Preface

We are very pleased to introduce the proceedings of the 3rd International Conference on Historical Cryptology, HISTOCRYPT 2020. The conference would have taken place in Budapest, Hungary, between June 15 and 17, 2020 but due to the COVID-19 crisis with closed boarders, travel restrictions and physical distancing, the actual meeting of HISTOCRYPT had to be canceled.

Just as in previous years, HISTOCRYPT 2020 addresses all aspects of historical cryptology/cryptography including work in closely related disciplines (such as history, history of ideas, computer science, AI, computational linguistics, linguistics, or image processing) with relevance to historical ciphertexts and codes. The subjects of the conference include, but are not limited to the use of cryptography in military, diplomacy, business, and other areas, 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, linguistic aspects of cryptology, the influence of cryptography on the course of history, or teaching and promoting cryptology in schools, universities, and the public.

The scientific program was carefully planned by an international scientific program committee, consisting of researchers in cryptology, history, intelligence and language technology. The program committee welcomed submissions in three distinct tracks: *regular papers* on substantial, original, and unpublished research, including evaluation results, where appropriate; *short papers* on smaller, focused contributions, work in progress, negative results, surveys, or opinion pieces; and *system demos and artifacts* presented as short papers.

The conference received 20 submissions from all over Europe including the Czech republic, France, Germany, Hungary, Italy, Poland, Slovakia, Spain, Sweden, and the UK as well as from Australia, Israel and the United States.

Following the previous events, our primary goal in the program committee was to deliver a high quality program with a wide variety of topics. We applied a double-blind review process and all papers were reviewed by at least three experts in the field. To synchronise recommendations among the reviewers, the senior members of the PC lead the discussion among reviewers on the submissions. The final selection of the papers was made by the senior members of the program committee. We rejected three papers and accepted 85% of the submissions, of which thirteen 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.

Originally, we also planned for four invited keynote speakers who kindly accepted our invitation: *David Kenyon*, research historian at Bletchley Park and Associate Lecturer in History at Brunel University, and author of the recently published *Bletchley Park and D-Day*; *Liza Mundy*, well-known journalist and author of the *Code Girls: The Untold Story of the American Women Code Breakers of World War II* in the United

States; *Paul Zimmermann*, researcher at Inria, the French National Institute for Research in Digital Science and Technology in Nancy, France, focusing on integer factorization, and *Gerhard F. Strasser*, professor emeritus of German and Comparative Literature at the Pennsylvania State University. After a special invitation from the program committee, we are happy to present Gerhard F. Strasser's work on *Encoded Communication with Ladies in a Turkish Harem, 17th-Century Style* as the first article in the proceedings.

Lastly, the conference program would have included a workshop about the well-known Rohonc Codex, which is located in Budapest. The workshop was planned by Levente Zoltán Király and Gábor Tokai, who are working on the decipherment of this mysterious manuscript from the 15th century. We hope that they will be given the chance to organize the event in connection to another HISTOCRYPT meeting in the near future.

Organizing a conference relies on the goodwill of many researchers involved in various scientific areas who take their valuable time to contribute to an interesting and fruitful conference. I am very grateful to all senior members of the program committee for their wise advice and work, and the 23 reviewers for their time and effort to give constructive and collegial feedback to help in the selection of papers. All authors without whom these proceedings would not have seen light receive hereby a huge thanks.

Even though we did not get the chance to organize a physical meeting, my greatest debt goes to the local organization, Benedek Láng and Anna Lehofer, whom I always enjoy working with, for carrying the burden of the local organization — it is very sad that we had to cancel the conference when almost everything was in place...

I hope to meet you all at the next HISTOCRYPT in 2021 and I wish you all a joyful time while reading the papers in this volume!

Beáta Megyesi
Program Chair for the HISTOCRYPT 2020 team

Program Committee

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

Local Organizing Committee

- Benedek Láng (Local Chair), Budapest University of Technology and Economics, Hungary
- Anna Lehofer, Budapest University of Technology and Economics, Hungary

Steering Committee

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

Extended Program Committee: Reviewers

- Eugen Antal, Slovak University of Technology in Bratislava, Slovakia
- Paolo Bonavoglia, Mathesis Venezia, Italy
- Nicolas Courtois, University College London, UK
- Camille Desenclos, Université de Haute-Alsace, France
- Joachim von zur Gathen, Emeritus, Bonn-Aachen International Center for Information Technology, Germany
- Pascal Junod, Snap, Switzerland
- Otokar Grošek, Slovak University of Technology in Bratislava, Slovakia

- Bradley Hauer, University of Alberta, Canada
- Julio Hernandez-Castro, School of Computing, University of Kent, UK
- Kevin Knight, DiDi Labs, USA
- Jozef, Kollár, Slovak University of Technology in Bratislava, Slovakia
- Grzegorz Kondrak, University of Alberta, Canada
- Nils Kopal, University of Siegen, Germany
- Karl de Leeuw, University of Amsterdam, Netherlands
- Sjouke Mauw, University of Luxembourg, Luxembourg
- Michal Musilek, University of Hradec Kralove, Czech Republic
- Valerie Nachef, UCY Cergy Paris Université, France
- Diego Navarro, Carlos III University of Madrid, Spain
- Jacques Patarin, Université de Versailles-Saint-Quentin-en-Yvelines, France
- Klaus Schmeh, Cryptovision, Germany
- Serge Vaudenay, Ecole Polytechnique Fédérale de Lausanne, Switzerland
- Arno Wacker, Bundeswehr University of Munich, Germany
- Pavol Zajac, Slovak University of Technology in Bratislava, Slovakia