MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Spirale – Part 1

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 1 of the Spirale series is a partly-known plaintext challenge. How the Spirale cryptosystem works is described in the extra pdf within the additional zip file.
Your task is to recover the 314-letter plaintext out of the given ciphertext. In addition, the first 75 letters of the plaintext are known. Both, ciphertext and known part of the plaintext are given in text files which are contained in the additional zip file, too.

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

Hint: Part 2 of this series uses the same four keys as this one.

Additional Files

The additional zip archive contains the following files:

- MTC3_Spirale_Description.pdf
  - ➥ detailed explanation of Spirale
- known-plaintext_Spirale-01.txt
  - ➥ the known part of the plaintext
- ciphertext_Spirale-01.txt
  - ➥ the complete ciphertext
- spirale.zip
  - ➥ Python code and test files for Spirale