Whether ensuring the privacy of data sent over the Internet, making password cracking more difficult, or providing integrity for digitally signed documents, cryptography is now a part of our everyday lives. Following two previous successful editions that have led it to become the most relied-upon source in the field, **Introduction to Modern Cryptography** provides a mathematically rigorous yet accessible treatment of this fascinating subject.

The book's focus is on modern cryptography, which is distinguished from classical cryptography by its emphasis on definitions, precise assumptions, and rigorous proofs of security. A unique feature of this book is that it presents theoretical foundations with an eye toward understanding the latest cryptographic standards in wide use today. This perspective motivated several changes introduced in the third edition, which include:

- Enhanced treatment of several modern aspects of private-key cryptography, including authenticated encryption and nonce-based encryption.
- Coverage of widely used standards such as GMAC, Poly1305, GCM, CCM, and ChaCha20-Poly1305.
- New sections covering the ChaCha20 stream cipher, sponge-based hash functions, and SHA-3.
- Increased coverage of elliptic-curve cryptography, including a discussion of various curves used in practice.
- A new chapter describing the impact of quantum computers on cryptography and providing examples of "post-quantum" encryption and signature schemes.

Containing worked examples and updated exercises, **Introduction to Modern Cryptography** can serve as a textbook for undergraduate- or graduate-level courses in cryptography, a reference for graduate students, researchers, and practitioners, or a general introduction suitable for self-study.

MATHEMATICS

CRC Press
Taylor & Francis Group
an **informa** business
www.routledge.com

CRC Press titles are available as eBook editions in a range of digital formats

ISBN: 978-0-8153-5436-9
90000
9 780815 354369