

HistoCrypt 2018

1st International Conference on
Historical Cryptology

Conference Program

June 18-20, 2018
Uppsala University
Uppsala, Sweden

Information

Venue

Welcome to *Humanistiska teatern*, inspired by an anatomic theater from the 17th century, on the English Park Campus of Uppsala University, Uppsala, Sweden.



Registration

You can register either at the welcome reception or during the conference days in the lobby of the main venue. The registration desk is open:

June 17: 18:00-21:00 at the Linnaeus Garden

June 18: 08:30-18:00 outside the main hall

June 19: 08:30-10:00 outside the main hall

Lunch and coffee

Lunches are served in room 2-0031 close to the main hall. Coffee is served in the lobby outside the main hall.

Welcome Reception June 17, 2018 18:00-21:00

The welcome reception is held at the beautiful Linnaeus Garden¹ with a guided tour of the Linnaeus Museum², which is located inside the garden. A buffet is served.

Street address: Svartbäcksgatan 27, Uppsala

Conference Dinner June 18, 2018 18:30-23:59

Norrlands nation³, Uppsala's largest student nation.

Street address: Västra Ågatan 14, Uppsala

Dresscode: casual

Conference Dinner June 19, 2018 19:00-23:59

Borgen, located by the Fyris River.

Street address: Orphei Drängars plats 1, Uppsala

Dresscode: casual

¹ <http://www.destinationuppsala.se/en/To-do/ToDo/?tlang=en&tid=788870>

² <http://www.destinationuppsala.se/en/To-do/ToDo/?tlang=en&tid=719635>

³ <http://www.norrlandsnation.se/organization/>

CONFERENCE PROGRAM

Sunday, June 17, 2018

Welcome Reception 18:00-21:00 at the Linnaeus Garden⁴, Sweden's oldest botanic garden.

Monday, June 18, 2018 MAIN CONFERENCE

Location: Main Hall

09:00 – 09:30 **Opening**

Arno Wacker Chair of the Steering Committee
Beáta Megyesi Chair of the Program Committee
Eva Pettersson Chair of the Local Organizing Committee

09:30 – 10:15 **Keynote**

Chair: Beáta Megyesi

Craig Bauer

Updates on the World's Greatest Unsolved Ciphers

10:15-11:00 **Historical Ciphers/Codes**

Chair: Gerhard Strasser

Ekaterina Domnina

Nicodemo Tranchellini's Diplomatic Cipher: New Evidence

Camille Desenclos.

Unsealing the Secret: Rebuilding the Renaissance French Cryptographic Sources (1530-1630)

11:00-11:30 Coffee Break

11:30-12:30 **Cryptanalysis of Classical Algorithms**

Chair: Anne-Simone Rous

Juan José Cabezas, Joachim von zur Gathen, and Jorge Tiscornia
Uruguayan Cryptographic Carpet

Nils Kopal

Solving Classical Ciphers with CrypTool 2

Mark Stamp, Fabio Di Troia, Miles Stamp and Jasper Huang

Hidden Markov Models for Vigenère Cryptanalysis

⁴ <http://www.botan.uu.se/our-gardens/the-linnaeus-garden/visit-the-garden/>

12:30-13:30 Lunch

13.30-14.15 **Keynote**

Chair: Bernhard Esslinger

David Naccache and Rémi Géraud

A French Code from the Late 19th Century

14:15-14:45 Coffee break

14:45-16.15 **World War I**

Chair: Marek Grajek

Karl de Leeuw

The Solving of a Fleissner Grille during an Exercise by the Royal Netherlands Army in 1913

George Lasry

Deciphering German Diplomatic and Naval Attaché Messages from 1914-1915

Ingo Niebel

Learning Cryptanalysis the Hard Way: A Study on German Culture of Cryptology in World War I

Paolo Bonavoglia

New Findings in a WWI Notebook of Luigi Sacco

16:15-16:45 Coffee break

16:45-17.30 **Keynote**

Chair: Benedek Láng

Katherine Ellison

Cryptology and the Fantasy of Reading

18:30-00:00 Conference Dinner at Norrlands Nation⁵

⁵ <http://www.norrlandsnation.se/>

Tuesday, June 19, 2018 MAIN CONFERENCE

Location: Main Hall

09:00-09:45 **Keynote**

Chair: Otokar Grošek

Ephraim Lapid
The Israeli Enigma

09:45-10:15 Coffee break

10:15-12:00 **World War II**

Chair: Karl de Leeuw

Anders Wik
The First Classical Enigmas. Swedish Views on Enigma Development 1924-1930

Marek Grajek
An Inventory of Early Inter-Allied Enigma Cooperation

Dermot Turing
The Poles and Enigma after 1940: le voile se lève-t-il?

Magnus Ekhall and Fredrik Hallenberg
US Navy Cryptanalytic Bombe – A Theory of Operation and Computer Simulation

Carola Dahlke
What We Know about Cipher Device "Schlüsselgerät SG-41" so far

12:00-13:00 Lunch

13:00–15:00 **Business meeting**

15:00-15.30 Coffee break

15:30-16:30 **Keynote: Special Session on Arne Beurling**

Chair: Anders H. Wik

Kjell-Ove Widman
Arne Beurling: Mathematician and Code Breaker

George Lasry
Modern codebreaking of T52

16:30-18:00

Poster and demo session with exhibition and coffee

Location: Room 2-0031 and the lobby outside the main hall

Posters

Noor R. Al-Kazaz, Sean A. Irvine and William J. Teahan

An Automatic Cryptanalysis of Playfair Ciphers Using Compression

Niels O. Faurholt

Willard's System

Anna Lehofer

The Application of Hierarchical Clustering to Homophonic Ciphers

Michal Musílek and Štěpán Hubálovský

Teaching and Promoting Cryptology at Faculty of Science University of Hradec Králové

