Preface

We are very pleased to present the proceedings of the 4th International Conference on Historical Cryptology, HISTOCRYPT 2021. Due to the COVID-19 pandemic, the respective conference has been postponed to June 20-22, 2022 in Amsterdam, the Netherlands. This means that all accepted papers and posters from 2021 will be presented together with the next year's contributions in Amsterdam in 2022.

HISTOCRYPT addresses all aspects of historical cryptography and cryptanalysis including work in closely related disciplines, such as history, history of ideas, computer science, artificial intelligence, computational linguistics, linguistics, or image processing with relevance to historical cipher-texts and codes. The conference's subjects include, but are not limited to the use of cryptography in military, diplomacy, business, and other areas, the analysis of historical ciphers with the help of modern computerized methods, unsolved historical cryptograms, the Enigma and other encryption machines, the history of modern (computer-based) cryptography, special linguistic aspects of cryptology, the influence of cryptography on the course of history as well as teaching and promoting cryptology in schools, universities, and the public.

The program committee welcomed submissions in two distinct tracks: *regular papers* on substantial, original, and unpublished research, including evaluation results, where appropriate, and *short papers* on smaller, focused contributions, work in progress, negative results, surveys, tutorials, or opinion pieces. The conference received 24 submissions from all over Europe including Austria, the Republic of Cyprus, the Czech Republic, Germany, Hungary, Italy, the Netherlands, Poland, Slovakia, Spain, Sweden and the U.K. as well as from Australia, Canada, Israel and the United States. Following the previous events, the primary goal of the program committee was to deliver a high quality program with a wide variety of topics by performing a double-blind review process. At least, three experts in the corresponding field evaluated each submission, and gave their recommendations to accept or decline. The reviews were synchronized and if ambiguous, were thoroughly discussed among the reviewers and the senior members of the PC, who made the final selection based on the recommendations and discussions. Finally, we rejected six papers and accepted 75% of the submissions, of which twelve papers were submitted as long and four were submitted as short papers. All accepted submissions are collected in this volume in alphabetical order after the last name of the first author.

Since the conference has been postponed, we do of course hope to be able to carry out a large part of our previously planned program in 2022. Nevertheless, we would like to take this opportunity to thank the invited keynote speakers who kindly accepted our invitation to speak at the conference this year: *Tanja Lange*, professor of Mathematics and expert in modern cryptography and leader of a European post-quantum project, *Maarten Oberman*, cryptologist specialized on Cold War cryptology and the Dutch cipher machine *ECOLEX*, *David Oranchak, Sam Blake, Jarl van Eycke* who solved *the Z-340 Zodiac Killer's Cipher*, *Paul Reuvers*, engineer, Hagelin expert, crypto collector and curator of *Crypto Museum* and *Gerhard F. Strasser*, professor emeritus of German and Comparative Literature, The Pennsylvania University.

Organizing a conference and a peer-review process always relies on the goodwill of many colleagues who take their valuable time to contribute to an interesting and

fruitful program. First of all, I would like to thank Karl de Leeuw for the great collaboration, and my special thanks go to Beáta Megyesi and Karl de Leeuw for your help in publishing these proceedings. Furthermore, I want to thank all senior members of the program committee, Bernhard Esslinger, Benedek Láng, George Lasry, Karl de Leeuw, Beáta Megyesi, and Dermot Turing for your both active and mental support, for our spontaneous meetings and wise decisions on difficult issues. I am glad that I can rely on you for another HistoCrypt period. As well, I want to thank the 28 members of our extended Program Committee for your time and effort to give constructive and collegial feedback to help in the review process and selection of papers. In addition, I would like to thank all the authors for making these proceedings again interesting, diverse and impressive. Furthermore, many thanks go to the Local Committee under Karl de Leeuw's leadership for the organisation in Amsterdam so far, even though it was unfortunately not feasible this year, to Arno Wacker and Christoph Ruhl for helping out with the conference website, and to the Steering Committee.

As the physical conference has been postponed to June 20-22, 2022 in Amsterdam, Netherlands, we are planning a half-day online event this year on 20 September 2021, which will feature an exciting small program with a keynote, an online workshop, time for administrative information about HISTOCRYPT and, most importantly, the opportunity to share and network together. The complete program, and the respective registration information, is available on the HISTOCRYPT homepage www.histocrypt.org. Hopefully, we will finally meet again for real in 2022. Until then, I wish you all the best, good health, and enjoyment of this year's HISTOCRYPT publications.

Carola Dahlke
Program Chair of HISTOCRYPT 2021

Program Committee

- Carola Dahlke (program chair), Deutsches Museum, Germany
- Bernhard Esslinger, University of Siegen, Germany
- Benedek Láng, Budapest University of Technology and Economics, Hungary
- George Lasry, The CrypTool Team, Germany
- Karl de Leeuw, University of Amsterdam, Netherlands
- Beáta Megyesi, Uppsala University, Sweden
- Dermot Turing, Kellogg College, Oxford, UK

Local Organizing Committee

- Karl de Leeuw (general chair)
- Jan Bergstra
- Matthijs Koot
- Paul Reuvers
- Jaap van Tuyll

Steering Committee

- Joachim von zur Gathen, Emeritus, Bonn-Aachen International Center for Information Technology, Germany
- Marek Grajek, Poland
- Klaus Schmeh, Private researcher, Germany
- Arno Wacker, Bundeswehr University Munich, Germany

Extended Program Committee: Reviewers

- Eugen Antal, Slovak University of Technology in Bratislava, Slovakia
- Paolo Bonavoglia, Mathesis Venezia, Italy
- Nicolas Courtois, University College London, U.K.
- Camille Desenclos, Centre d'Histoire des Sociétés, des Sciences et des Conflits, Université de Picardie Jules Verne, France

- Ekaterina Domnina, Moscow State Lomonosov University, Russia
- John Dooley, Knox College, U.S.A.
- Joseph Fitsanakis, Coastal Carolina University, U.S.A.
- Otokar Grošek, Slovak University of Technology in Bratislava, Slovakia
- Emrah Safa Gurkan, Istanbul 29 Mayis University, Turkey
- Julio Hernandez-Castro, School of Computing, University of Kent, U.K.
- Kevin Knight, DiDi Labs, USA
- Grzegorz Kondrak, University of Alberta, Canada
- Nils Kopal, University of Siegen, Germany
- Jakub Mírka, The State Regional Archives in Pilsen, Czech Republic
- Valerie Nachef, UCY Cergy Paris Université, France
- Diego Navarro, Carlos III University of Madrid, Spain
- Ingo Niebel, Historian and Journalist, Germany
- Marie-Louise Rodén, Kristianstad University, Sweden
- Klaus Schmeh, Cryptovision, Germany
- Betsy Rohaly Smoot, Independent scholar, U.S.A.
- Gerhard F. Strasser, The Pennsylvania State University, U.S.A.
- Jörg Ulbert, Université Bretagne Sud, France
- Serge Vaudenay, Ecole Polytechnique Fédérale de Lausanne, Switzerland
- Arno Wacker, Bundeswehr University of Munich, Germany
- Michelle Waldispühl, Göteborg University, Institute for språk och litteraturer, Sweden

Extended Program Committee: Subreviewers

- Colin Choi, University of Alberta, Canada
- Bradley Hauer, University of Alberta, Canada
- Abram Hindle, University of Alberta, Canada