MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

Extended Handycipher – Part 4

Author: Bruce Kallick

April 2016

Introduction (1/2)

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.

Introduction (2/2)

Extended Handycipher (EHC) operates with the same plaintext and ciphertext alphabets as Handycipher (HC), but has an extended complexity. It encrypts a message M using a key K by first generating a random session key K', and encrypting M with HC using K' to produce an intermediate ciphertext C'. K' is then encrypted with HC using K and embedded in C' at a location based on K and the length of M, producing the final ciphertext C.

Extending Handycipher in this way confers advantages in security at little computational cost. Because each plaintext message is encrypted with a different randomly generated session key, the primary secret key is less exposed to any attack that depends on having a lot of ciphertext to work with, and the security of the cipher is less compromised by encrypting multiple messages with the same key.

Challenge

Part 4 of the Extended Handycipher series is a partly-known plaintext challenge. How Extended 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 ciphertexts C_a, C_b and C_c created by encrypting M with Extended Handycipher and K three times, using three different, randomly generated session keys K'_a, K'_b and K'_c.

The ciphertexts are given as text files within the additional zip file. Also given there is another text file containing the **first** 229 letters of the plaintext M.

The solution consists of the **fifth word in each of the sentences** of 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 and Extended Handycipher
- known-plaintext_EHC-04.txt
  ➥ the known part of the plaintext
- ciphertext_Ca_EHC-04.txt, ciphertext_Cb_EHC-04.txt, ciphertext_Cc_EHC-04.txt
  ➥ three complete ciphertexts
- handycipher.zip
  ➥ Python code and test files for HC and EHC
  Remark: EHC will be used when using the option -x.

References (1/2)

The ciphers HC and EHC are explained in detail in the document "`mtc3_handycipher-6_description.pdf`" found 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

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