MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Double Column Transposition/Granit – Part 3

Author: Joerg Drobick

May 2015

Introduction (1/2)

While nowadays one encrypts almost exclusively by computer systems, in the centuries before the development of IT, simpler methods had to be used. For example, in the 19th and early 20th centuries, the double-column transposition (DTP) was often used. DTP applies a columnar transposition twice.
This method can be done manually, and up-to-now no ciphertext-only attack is known, provided that the method has been parameterized correctly: The two words used as permutation keys are each at least 20 characters long, the plaintext is unknown and the wordlengths are co-prime.
See the challenges "DCT Reloaded":
https://www.mysterytwisterc3.org/en/challenges/level-iii/double-column-transposition-reloaded-part-1

Introduction (2/2)

Among others, the spy Guenter Guillaume used the double-column transposition for his communication with the Ministry of State Security of the former GDR until about 1960.
More precisely, he used an even stronger two-stage method known as GRANIT E160: In the first step the plaintext is converted into a numerical sequence with the help of a codebook and a matrix (a variant of the Polybius square), and in the second step the actual double-column transposition is run.

This challenge series is about that GRANIT method.

Challenge Description (1/2)

Part 3 of this GRANIT series is a ciphertext-only challenge. Your task is to recover the plaintext out of the given ciphertext.

The ciphertext looks like this:

```
81589 81589 93172 10169 83289
11589 17531 00912 78604 68783
79684 60109 68694 91988 74826
45991
```

Hint: All challenges of this series use the very same keyword W for the generation of the key matrix (used in the substitution step): `MEINHAUS`. The empty fields of the first row are also identical.

Challenge Description (2/2)

To obtain the correct plaintext, you will need to undo the double-column transposition and the substitutions (with the help of the matrix). Moreover, possible padding at the end of the text should be removed.

As solution, submit the name of the sender from your putative plaintext in capital letters.

You can find a detailed example in part 1 of this series.

Links

- Website with nearly all codes and encryption mechanisms used in the former GDR – (only German): http://scz.bplaced.net/m.html#dwa

- An interesting thread about double column transposition – (only German): http://www.buha.info/showthread.php?10834-Verfahren-des-Doppelw%FCrfel/page2