MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

ASAC – A Strong(er) ADFGVX Cipher – Part 3

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

The third part of the series for ASAC uses the complete cipher, but substitutes the double-column transposition with a single-column transposition (i.e. in step 3 we need only one key).
A description of the complete cipher together with a detailed example can be found in the template of part 1 of this series.
The goal of this challenge (part 3 of the series) is to decrypt the given ciphertext that can be found in the additional text file `mtc3-fendt-03-asac-03-ciphertext.txt`.

As solution, please enter the 20^{th}, 21^{st}, and 22^{nd} word together in capital letters. As example: Would the words 20 to 22 be 'Hallo du da' you would have to enter the solution this way: HALLODUDA.