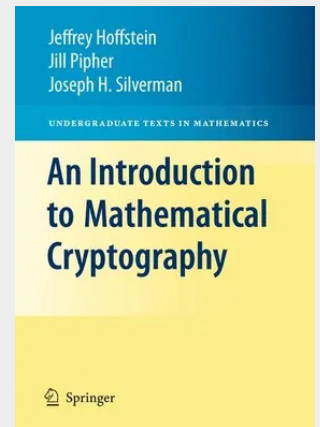


An Introduction to Mathematical Cryptography

An Introduction to Mathematical Cryptography provides an introduction to public key cryptography and underlying mathematics that is required for the subject. Each of the eight chapters expands on a specific area of mathematical cryptography and provides an extensive list of exercises. It is a suitable text for advanced students in pure and applied mathematics and computer science, or the book may be used as a self-study. This book also provides a self-contained treatment of mathematical cryptography for the reader with limited mathematical background.

The creation of public key cryptography by Diffie and Hellman in 1976 and the subsequent invention of the RSA public key cryptosystem by Rivest, Shamir, and Adleman in 1978 are watershed events in the long history of secret communications. It is hard to overestimate the importance of public key cryptosystems and their associated digital signature schemes in the modern world of computers and the Internet. This book provides an introduction to the theory of public key cryptography and to the mathematical ideas underlying that theory. Public key cryptography draws on many areas of mathematics, including number theory, abstract algebra, probability, and information theory. Each of these topics is introduced and developed in sufficient detail so that this book provides a self-contained course for the beginning student. The only prerequisite is a first course in linear algebra. On the other hand, students with stronger mathematical backgrounds can move directly to cryptographic applications and still have time for advanced topics such as elliptic curve pairings and lattice-reduction algorithms. Among the many facets of modern cryptography, this book chooses to concentrate primarily on public key cryptosystems and digital signature schemes. This allows for an in-depth development of the necessary mathematics required for both the construction of these schemes and an analysis of their security. The reader who masters the material in this book will not only be well prepared for further study in cryptography, but will have acquired a real understanding of the underlying mathematical principles on which modern cryptography is based.



43,82 €
40,95 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9780387779935
Medium: Buch
ISBN: 978-0-387-77993-5
Verlag: Springer Netherlands
Erscheinungstermin: 12.08.2008
Sprache(n): Englisch
Auflage: 1. Auflage 2008
Serie: Undergraduate Texts in Mathematics
Produktform: Gebunden
Gewicht: 2060 g
Seiten: 524
Format (B x H): 155 x 235 mm

