Segurança de Dados - Assignment 1

Pedro Malainho PG61005

1. Question 1

In this question, I searched for the most effective approach and ended up using cryptanalysis along with an algorithm called hill climbing. I applied it repeatedly to determine all the letters required to reconstruct the unknown key and its permutation.

I eventually realized that the encrypted text referred to a book by José Saramago, Ensaio Sobre a Cegueira. From that point on, the decryption process became significantly easier and faster.

Letters that did not appear in the ciphertext, such as K, W, and Y, were placed in the remaining available positions in alphabetical order.

The permutation used to decrypt was: “VJGEKTZABDPQYULOSNFMXIRHCW”

The (permutation,key) used to encrypt can be:

(“AHXUNRWZGCYMTFSQLOPKEDJBIV”, k=1) ⇒ “HIYJDSCXVBEOTRPKLWQFNAMUZG”

2. Question 2

To answer this question, I first divided the ciphertext according to the key length. Then, I used a Portuguese letter frequency dictionary, using the chi-squared statistic to determine the optimal shift for each column and reconstruct the key. Finally, I applied a simple decryption algorithm to convert the ciphertext into plaintext.
The key used to decrypt was: “AGIR”