Klaus Schmeh

Examining the Dorabella Cipher with Three Lesser-Known Cryptanalysis Methods

Jaap van Tuyl

Design and Strength of a Feasible Electronic Ciphemachine from the 1970s

Demos

Eugen Antal and Pavol Zajac

ManuLab System Demonstration

Magnus Ekhall and Fredrik Hallenberg

US Navy Cryptanalytic Bombe - A Theory of Operation and Computer Simulation

Nils Kopal

Solving Classical Ciphers with CrypTool 2

Extra demo by the organizers: Beáta Megyesi, Nils Blomqvist and Eva Pettersson

The DECODE database

Exhibition by FRA⁶: Anders H. Wik and Åsa Ljungqvist

Enigma machines

18:00-18:15

Closing

Location: Main Hall

19:00-00:00

Conference Dinner at Restaurant Borgen⁷

⁶ <http://www.fra.se/snabblankar/english.10.html>

⁷ <https://www.borgenuppsala.se/>

Wednesday, June 20, 2018 WORKSHOPS

09:00-12:00 (Automated) Cryptanalysis of Classical Ciphers with CrypTool 2

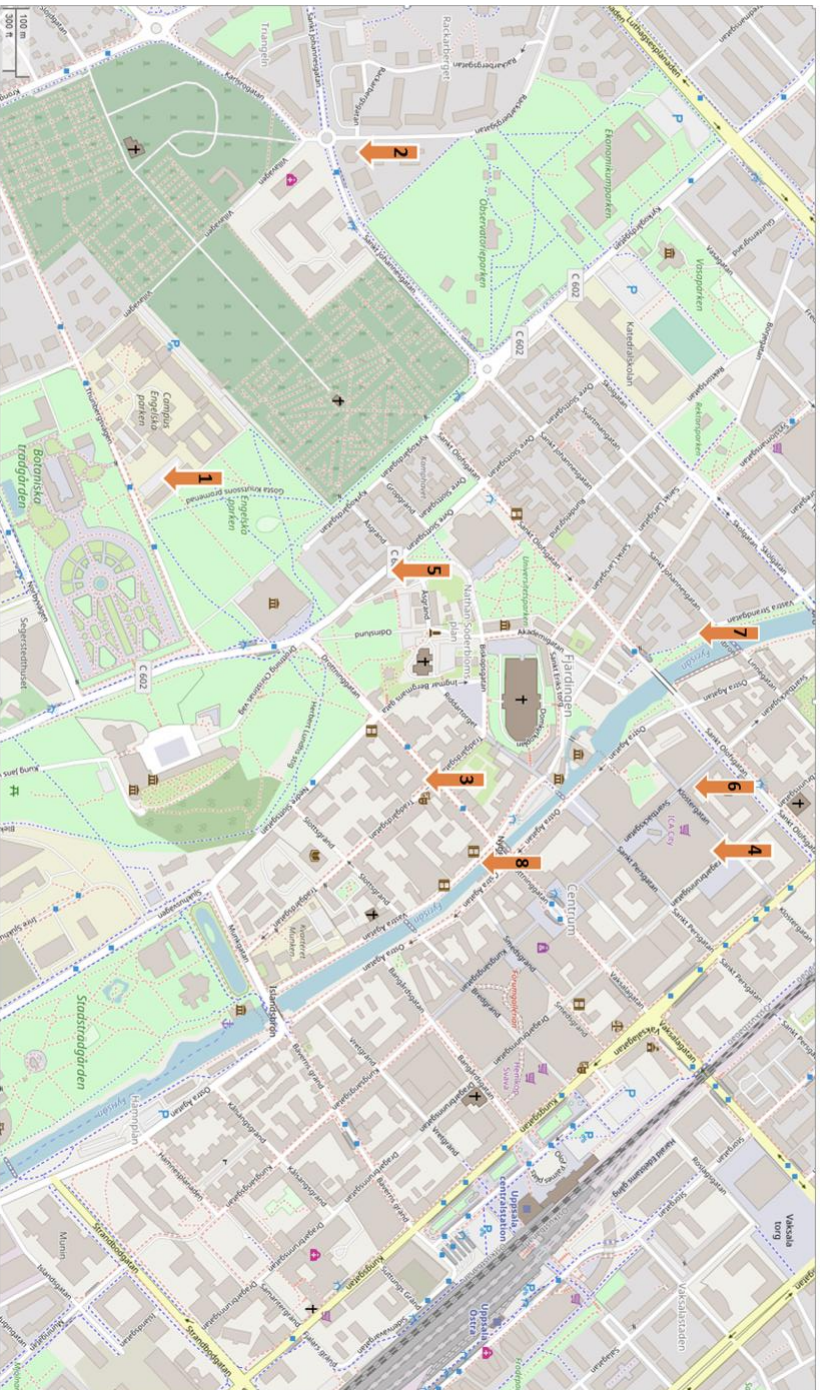
Workshop organizers: Nils Kopal, Armin Krauss, Bernhard Esslinger
Location: Room 22-1017

12:00-13:00 Lunch

13:00-17:00 Solving Codes rather than Ciphers. Is there a Software Challenge?

Workshop organizer: Karl de Leeuw
Location: Room 22-1017

Map: Venue, Hotels and Social Events



1. Humanistiska teatern
2. Hotell Stella
3. CityStay
4. Clarion Hotel Gillet
5. Akademihotellet
6. Linnéträdgården
7. Restaurang borgen
8. Norrlands nation