MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Spirale – Part 4

Author: Philippe Allard

July 2015

Introduction

Despite our epoch of high technology and the powerfulness of modern personal computers allowing implementation of sophisticated digital ciphers with symmetric or public keys, there is still some effort to produce a modern hand cipher for paper & pencil encryption, too.

Spirale is a OTP cipher designed to be simple to implement by hand, with a high level of variability in keys equivalent to a 128-bit key cryptosystem. Also, the process is resilient to errors as they have only a local effect without obscuring all the ciphertext.

Challenge Description

Part 4 of the Spirale series is a ciphertext-only challenge. How the Spirale cryptosystem works is described in the extra pdf within the additional zip file.
Your task is to recover the 485-letter plaintext out of the given ciphertext. The whole ciphertext is given in a text file also contained in the additional zip file.

As solution, please enter the first four words of the second sentence in capital letters and with spaces.

Hint: Unlike the other three parts, this one uses four new random keys.

Additional Files

The additional zip archive contains the following files:

- MTC3_Spirale_Description.pdf
  ➥ detailed explanation of Spirale
- ciphertext_Spirale-04.txt
  ➥ the complete ciphertext
- spirale.zip
  ➥ Python code and test files for Spirale