MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Extended Handycipher – Part 3

Author: Bruce Kallick

March 2015

Introduction

Extended Handycipher (EHC) operates with the same plaintext and ciphertext alphabets as Handycipher (HC), and 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 3 of the Extended Handycipher series is a ciphertext-only challenge. How Extended Handycipher works is described in detail in the extra pdf within the additional zip file.

Your task is to recover some of the 996-character plaintext message M, given the ciphertexts C_a and C_b created by encrypting M with Extended Handycipher and K two times, using two different, randomly generated session keys K'_a and K'_b.
The ciphertexts are given as text files within the additional zip file.

The solution consists of the **first four words** of the **next-to-last** sentence of M. Please enter the solution in capital letters with spaces between the words.

References

The ciphers HC and EHC are explained in detail in the two documents "MTC3_Handycipher_Description.pdf" and "MTC3_Extended-Handycipher_Description.pdf" found within the additional zip file.

Another detailed explanation of the cipher methods HC and EHC can be found at http://eprint.iacr.org/2014/257.pdf

Additional Files

The additional zip archive contains the following files:

- MTC3_Handycipher_Description.pdf
  ➥ detailed explanation of Handycipher
- MTC3_Extended-Handycipher_Description.pdf
  ➥ detailed explanation of Extended Handycipher
- ciphertext_Ca_EHC-03.txt, ciphertext_Cb_EHC-03.txt
  ➥ two complete ciphertexts
- handycipher.zip
  ➥ Python code and test files for HC and EHC.
  Remark: EHC will be used when using the option -x.