

# MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

## HANDYCIPHER – PART 9

Author: Bruce Kallick

December 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 9 of the Handycipher series presents the same challenge as Part 6, but incorporates a slight change in the cipher to remove a known vulnerability.

# Challenge

Part 9 of the Handycipher series is a ciphertext-only challenge. A 12,775-character ciphertext  $C$ , generated by encrypting a plaintext message  $M$  with Handycipher and the secret key  $K$ , is given as a text file within the additional zip file. This zip file also contains a PDF that describes in detail how Handycipher works.

Your task is to recover some of the the plaintext message  $M$ . For a full break, you also could try to discover  $K$ .

The solution consists of the **fifth word in each of the sentences** in  $M$ . 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-6.10\_description.pdf
  - ↳ detailed explanation of Handycipher
- ciphertext\_HC-09.txt
  - ↳ the complete ciphertext
- handycipher.zip
  - ↳ Python code and test files for Handycipher

## References (1/2)

In the document "mtc3\_handycipher-6.10\_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 & 7: known initial segment of the plaintext
- HC, Parts 2, 5 & 8: known segment occurring somewhere in the plaintext
- HC, Parts 3, 6 & 9: ciphertext-only
- 
- EHC, Parts 1, 4 & 7: known initial segment of the plaintext; three different encryptions of the same plaintext using the same key (but different session keys  $K'$ )
- EHC, Parts 2, 5 & 8: known segment occurring somewhere in the plaintext
- EHC, Parts 3, 6 & 9: ciphertext-only
- 
- WHC, Parts 1, 4 & 7: known initial segment of the plaintext
- WHC, Parts 2, 5 & 8: ciphertext-only with some information about the key matrix
- WHC, Parts 3, 6 & 9: ciphertext-only