MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Handycipher – Part 10

Author: Bruce Kallick

June 2019

Introduction (1/5)

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 10 of the Handycipher series presents the same challenge as Part 9 but instead of using a randomly chosen 51-character key, the key has been chosen in a way designed to thwart attacks based on finding groups of consecutive colinear ciphertext characters.

Introduction (2/5)

Two or more characters are said to be colinear if they all lie in the same row, column, or diagonal of the 5 x 5 matrix.

Handycipher assigns to each character in the 31-character plaintext alphabet a 5-bit binary number $1 \leqslant b_1b_2b_3b_4b_5 \leqslant 31$ (according to the 31-character derived subkey). The number of "1" bits in $b_1b_2b_3b_4b_5$ then determines the number of consecutive colinear characters in the homophones generated in encrypting that character.

So, in order to decrease the number of groups of consecutive colinear characters in the ciphertext, the key has here been chosen so that the more frequently occurring plaintext letters are assigned binary numbers containing fewer "1" bits.

Introduction (3/5)

For example, on page 1 of the detailed explanation of Handycipher (see mtc3_handycipher-6.10_description.pdf, included in the additional zip archive) an example key is given from which is derived the 31-character sub-key

QGC,USNLHAVDOZIBKJWF?P^-XMTYR.E

displayed as the following substitution table:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
10	16	3	12	31	20	2	9	15	18	17	8	26	7	13	22

Q	R	S	T	U	V	W	X	Y	Z	,	.	-	?	^
1	29	6	27	5	11	19	25	28	14	4	30	24	21	23

Introduction (4/5)

Note that with this choice of key the seven most frequently occurring letters in English ^ETOAIN are assigned binary numbers as follows:

^	23	=	10111
E	31	=	11111
T	27	=	11011
O	13	=	01101
A	10	=	01010
I	15	=	01111
N	7	=	00111

Since so many frequently occurring letters are assigned binary numbers containing three, four, or five "1" bits this would be a particularly injudicious choice of key.

Introduction (5/5)

The few successful attacks on the Part 6 and Part 9 challenges over the last three years have all relied on hill-climbing with a goal function of maximizing the number of consecutive colinear characters, and have all required fairly large plaintexts to break the cipher. One of the solvers, George Lasry, has estimated that the cipher would remain secure against his attack for plaintexts less than 500 characters.

http://scienceblogs.de/klausis-krypto-kolumne/2017/06/02/the-handycipher-a-low-tech-encryptionalgorithm-2/

With the Part 10 challenge we propose to test whether the cipher remains secure for plaintexts even as long as 5,000 characters, if the key is chosen strategically.

Challenge

Part 10 of the Handycipher series is a ciphertext-only challenge. A 27,350-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 the plaintext message M.

The solution consists of the **fifth word in every fifth sentence** of M starting with sentence 1 (where sentences are defined as character strings ending in either a period or a question mark followed by a space). Please enter the solution with spaces between the words.

Additional Files

The additional zip archive contains the following files:

- mtc3_handycipher-6.10_description.pdf
  ➥ detailed explanation of Handycipher
- ciphertext_HC-10.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

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 occuring somewhere in the plaintext
HC,	Parts 3, 6, 9 & 10:	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 occuring 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