MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Weakened 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 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 fourth challenge of the weakened Handycipher series is a partially-known-plaintext challenge. Your task is to discover the plaintext message M_{7a}, and the key K_{7a}, given the 6,372-character ciphertext C_{7a} generated by $E(K_{7a}, M_{7a})$ where E is the core cipher part within Handycipher. With P_{7a} there are also given the first 1,009 characters of M_{7a}, and there is given that one of the 20 rows, columns, and diagonals of the key matrix contains the 5 characters {x, C, U, e, G} – not necessarily in that order.

Challenge Description (2/2)

C_{7a} and P_{7a} are given as text files within the additional zip file. This zip file also contains a PDF that describes in detail how Handycipher works.

The solution consists of the **fifth word in each of the sentences** in M **not written by Jack London**. 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
- p7a.txt
  - ➥ the known part of the plaintext for WHC-04 (Weakened Handycipher challenge, Part 4)
- c7a.txt
  - ➥ the complete ciphertext for WHC-04 (Weakened Handycipher challenge, Part 4)
- 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 occuring 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 occuring 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