Laboratory 1 - AISC

Breaking classical encryption schemes

members

March 15th, 2023

A.Y. 2021-2022

1 Introduction

To be filled

2 Exercise 1 - Monoalphabetic cipher

3 Exercise 2 - Vigenère cipher

The Vigenère is an encryption scheme based on the use of a key k of length m to encrypt the plaintext p as follows:

$$c_i = E(p, k) = (p_i + k_{i \mod m}) \mod 26$$

This means that letters at distance m are shifted by the same amount, as in a generic Caesar's cipher. As a consequence, a possible approach for cryptanalysis can be that of looking at the ciphertext as a set of subsequences obtained by considering letters at distance m of the cipher. Then, it is possible to act on these subsequences by analyzing letter frequencies. In this case, a brute force approach would be time consuming as the subsequences do not contain english words, but rather (pseudo-)random letters. In any case the frequency analysis is feasible, since these letters are extracted from an (encrypted) English text.

The cracking mechanism is that of trying evaluating the circular correlation of the letters in each subsequence with the theoretical vector of letter densities for the English language. This, however requires to estimate the length of the key, and to achieve this another previous step is needed.

The estimate of the key length is done once again by extracting information from the ciphertext, once again revealing the main disadvantage of this encryption scheme. Indeed, it is possible to evaluate a score, corresponding to the sum of squared frequencies of each letter for different subsequences lengths. Each language has a specific value for this score, which, in the case of English is 0.065.

By comparing the scores as functions of m, it is possible to find out the best value for the key length as the one for which the score is closest to 0.065.

In the case of the ciphertext found in document ‘cryptogram02.txt’, the estimated key length was 15 and the key was found to be “nowyouseethekey”.

3.1 Complexity of the algorithm

The complexity of the algorithm for breaking the Vigenère cipher can be estimated as:

4 Conclusions