INVITED TALK:
SPECIAL SESSION ON ARNE BEURLING

Modern Codebreaking of T52

George Lasry
University of Kassel, Germany

Abstract

The Siemens and Halske T52 is a family of teleprinter encryption systems, used in WWII by the Luftwaffe, the German Navy and Army, and German diplomatic services. Codenamed "Sturgeon" by the Allied, it was designed to provide enhanced security, compared to the other German teleprinter encryption system, the Lorenz SZ42 ("Tunny"). In one of the most impressive feats of cryptographic genius, the first model, the T52a/b, was reconstructed by Arne Beurling only from encrypted traffic. It was also reconstructed at Bletchley Park. Until the end of 1942, Sweden was able to read current T52 traffic that passed through its teleprinter lines, taking advantage of errors by German operators (e.g., messages sent in depth). At the beginning of 1943, Germany increased their security measures, also introducing a new model, the T52d. The T52d was a much more secure system, featuring an irregular movement of the wheels, and a "Klartext" (autokey) function. Sweden could not read its traffic, and a Bletchley Park report from 1944 considers the T52d problem to be "completely hopeless".

The T52 problem (when no depth is available) is still daunting today, even with modern computing. Since WWII, no new methods for the cryptanalysis of the T52 have been published. The machine complexity, and its huge keyspace size, 10^{27}, prohibit any brute-force attack. In this presentation, George will describe how he applied a novel statistical approach, to decipher rare original telegrams from 1942, encrypted using the T52a/b, and found in FRA archives. Also, he will present a first-ever practical attack on the T52d and its successor, the T52e, which takes advantage of a subtle weakness in the design of their stepping mechanism.

Bio

George Lasry specializes in the codebreaking of historical ciphers using modern optimization techniques. He has developed state-of-the-art attacks for a series of challenging cipher machines and systems. In 2013, he deciphered a collection of 600 original ADFGVX ciphertexts from 1918, which provide new insights into key events in the Eastern Front of WWI. In 2017, he also reconstructed German diplomatic and naval codebooks and deciphered hundreds of encoded messages from 1910 to 1915. Also, George has solved several public challenges, including the Double Transposition challenge, Chaocipher Exhibit 6, the M-209 Challenge and the 2015 Enigma Challenge. George Lasry regularly writes about his findings in Cryptologia. The subject of his Ph.D. thesis is the *Cryptanalysis of Classical Ciphers with Search Metaheuristics*.