



Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century

Aiden A. Bruen, Mario A. Forcinito

E-Book	ISBN: 978-1-118-03138-4	September 2011	CAD \$179.99
Hardcover	ISBN: 978-0-471-65317-2	December 2004	CAD \$223.99

DESCRIPTION

Discover the first unified treatment of today's most essential information technologies# Compressing, Encrypting, and Encoding

With identity theft, cybercrime, and digital file sharing proliferating in today's wired world, providing safe and accurate information transfers has become a paramount concern. The issues and problems raised in this endeavor are encompassed within three disciplines: cryptography, information theory, and error-correction. As technology continues to develop, these fields have converged at a practical level, increasing the need for a unified treatment of these three cornerstones of the information age.

Stressing the interconnections of the disciplines, Cryptography, Information Theory, and Error-Correction offers a complete, yet accessible account of the technologies shaping the 21st century. This book contains the most up-to-date, detailed, and balanced treatment available on these subjects. The authors draw on their experience both in the classroom and in industry, giving the book's material and presentation a unique real-world orientation.

With its reader-friendly style and interdisciplinary emphasis, Cryptography, Information Theory, and Error-Correction serves as both an admirable teaching text and a tool for self-learning. The chapter structure allows for anyone with a high school mathematics education to gain a strong conceptual understanding, and provides higher-level students with more mathematically advanced topics. The authors clearly map out paths through the book for readers of all levels to maximize their learning.

This book:

- Is suitable for courses in cryptography, information theory, or error-correction as well as courses discussing all three areas

- Provides over 300 example problems with solutions
- Presents new and exciting algorithms adopted by industry
- Discusses potential applications in cell biology
- Details a new characterization of perfect secrecy
- Features in-depth coverage of linear feedback shift registers (LFSR), a staple of modern computing
- Follows a layered approach to facilitate discussion, with summaries followed by more detailed explanations
- Provides a new perspective on the RSA algorithm

Cryptography, Information Theory, and Error-Correction is an excellent in-depth text for both graduate and undergraduate students of mathematics, computer science, and engineering. It is also an authoritative overview for IT professionals, statisticians, mathematicians, computer scientists, electrical engineers, entrepreneurs, and the generally curious.

ABOUT THE AUTHOR

AIDEN A. BRUEN, PHD, is a Professor of Mathematics and Statistics at the University of Calgary in Calgary, Alberta, Canada. He has over 100 published articles in refereed journals and has served for many years on the Editorial Board of Designs, Codes and Cryptography. His research interests include error-correcting codes, number theory, algebraic geometry, algebra finite geometries, information theory, and cryptography.

MARIO A. FORCINITO, PHD, is a professional engineer with over ten years' experience as an industrial consultant. He is President of SUR Consultants in Engineering Science Inc., a member of the IEEE Computer Society, and has published extensively in peer-reviewed journals. Dr. Forcinito has experience lecturing on cryptography and numerical methods at several technical meetings.

SERIES

Wiley Series in Discrete Mathematics and Optimization

For additional product details, please visit <https://www.wiley.com/en-ca>