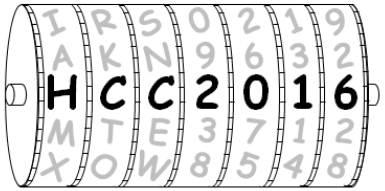
2ND HISTORIC CIPHERS COLLOQUIUM 2016 KASSEL



May 5th 2016, 9:00h-18:00h
Pfannkuchstr. 1

UNIKASSEL VERSITÄT | ELEKTROTECHNIK INFORMATIK

AIS Angewandte Informations Sicherheit

The research group for Applied Information Security invites for the 2nd colloquium on historical ciphers.

The colloquium will cover modern computerized cryptanalysis of classical ciphers and algorithms as well as their historical background.

Description

The colloquium's subject will be the analysis of historical ciphers and cryptographic algorithms and machines with the help of modern computerized methods as well as the historical backgrounds. The reasons for analyzing and attacking classical ciphers are manifold: First, developing heuristic approaches for cryptanalysis helps cryptanalysts and researchers to get a better understanding of the classical cipher as well as a deeper insight into the used heuristics, i.e. hillclimbing, simulated annealing, genetic algorithms, tabu search, etc. Second, it helps other researchers, like historians, to decipher encrypted historical messages. That, in turn helps to get new knowledge of previously unknown historical events.

The Talks

Our first speaker is **Mr. George Lasry**. He is a computer scientist in the high-tech industry in Israel and a PhD student with the research group "Applied Information Security" (AIS) at the University of Kassel. Prior to this, he worked for many years on the development of communications systems, and also managed R&D and sales organizations. His primary interest in cryptographic research is the application of specialized optimization techniques for the computerized cryptanalysis of classical ciphers. Using such a technique, he solved in November 2013 the Double Transposition (Doppelwürfel) cipher challenge which was published by Klaus Schmeh in 2007. George Lasry will give a talk about the deciphering of ADFGVX messages of the "forgotten" Eastern Front of WW1.

Our second speaker is **Dr. Ingo Niebel**. He is a historian and freelance journalist living and working in Germany. He received his PhD from the University of Cologne in 2012. Since 1996, he is also a member of Eusko Ikaskuntza, the Society of Basque Studies. He has published several books in German and Spanish about the Basque Country and intelligence during the Spanish Civil War (1936–1939). During his research he uncovered Civil War original telegrams encrypted using the Spanish Strip Cipher, which could not be read as the encryption keys had been lost. He was part of a team led by Professor Christof Paar, who has the Chair for Embedded Security at Ruhr University Bochum, Germany. The team successfully decrypted those historical messages. He, furthermore, worked together with Mr. Lasry on the ADFGVX messages. In his talk, he will give an overview of the historical content and relevance of those messages.

Our third speaker is **Mr. Klaus Schmeh**. He is one of the world's leading experts on historical ciphers. His books "Nicht zu knacken" (the ten biggest unsolved mysteries of encryption) and "Codeknacker gegen Codemacher" (about the history of encryption technologies) are standard books. In his blog "Klausis Krypto Kulumne" he writes about his favorite topic. In his talk, he will give an overview about "encryption and crimes". He will present if backdoors actually help law enforcement to catch bad guys.

Our fourth Speaker is **Prof. Dr. Nicolas Courtois**. He is author of more than 100 papers in cryptography. One of his specialties is cryptanalysis with particular attention paid to operational software algebraic attacks and focus on realistic attack scenarios with low quantities of data available to the attacker. He is author of numerous attacks on systems used by millions of people every day: MiFare Classic, stream cipher E0 in Bluetooth encryption, DES, AES, GOST, etc. For a very long time and until today numerous ciphers have been built from compositions of permutations. In his talk he will survey some basic principles of cryptanalysis in this setting. The concepts of SAT/UNSAT immunity, fixed point attacks, slide attacks, involution attacks, cycle structure attacks, permutation factoring, amplification, cycle structure attacks, reflections etc. These principles and methods have been with us since 1920s and we still see them on a regular basis in cipher cryptanalysis.

Agenda

09:00 – 10:00	Welcome/Arrival *Room 0420*
10:00 – 10:15	Opening *Room 0420*
10:15 – 11:00	Breaking ADFGVX Messages *Room 0420* *Talk by George Lasry*
11:00 – 11:45	Historical Background ADFGVX Eastern Front *Room 0420* *Talk by Ingo Niebel*
11:45 – 12:45	Lunch Break *Room 0420*
12:45 – 13:30	Cryptography and Crime *Room 0420* *Talk by Klaus Schmeh*
13:30 – 14:15	100 years of Cryptanalysis: Compositions of Permutations *Room 0420* *Talk by Nicolas T. Courtois*
14:15 – 14:30	*Coffee Break*
14:30 – 15:30	Short Talks *Room 0420*
15:30 – 17:30	Open - Discussion and/or further talks
17:30- 18:00	Future of HCC (Persisting the event?)

Organization

Date: 5th of May, 2016
Time: 9:00h-18:00h

Address:

University of Kassel
Applied Information Security

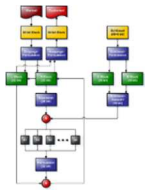
Pfannkuchstr. 1
34121 Kassel

Registration:

Lunch and coffee will be provided for free. No participation fee. However, for planning reasons we need to know the amount of participants (for lunch, coffee, etc.).For registration please write an email to Mr. Nils Kopal (nils.kopal@uni-kassel.de).

Host:

The host of the "2ND HISTORIC CIPHERS COLLOQUIUM 2016 (HCC2016) KASSEL" is the research group "Applied Information Security" of the University of Kassel.



Contact:

Prof. Dr. Arno Wacker

Nils Kopal, M.Sc.

Universität Kassel
Fachbereich 16 Elektrotechnik/Informatik
Fachgebiet Angewandte Informationssicherheit

Pfannkuchstr. 1
34121 Kassel

Tel: +49 (561) 804 6644
Fax: +49 (561) 804 6643
E-Mail: arno.wacker@uni-kassel.de
nils.kopal@uni-kassel.de

Web: http://www.ais.uni-kassel.de