

Preface

The program committee is delighted to present the proceedings of the 8th International Conference on Historical Cryptology (HISTOCRYPT 2025). The conference will be held on June 16-18, 2025 in Poznań, Poland.

Following the tradition of previous HISTOCRYPT conferences, HISTOCRYPT addresses all aspects of historical cryptography and cryptanalysis. It is inherently cross-disciplinary, incorporating work from various fields such as mathematics, history, computer science, AI, computational linguistics, linguistics, and image processing. The conference's topics include, but are not limited to, the use of cryptography in military, diplomacy, business, and other areas, the use of automatic methods including AI in the field of historical cryptology, unsolved historical cryptograms, cipher machines, the history of cryptography, the roots of modern ciphers in historical cryptology, linguistic aspects of cryptology, the influence of cryptography on the course of history, cryptology and its connections to neighbouring fields of study, and teaching and promoting cryptology in schools, universities, and the public.

The scientific program was compiled by an international scientific program committee, consisting of researchers in computer science, cryptology, history, intelligence, language technology, and linguistics. The program committee welcomed submissions in two tracks: regular papers up to 10 pages (including appendices, excluding references) on substantial, original, and unpublished research, including evaluation results, where appropriate; and short papers up to 4 pages (including appendices, excluding references) on smaller, focused contributions, work in progress, negative results, surveys, tutorials, or opinion pieces.

The conference received 24 submissions from all over the world, including from Albania, Australia, Austria, Belgium, Canada, Czechia, France, Germany, Ghana, Hungary, Indonesia, Israel, Italy, Japan, Netherlands, Norway, Slovakia, Spain, Sweden, Switzerland, United Kingdom, United States.

The program committee aimed to compile a high-quality program with a wide variety of topics by conducting a double-blind review process. Each submission was evaluated by at least three expert reviewers in the corresponding field. The reviews were synchronized and, if necessary, thoroughly discussed among the reviewers and area chairs of the program committee. The final selection was based on their recommendations and discussions. In the end, we accepted 15 regular papers and 4 short papers for publication, resulting in a total of 19 papers (79% acceptance rate). One accepted paper was later withdrawn by the author. The remaining 18 accepted submissions are included in this volume, organized alphabetically by the surname of the first author.

For the conference in Poznań, we have invited three keynote speakers who have graciously accepted our invitation. They are:

- *François Desset*,
European archaeologist and philologist specializing in Ancient Near Eastern history, Université de Liège/Tehran University/ArchéOrient, he led the decipherment of Linear Elamite writing, an ancient script used in southern Iran between the late 3rd and early 2nd millennium BCE;

- *Marek Grajek*, freelance researcher, he is a retired consultant in cryptology applications and a historian of the discipline, he is the author of more than a dozen books in this field;
- *Kevin Knight*, chief scientist, Threeven Labs, he has co-authored over 150 research papers on natural language processing, as well as the widely adopted textbook “Artificial Intelligence”.

Organizing a conference and a peer-review process always relies on the goodwill and support of many colleagues to take their valuable time and contribute to an interesting and fruitful program. First of all, I would like to thank the local organizing committee: *Piotr Bojarski* and *Marcin Stomiński* for the great collaboration and the great conference location, and for managing the ticketing system. My special thanks goes to all area chairs of the program committee: *Carola Dahlke*, *Benedek Láng*, *Beáta Megyesi*, and *Michelle Waldispühl* for their substantial support and for many constructive online-meetings. I also want to thank the 23 reviewers for their time, effort, and constructive feedback during the review process. In addition, I would like to thank all the authors who have made these proceedings possible. Lastly, I would like to express my gratitude to Arno Wacker and Christoph Ruhl for managing the conference website.

Bratislava, May 8, 2025

Eugen Antal
Program Chair of HISTOCRYPT 2025

Program Committee

- Eugen Antal (program chair), Slovak University of Technology in Bratislava, Slovakia
- Carola Dahlke (area chair), Deutsches Museum, Germany
- Benedek Láng (area chair), Budapest University of Technology and Economics, Hungary
- Beáta Megyesi (area chair), Stockholm University, Sweden
- Michelle Waldspühl (area chair), University of Oslo, Norway
- Richard Bean, University of Queensland, Australia
- Paolo Bonavoglia, Mathesis Venezia c/o Convitto “Marco Foscarini”, Italy
- Camille Desenclos, Université de Picardie Jule Verne, France
- Jörgen Dinnissen, Independent researcher, The Netherlands
- John Dooley, Knox College, United States
- Magnus Ekhall, Private Researcher, Sweden
- Joachim von zur Gathen, Bonn-Aachen International Center for Information Technology, Germany
- Otokar Grošek, Slovak University of Technology in Bratislava, Slovakia
- Kevin Knight, Threeven Labs, United States
- Jozef Kollár, Slovak University of Technology in Bratislava, Slovakia
- Nils Kopal, University of Siegen, Germany
- George Lasry, DECRYPT and CrypTool projects, Germany
- Jakub Mírka, The State Regional Archives in Pilsen, Czechia
- Diego Navarro, University Carlos III of Madrid, Spain
- Ingo Niebel, Private Researcher, Germany
- Paul Reuvers, Crypto Museum, Netherlands
- Anne-Simone Rous, State Palaces, Castles and Gardens of Saxony, Germany
- Klaus Schmech, Codebreaking-Guide.com, Germany
- Gerhard F. Strasser, The Pennsylvania State University, United States
- Satoshi Tomokiyo, Cryptiana, Japan

- Serge Vaudenay, EPFL, Switzerland
- Frode Weierud, Crypto Cellar Research, Norway
- Pavol Zajac, Slovak University of Technology in Bratislava, Slovakia

Local Organizing Committee

- Piotr Bojarski, Enigma Cipher Centre, Poland
- Marcin Słomiński, Enigma Cipher Centre, Poland

Steering Committee

- Carola Dahlke (chair), Deutsches Museum, Germany
- Benedek Láng (vice chair), Budapest University of Technology and Economics, Hungary
- Richard Bean (secretary), University of Queensland, Australia
- Dermot Turing (member), Kellogg College Oxford, UK
- Camille Desenclos (member), Université de Picardie Jules Verne, France