MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Weakened Granit – Part 2

Author: Joerg Drobick

August 2015

Introduction (1/2)

Spies always depended on secure communication for not being discovered. For that, transmitted messages had to be encrypted. One of the methods to do that was the so called double-column transposition (DCT). Among others, the spy Guenter Guillaume used the DCT for his communication with the Ministry of State Security of the former GDR until about 1960.
More precisely, he used a 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 DCT is run.

Introduction (2/2)

DCT is a method applying two consecutive columnar transpositions. This method can be done manually, but even today 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 and random, the plaintext is unknown and the two wordlengths are co-prime.

About DCT see the challenges "DCT Reloaded": https://www.mysterytwisterc3.org/en/challenges/level-iii/double-column-transposition-reloaded-part-1

A short description of GRANIT (1/3)

This challenge series serves as exercise in dealing with GRANIT and uses a simplified form, in which at least one of the two grids is known.

You can find a detailed description of GRANIT in the original challenge, on the last page there is a link to said challenge. For a basic understanding we just roughly describe the method here:

a) The plaintext is transformed into a number sequence using a substitution matrix. Before, the plaintext is modified so it only consists of characters which are contained in the substitution matrix.

A short description of GRANIT (2/3)

b) Out of two randomly chosen word sequences each consisting of 5 words, we generate two permutations by numbering the single characters from left to right in the order in which they appear in the alphabet.
Then we generate two rectangular matrices – these are named R_1 and R_2 and consist of as much columns as the permutations are long. The permutations respectively are entered into the upmost row as column headers.
R_1 is for the first, and R_2 for the second column transposition.

A short description of GRANIT (3/3)

c) We enter the number sequence from a) line by line and from the left to the right into R_1. Then we read the numbers column by column with increasing column number (with the numbering from b)) and enter them into R_2. Then we read the numbers column by column according to the order of the column headers and thus obtain the ciphertext.

d) For the final ciphertext we add a key group (German: Kenngruppe) twice in front of the text. This key group is used to obtain the words of the grids R_1 and R_2.

Challenge description (1/2)

Part 2 of this series is a ciphertext-only challenge. Your task is to recover the plaintext from the given ciphertext. The complete ciphertext is given in the extra text file.
Also, the grid R_1 is known. It is generated by the 5 words "*Dabei entbehrt es nicht der*", which corresponds to the numbering "5,1,2,7,14,8,16,21,3,9,12,18,22,10,20,17,15,4,13,23,6,11,19". Part 1 contains a short description on how to get this numbering.

Challenge description (2/2)

To obtain the correct plaintext, you will need to undo the DCT and the substitutions (with the help of the matrix). No codebook is used. Moreover, possible padding at the end of the text should be removed.

As solution, please submit the last four words of the first sentence in capital letters, with spaces, and without special characters.

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 DCT – (only German): http://www.buha.info/showthread.php?10834-Verfahren-des-Doppelw%FCrfel/page2

- Challenge for double-column-transposition/GRANIT with a detailed example (this is the NOT weakened original cipher): https://www.mysterytwisterc3.org/en/challenges/level-ii/double-column-transposition-granit-part-1