Wissenschaftliches Zentrum für Informationstechnik-Gestaltung

Angewandte Informations Sicherheit

Research Talk by George Lasry

"Cracking Unsolved Historical Ciphers and Challenges"

October 02, 2015 / 11:00 – 12:00
ITeG (Pfannkuchstr. 1), Room 0420

Abstract: Despite the advent of modern computing technology, several major historical ciphers have not yet been solved. For other types of ciphers and cipher machines, cryptanalysis methods have been published, but only for special or favorable conditions. Over the last few years, George Lasry has been engaged in a research program, together with Prof. Wacker and Nils Kopal from the University of Kassel in Germany, to map unsolved or partially solved ciphers, and apply specialized techniques and algorithms, for their cryptanalysis, and for the solution of related cipher challenges. This research led to some groundbreaking results, including the solution of Klaus Schmeh's Double Transposition (Doppelwürfel) Challenge, the decipherment of 600 original WWI German Army messages, and the solution of other unsolved cipher challenges. This also led to the development of new and improved codebreaking techniques for cipher machines such as the German Enigma and Fish (Lorenz SZ42) systems, and several Hagelin encryption devices. George Lasry will present his findings and some of the methods he used to solve those cipher systems and challenges.

George Lasry is a computer scientist at Google, where he develops machine learning algorithms to detect and prevent malicious online activity. After graduating from the Technion Institute of Technology in Israel, George served as an officer in the SIGINT branch of the Israeli Army, Unit 8200. He later worked for 15 years on the development of communications systems. Prior to joining Google, he managed R&D and Sales organizations in several communications and Internet companies. His primary interest in cryptographic research, in cooperation with a team from the University of Kassel in Germany, is in the application of modern optimization and statistical techniques for the cryptanalysis of challenging historical ciphers. In December 2013, he solved the 2007 Double Transposition challenge, proposed by Otto Leiberich, the former head of the BSI (Germany's Federal Office for Information Security) and ranked by Klaus Schmeh as one of the five top unsolved ciphers.

UNIKASSEL VERSITÄT