBZKLFAFGQVFZFVWE  
OGWOPFGFHWOLPHRLLOLDFMFGQWBLWBWQOLKFWBYLBLYLFSFLJGRMQBOLWJVFP  
FWQVHQWFFPQOQVFPQOCFPOGFWFJIGFQVHLHLROQVFGWJVFPFOLFHHGQVQVFILE  
OGQILHQFQGIQVVOSFAFGBWQVHQWIJVWJVFPFWHGFIIHZZRQGBABHZQOCGFHX

## 1.2 Provide a formal definition of the Gen, Enc, and Dec algorithms for the mono-alphabetic substitution cipher.

*Gen*: Letting  $A = \{a, b, c, \dots, z\}$ , *Gen* is the function that *uniformly* generates a one-to-one and onto (*bijective*) mapping from  $A$  to  $A$ .

*Enc*: Denoting the output of *Gen* as  $k$ , *Enc* is the function that replaces each character,  $p_i$ , in the plaintext with the value given by  $k(p_i)$ .

*Dec*: *Dec* is the function that replaces each character,  $c_i$  in the ciphertext with the value given by  $k^{-1}(c_i)$ .

## 1.3 Provide a formal definition of the Gen, Enc, and Dec algorithms for the Vigenere cipher. (Note: there are several plausible choices for Gen; choose one.)

*Gen*: *Gen* uniformly and randomly chooses an integer  $t$  and generates  $k = k_1 k_2 \dots k_t$  by choosing  $k_i = A_j$ , where  $A_j$  is a uniformly random choice from  $A = \{a, b, c, \dots, z\}$ .

*Enc*: Assuming that we have  $a = 0, b = 1, \dots, z = 25$ , *Enc* is given by the function that calculates the  $i$ th value of the ciphertext as  $c_i = (p_i + k_{(i \bmod t)+1}) \bmod 26$ .

*Dec*:  $p_i = (c_i - k_{(i \bmod t)+1}) \bmod 26$

## 1.4 Implement the attacks described in this chapter for the shift cipher and the Vigenere cipher.

See shift.py and vigenere.py

## 1.5 Show that the shift, substitution, and Vigenere ciphers are all trivial to break using a chosen-plaintext attack. How much chosen plaintext is needed to recover the key for each of the ciphers?

*Shift*: We just need one character of plaintext: Obtain the ciphertext and observe the difference mod 26 between the plaintext and ciphertext. That is the shift.

*Substitution*: We need 26 characters of plaintext: Obtain the ciphertext for a string containing all letters of the alphabet and observe the corresponding mappings in the ciphertext.

*Vigenere*: We would need to choose a plaintext string that is at least as long as the longest possible key length and observe the offset. Whenever the offsets begin repeating, we have discovered the key.

- 1.6 Assume an attacker knows that a user's password is either abcd or bedg. Say the user encrypts his password using the shift cipher, and the attacker sees the resulting ciphertext. Show how the attacker can determine the user's password, or explain why this is not possible.**

With a shift cipher, each character of the plaintext is offset by the same amount. If the user's password is abcd, then the first two characters will be offset by 1, and if the user's password is bedg, then the first two characters will be offset by 3.

- 1.7 Repeat the previous exercise for the Vigenere cipher using period 2, using period 3, and using period 4.**

- 1.8 The shift, substitution, and Vigenere ciphers can also be defined over the 128-character ASCII alphabet (rather than the 26-character English alphabet).**

- 1.8.1 Provide a formal definition of each of these schemes in this case.**

- 1.8.2 Discuss how the attacks we have shown in this chapter can be modified to break each of these modified schemes.**