Cryptologia
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ucry20

Rejewski-Różycki-Zygalski Lectures in Computer Science

Jerzy Jaworski

Available online: 01 Oct 2008

To cite this article: Jerzy Jaworski (2008): Rejewski-Różycki-Zygalski Lectures in Computer Science, Cryptologia, 32:4, 348-350

To link to this article: http://dx.doi.org/10.1080/01611190802253128

Cryptologia, 32:348–350, 2008

ISSN: 0161-1194 print
DOI: 10.1080/01611190802253128

Taylor & Francis
Taylor & Francis Group

Rejewski-Różycki-Zygalski Lectures in Computer Science

JERZY JAWORSKI

Abstract The Faculty of Mathematics and Computer Science of Adam Mickiewicz University established an annual series of lectures in computer science. The series is named after Marian Rejewski, Jerzy Różycki, and Henryk Zygalski, alumni of the University who played a key role in the Enigma cipher machine breaking. The inaugural lectures were given by Marek Grajek, Adrew Odlyzko, and Józef Pieprzyk on Cryptology Day, January 25th, 2008.

Keywords Enigma, lectures in computer science, Rejewski, Różycki, Zygalski

To commemorate the 75th anniversary of the breaking of the German Enigma cipher machine, the Faculty of Mathematics and Computer Science of Adam Mickiewicz University established an annual series of lectures in computer science. The series is named after Marian Rejewski, Jerzy Różycki, and Henryk Zygalski, alumni of the University who played a key role in the Enigma breaking. The inaugural lectures were presented on Cryptology Day, January 25th, 2008.

Rejewski, Różycki, and Zygalski achieved the first break of Enigma in 1932. Their success allowed the reading of secret communications of the Third Reich. Six years later, just before Germany's attack on Poland, full technical information about the decryption methods, including copies of the German cipher machine and auxiliary devices used to cryptanalyze it, were transferred to French and English intelligence agencies. Historians agree that the Allies' ability to read communications encrypted with the Enigma significantly shortened the war and saved many human lives. The Polish transfer of information to the French and English significantly accelerated these countries' cryptanalytic progress, and thus contributed to the Allies' victory.

The achievements of Marian Rejewski, Jerzy Różycki, and Henryk Zygalski are worthy of commemoration because their research was very significant to the development of computer science as a whole. It is worth noting that their success, which marked the beginning of use of advanced mathematics in cryptology, was made possible by the very high quality of the education they received at the University of Poznań under professor Zdzisław Krygowski's tutelage. At the same time, contributions to breaking the Enigma cipher by Gwidon Langer, Maksymilian Ciężki, Antoni Palluth, and their co-workers from the pre-war Cipher Bureau and Polish intelligence service must not be underestimated.

Address correspondence to Jerzy Jaworski, Department of Discrete Mathematics, Faculty of Mathematics and Computer Science, Adam Mickiewicz University, ul. Umultowska 87, 61-614 Poznań, Poland. E-mail: jaworski@amu.edu.pl

The following invited guests lectured on Cryptology Day.

Marek Grajek: *Guardians of Lies*

By trade a cryptologist and computer scientist, a historian by avocation. One of the people behind the idea of a statue of Enigma-breakers erected in front of Poznań Castle in 2007 [1]. Consultant in the field of cryptologic applications in the financial and capital markets. Author of a recently published book ''Enigma. Bliżej prawdy'' (''Enigma. Closer to the Truth''), lauded for the innovative combination of author's knowledge of cryptology and his passion for history.

Andrew Odlyzko: *Cybersecurity, Mathematics, and Limits on Technology*

Andrew Odlyzko is a Professor at the University of Minnesota, and the Director of the interdisciplinary Digital Technology Center. Before that, he worked for 26 years at Bell Laboratories, after getting a PhD at the Massachusetts Institute of Technology. He has written over 150 papers in cryptography, number theory, computational complexity, combinatorics, coding theory, probability theory, analysis, economics of data networks, electronic publishing, electronic commerce, and related fields. He has three patents. In 1985, together with Herman J.J. te Riele, he disproved the Mertens conjecture, which, had it been true, would imply the Riemann Hypothesis.

Józef Pieprzyk: *Multi-Party Computations via Graph Coloring*

Józef Pieprzyk is a Professor at Macquarie University, Sydney, Australia, and the Director of Centre for Advanced Computing – Algorithms and Cryptography (ACAC). He has published 5 books, 3 book chapters, and around 160 papers in refereed journals and refereed international conferences. His research interest includes computer network security, database security, design and analysis of cryptographic algorithms, algebraic analysis of block and stream ciphers, theory of cryptographic protocols, secret sharing schemes, threshold cryptography, copyright protection, e-Commerce, and Web security.

Their lectures were well received by the mathematicians representing major Polish academic centers, invited at that opportunity to Poznań, and the students filling three lecture halls and watching the online video transmission. The Rejewski-Różycki-Zygalski lectures will be organized on an annual basis. Their organizers, the Faculty of Mathematics and Computer Science of Adam Mickiewicz University, hope that future editions will gather the ever growing number of mathematicians and computer scientists from all over the world and enjoy a warm welcome as their première.

For more information, see the websites of the Rejewski-Różycki-Zygalski Lectures in Computer Science [2] and of the Faculty of Mathematics and Computer Science of Adam Mickiewicz University [3].

About the Author

Jerzy Jaworski is a Professor at Adam Mickiewicz University, Poznań, Poland. He is a member of the Faculty of Mathematics and Computer Science (Department of

Discrete Mathematics) and head of the Cryptology Centre. His research interests include combinatorial probability, coding, random combinatorial structures, and their applications in cryptology and computer science.

References

1. Grajek, M. April 2008. "Monument *in Memoriam* of Marian Rejewski, Jerzy Różycki and Henryk Zygalski Unveiled in Poznań," *Cryptologia*, 32(2), 101–103.
2. Rejewski-Różycki-Zygalski Lectures in Computer Science: http://enigma.fmcs.amu.edu.pl/
3. Faculty of Mathematics and Computer Science of Adam Mickiewicz University: http://web.wmi.amu.edu.pl/