MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Weakened ElsieFour – Part 3

Author: Anna Lena Rotthaler (using an idea of Pedro Roch)

September 2017

Introduction

ElsieFour (LC4) is a low-tech cipher. It is intended for encrypted communication between humans and can be computed by hand. The alphabet, of which plaintext and ciphertext are built up, consists of 36 characters (the 26 Latin letters plus a few other characters). The key is a random permutation of the characters of the alphabet.

LC4 mixes ideas of modern RC4 stream cipher, historical Playfair cipher, and plaintext-dependent keystreams. LC4 is based on a state that is continually updated as encryption progresses. The state is a permutation of the integers 0 to 35 in a 6x6 matrix.

Challenge

This challenge uses an intentionally weakened version of the LC4 cipher. It is offered only as an exercise meant to explore the extent to which LC4's security depends on the nonce.

Part 3 of the Weakened ElsieFour series is a partly-known plaintext challenge. How ElsieFour works is described in detail in a short description (pdf) within the additional zip file.
Your task is to decrypt ciphertext 2 and to extract the signature. Therefore, you are given the pair plaintext 1 / ciphertext 1, which was encrypted with the same key. Both messages were encrypted without a nonce. What you do not know, is the used key. The signatures 1 and 2 are different.

The solution consists of the **signature** of **plaintext 2**. The signature begins with the # sign (see short description).

References (1/2)

The LC4 cipher is explained in detail in the short description "MTC3_Rotthaler_ElsieFour_Description.pdf". You can find this document within the additional zip file.

The original detailed explanation of the LC4 cipher by Alan Kaminsky can be found at https://eprint.iacr.org/2017/339.pdf

Java source code and examples for LC4 (not weakened LC4) can be found at https://www.cs.rit.edu/~ark/parallelcrypto/elsiefour/

Example call of the Java code under Windows:

```
java -classpath "<path to>pj_20170829.jar;<path to>
    LC4_20170412.jar" LC4Encrypt -v key nonce plaintext
```

References (2/2)

Java source code and examples of the weakened version of LC4 can be found in the additional zip archive.
Example calls can be found in the file "Readme_java.txt".

Python code and examples (also of the weakened version of LC4) can be found in the additional zip archive, too.
Example calls can be found in the file "Readme_python.txt".

Additional Files

The additional zip archive contains the following files:

- MTC3_Rotthaler_ElsieFour_Description.pdf
    - ➥ detailed explanation of LC4
- plaintext_1_WLC4-03.txt
    - ➥ the known plaintext 1
- ciphertext_1_WLC4-03.txt
    - ➥ the complete ciphertext 1
- ciphertext_2_WLC4-03.txt
    - ➥ the complete ciphertext 2
- LC4-code.zip
    - ➥ Java and Python source code and examples

Overview Weakened ElsieFour

- Part 1: partly-known key challenge (the first 12 characters of the key are given)
- Part 2: partly-known key challenge (12 consecutive characters of the key are given)
- Part 3: partly-known plaintext challenge
  (a plaintext/ciphertext pair is given which was encrypted with the same key as the challenge ciphertext)