

Introduction to Cryptography

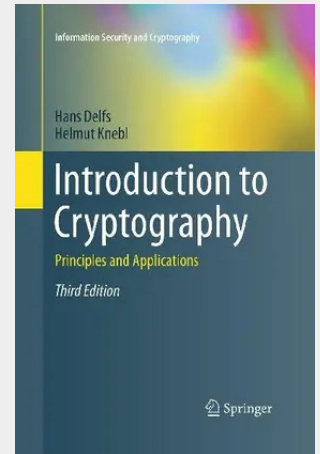
Principles and Applications

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 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. 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 appropriate 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 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. 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 appropriate for undergraduate and graduate students in computer science, mathematics, and engineering.



53,49 €

49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783662499665

Medium: Buch

ISBN: 978-3-662-49966-5

Verlag: Springer

Erscheinungstermin: 23.08.2016

Sprache(n): Englisch

Auflage: Softcover Nachdruck of the original 3rd Auflage 2015

Serie: Information Security and Cryptography

Produktform: Kartoniert

Gewicht: 7898 g

Seiten: 508

Format (B x H): 155 x 235 mm

