

MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

HANDYCIPHER – PART 4

Author: Bruce Kallick

April 2016

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 further improved in 2015 and 2016.

Part 4 of the Handycipher series presents the same challenge as Part 1, but employs an improved version of the cipher, which has been strengthened:

- (1) by adding another ten characters to the ciphertext alphabet,
- (2) by enlarging the key from 41 to 51 characters,
- (3) by increasing the number of null characters from 15 to 25, and
- (4) by interweaving random non-null "noise" characters in the Core part of the cipher before the null characters are added.

Challenge

Part 4 of the Handycipher series is a partly-known plaintext challenge. How Handycipher works is described in detail in the pdf within the additional zip file.

Your task is to recover some of the plaintext message M , given the 6,569-character ciphertext C generated by encrypting M with Handycipher and the secret key K . For a full break, you also could try to discover K .

The ciphertext C is given as a text file within the additional zip file. Also given there is another text file containing the **first** 229 letters of the plaintext M (therefore partly-known).

The solution consists of the **fifth word in each of the sentences** in M **not written by Tennessee Williams**. Please enter the solution with spaces between the words.

Remark: The end of each sentence is determined by a letter pair ". " or "? " which is not part of an ellipsis, an abbreviation, or a quotation attribution.

Additional Files

The additional zip archive contains the following files:

- mtc3_handycipher-6_description.pdf
 - ➡ detailed explanation of Handycipher
- known-plaintext_HC-04.txt
 - ➡ the known part of the plaintext
- ciphertext_HC-04.txt
 - ➡ the complete ciphertext
- handycipher.zip
 - ➡ Python code and test files for Handycipher

References (1/2)

In the document "mtc3_handycipher-6_description.pdf" the cipher is explained in detail. You can find it within the additional zip file.

A complete version history of Handycipher can be found at <http://eprint.iacr.org/eprint-bin/versions.pl?entry=2014/257>

Successful cryptanalysis of an earlier version 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/>

References (2/2): Overview of all HC challenges

- HC, Parts 1 & 4: known initial segment of the plaintext
- HC, Parts 2 & 5: known segment occurring somewhere in the plaintext
- HC, Parts 3 & 6: ciphertext-only

- EHC, Parts 1 & 4: known initial segment of the plaintext; three different encryptions of the same plaintext using the same key (but different session keys)
- EHC, Parts 2 & 5: known segment occurring somewhere in the plaintext
- EHC, Parts 3 & 6: ciphertext-only

- WHC, Parts 1 & 4: known initial segment of the plaintext
- WHC, Parts 2 & 5: ciphertext-only with some information about the key matrix
- WHC, Parts 3 & 6: ciphertext-only