HISTOCRYPT 2019 CONFERENCE PROGRAM

Version: 2019-05-30

June 23-26, 2019, Mundaneum, Mons. Belgium

Sunday, June 23, 2019

18:00 Welcome Reception

21:00 End

Monday, June 24, MAIN CONFERENCE

08:30 Registration

09:00 Opening

Arno Wacker – Chair of the Steering Committee

Klaus Schmeh – Chair of the Program Committee

Jean-Jacques Quisquater – Chair of the Local Organizing Committee

09:30 Invited Speech 1

Marc McMenamin: Codebreaker Richard Hayes

10:00 Session 1

1. Gerhard Strasser: Johann J. H. Bücking (1749-1838) – Medical Doctor, Inventor, and Cryptologist
2. Paolo Bonavoglia: Hieronimo di Franceschi and Pietro Partenio, two unknown Venetian cryptologists
3. Florent Dewez, Valentin Montmirail: Decrypting the Hill Cipher via a Restricted Search Over the Text-Space

11:00 Coffee Break

11:30 Session 2

4. Eugen Antal, Pavol Zajac and Otokar Grošek: Cryptology in the Slovak State During WWII
5. Dermot Turing: The Typex Scare of 1943
6. George Lasry: A Practical Meet-in-the-Middle Attack on SIGABA

12:30 Lunch

13.30 Invited Speech 2

Bart Preneel: Lumumba; or Breaking 1961 Hagelin Ciphertexts

14:00 Session 3

7. Jerry McCarthy: Recreating the Polish Bomba, Predecessor to the Turing-Welchman Bombe
8. Carola Dahlke: From Antiquity to Post-Quantum Cryptography: A New Gallery on Cryptology at the Deutsches Museum, Munich

14:45 Invited Speech 3

Bernard Fabrot: Breaking LCS35

15:15 Coffee break

15:45 Session 4

9. Benedek Láng: Dead ends in breaking an unknown cipher: experiences in the historiography of the Rohonc Codex
10. Juan José Cabezas, Francisco Castro, Joachim von zur Gathen, Jorge Tiscornia and Alfredo Viola: Uruguayan cryptography: printed book covers
11. Beáta Megyesi, Nils Blomqvist and Eva Pettersson: The DECODE Database – Collection of Historical Ciphers and Keys
12. Peter Krapp: Beyond Shlock on Screen: Teaching the History of Cryptology through Media Representations

17:15 End

18:30 Conference Dinner

Tuesday, June 25, MAIN CONFERENCE

8:30 Registration

09:00 Session 4

13. George Lasry: Solving a 40-Letter Playfair Challenge with CrypTool 2
14. Klaus Schmeh, Tony Gaffney: Cryptanalysis of an Early 20th Century Encrypted Journal
15. Nils Kopal: Cryptanalysis of Homophonic Substitution Ciphers Using Simulated Annealing with Fixed Temperature – A Work-in-Progress Paper

10:00 Invited Speech 4

Vincent Rijmen, Joan Daemen: The History of AES

10:30 Coffee break

11:00 Session 5

16. Tom S Juzek: Using the entropy of n-grams to evaluate the authenticity of substitution ciphers and z340 in particular
17. Monir Azraoui, Solenn Brunet, Sébastien Canard, Aïda Diop, Lélia Eveillard, Alicia Filipiak, Adel Hamdi, Flavie Misarsky, Donald Nokam Kuate, Marie Paindavoine, Quentin Santos and Bastien Vialla: CYBERCRYPT: Learn Basic Cryptographic Concepts while Playing
18. Giuseppe Bianchi: Voynich, Hardware and Software

12:00 Invited Speech 5

René Zandbergen: No news about the Voynich MS?

12:30 Lunch

13:15 Business meeting

15:15 Invited Speech 6

Ingo Niebel: The German Crypto-Crisis of 1917 - How the Zimmermann telegram completed the genesis of German cryptology

15:45 Poster and demo session with exhibition and coffee

Nils Kopal, Tobias Schrödel: Crypto Books

Mauran Philippe: Cyphers and shadow diplomacy in England during 17th Century: Prince of Condé looking for support

16:45 Closing

17:00 End

17:15 Guided Tour Mundaneum

19:00 Free Evening in Mons

Wednesday, June 26, WORKSHOPS

09:00 Workshop 1

Breaking Homophonic Substitution Ciphers with CrypTool 2

Lunch: 12:00

12:30 End