MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

HANDYCIPHER – PART 1

Author: Bruce Kallick

January 2015

Introduction

Handycipher is a low-tech stream cipher, simple enough to permit pen-and-paper encrypting and decrypting of messages, while providing a significantly high level of security. Handycipher was published and further improved in 2014.
Handycipher consists of a core cipher augmented by a random interspersing of null characters throughout the ciphertext as decoys intended to thwart attacks based on recognizing patterns in the ciphertext.
The core cipher incorporates two ciphers based on the same key: a simple substitution cipher and a nondeterministic homophonic substitution cipher.

Challenge

Part 1 of the Handycipher series is a partly-known plaintext challenge. How Handycipher works is described in detail in the extra pdf within the additional zip file.
Your task is to recover some of the 858-character plaintext message M, given the 3,679-character ciphertext C generated by encrypting M with Handycipher and the secret key K. (For a full break, try also to discover K.)
The ciphertext C is given as a text file within the additional zip file. You are also given there another text file containing the first 229 letters of the plaintext M.
The solution consists of the **first five words** of the **second-to-last** sentence of M. Please enter the solution with spaces.

References

In the document "MTC3_Handycipher_Description.pdf" the cipher is explained in detail. You can find it within the additional zip file.

Another detailed explanation can be found at
http://eprint.iacr.org/2014/257.pdf
Remark: The eprint paper also introduces the Extended Handycipher method (EHC). For the EHC cipher we will offer another series of MTC3 challenges.

Successful cryptanalysis of earlier versions of Handycipher can be found here – however, it's more fun to try by yourself ☺
https://oilulio.wordpress.com/2014/06/19/handycipher-decrypt/
https://oilulio.wordpress.com/2014/07/28/breaking-handycipher-2/

Additional Files

The additional zip archive contains the following files:

- MTC3_Handycipher_Description.pdf
  - ➥ detailed explanation of Handycipher
- known-plaintext_HC-01.txt
  - ➥ the known part of the plaintext
- ciphertext_HC-01.txt
  - ➥ the complete ciphertext
- handycipher.zip
  - ➥ Python code and test files for Handycipher