MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Weakened Handycipher – Part 1

Author: Bruce Kallick

May 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 first published in 2014 and then further improved.

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 Description (1/2)

This challenge uses an intentionally weakened version of Handycipher (HC) and is offered only as an exercise meant to explore the extent to which HC's security depends on the admixture of null characters.

The first challenge of the weakened Handycipher series is a partially-known-plaintext challenge. Your task is to discover the 2,185-character plaintext message M_7, and the key K_7, given the 5,928-character ciphertext C_7 generated by $E(K_7, M_7)$ where E is the core cipher part within Handycipher. With P_7 you are also given the first 1,009 characters of M_7, and you are given that one of the 20 rows, columns, and diagonals of the key matrix contains the characters $\{2\ 8\ 9\ H\ K\}$ – not necessarily in that order.

Challenge Description (2/2)

C_7 and P_7 are given as text files within the additional zip file. This zip file also contains an extra PDF that describes in detail how Handycipher works.

The solution consists of the names of the ten dogs mentioned in M_7. Please enter the names in the order in which they appear in the text, separated by commas.

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

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
- p7.txt
  - ➥ the known part of the plaintext for WHC-01 (Weakened Handycipher challenge, Part 1)
- c7.txt
  - ➥ the complete ciphertext for WHC-01 (Weakened Handycipher challenge, Part 1)
- handycipher.zip
  - ➥ Python code and test files for Handycipher