MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

ASAC – A Strong(er) ADFGVX Cipher – Part 5

Author: Stefan Fendt

May 2016

Introduction (1/2)

Even today it could be useful for short texts to know a strong cipher which is doable by hand. A computer could be compromized without noticing it. Our own head, a pen, and a sheet of paper (for this cipher some more sheets) are unlikely to be compromised unnoticed.

The cipher in this series of challenges consists of three steps: A Polybius square, a pseudorandom number generator ('PRNG') out of a Polybius square, and a double-column transposition.

This series consists of 5 challenges that are based on each other. The first part only involves the Polybius square and serves as introduction, part 2 adds the PRNG, and part 3 uses the complete cipher but substitutes the double-column transposition with a single-column transposition (as in ADFGVX). Part 4 works with the complete ASAC cipher. At last, part 5 is a "bonus challenge" which just modifies the PRNG step in part 2 of the series.

Introduction (2/2)

The goal of the author was to get a cipher that – only just – can be done by hand, ensures a hopefully high degree of security even against computerized attacks and that can be easily remembered and built from memory.
The cipher is similar to ADFGVX, but has three major changes:

1. The Polybius square is a little bit bigger. This allows (by approximation) a compensation for the frequency of single characters.
2. A simple PRNG has been added.
3. Instead of the single-column transposition a double-column transposition is used.

Challenge Description (1/2)

The fifth and last part of the series for ASAC aborts the cipher after the second step as in the second challenge. However, now the pseudorandom sequence of the second step is not simply repeated, but after each 100 digits gets rotated anew.
This means that we repeat the rotation of the rows and columns to get a new pseudorandom sequence with 100 digits. We do this again until we have at least as much pseudorandom digits as the substituted plaintext has.

A description of the complete cipher together with a detailed example can be found in the template of part 1 of this series.

Challenge Description (2/2)

The goal of this challenge (part 5 of the series) is to decrypt the given ciphertext that can be found in the additional text file `mtc3-fendt-05-asac-05-ciphertext.txt`.

As solution, please enter the names mentioned in the plaintext in the order of their appearance in the text in capital letters, parted by commas, and without spaces. This time all names shall be considered, even those mentioned more than once.