

MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

HILLY – PART 2

Author: Yahya Almardeny

October 2017

Introduction

Hilly is an improved version of Hill cipher.

In the previous challenge (Hilly Part 1) you were given a plaintext P_1 and its corresponding ciphertext C_1 . The task was to decrypt a ciphertext C_2 and find its plaintext P_2 which was encrypted with the same key that was used for the aforementioned pair (P_1, C_1) .

In this challenge you are given a partly-known key K and a ciphertext C . The task is to decrypt this ciphertext and find its corresponding plaintext P .

Challenge (2/2)

You are also given the partly-known key K that was used to encrypt the ciphertext C :

?	?	472	?	?	13
4	?	?	234	?	?
?	-55	?	?	?	75
?	?	?	?	?	?
?	?	?	?	?	?
12	?	?	88	?	?

The solution consists of the plaintext P .

Please enter the solution in capital letters with spaces between the words.

Additional Files

The additional zip archive contains the following files:

- mtc3_hilly_description.pdf
 - ➔ detailed explanation of Hilly
- ciphertext_hilly-02.txt
 - ➔ the complete ciphertext C
- partly-known-key_hilly-02.txt
 - ➔ the partly-known key K
- hilly.zip
 - ➔ Python code and test files for Hilly

References

In the document "mtc3_hilly_description.pdf" the cipher is explained in detail.

You can find it within the additional zip file.

To avoid any confusion: The order of the symbols in the substitution table T_A in this challenge is different from the order in the example in the description file.