Delfs, Hans; Knebl, Helmut
Introduction to cryptography. Principles and applications. 3rd edition. (English)
[Zbl 1333.94001]

From the text: The third edition is a further substantive extension, with new topics added, including: elliptic curve cryptography, Paillier encryption, quantum cryptography, the new SHA-3 standard for cryptographic hash functions, a considerably extended section on electronic elections and Internet voting, mix nets, and zero-knowledge proofs of shuffles.

The book is well-suited for undergraduate and graduate students in computer science, mathematics, and engineering.

The first part of this book covers the key concepts of cryptography on an undergraduate level, from encryption and digital signatures to cryptographic protocols. Essential techniques are demonstrated in protocols for key exchange, user identification, electronic elections and digital cash. In the second part, more advanced topics are addressed, such as the bit security of one-way functions and computationally perfect pseudorandom bit generators. The security of cryptographic schemes is a central topic. Typical examples of provably secure encryption and signature schemes and their security proofs are given. Though particular attention is given to the mathematical foundations, no special background in mathematics is presumed. The necessary algebra, number theory and probability theory are included in the appendix. Each chapter closes with a collection of exercises.

In the second edition [Zbl 1229.94001] the authors added a complete description of the AES, an extended section on cryptographic hash functions, and new sections on random oracle proofs and public-key encryption schemes that are provably secure against adaptively-chosen-ciphertext attacks.

An extensive review was given in Zbl 0995.94001.

Reviewer: Olaf Ninnemann (Berlin)

MSC:
94-01 Introductory exposition (textbooks, tutorial papers, etc.) pertaining to information and communication theory
94A60 Cryptography
68P25 Data encryption (aspects in computer science)
81P94 Quantum cryptography (quantum-theoretic aspects)

Full Text: DOI