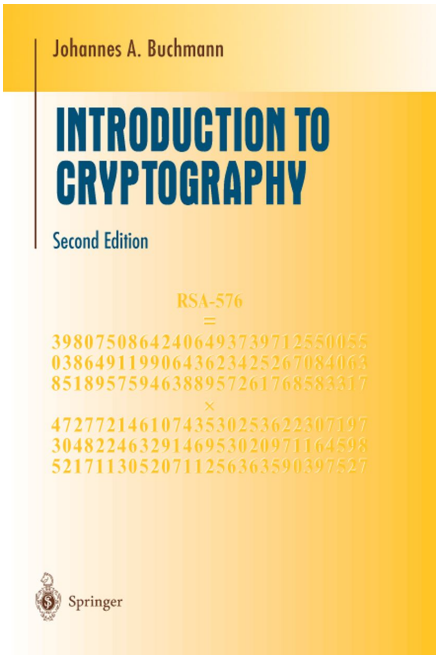

Johannes Buchmann

Introduction to Cryptography

Series: Undergraduate Texts in Mathematics

Cryptography is a key technology in electronic key systems. It is used to keep data secret, digitally sign documents, access control, and so forth. Users therefore should not only know how its techniques work, but they must also be able to estimate their efficiency and security. Based on courses taught by the author, this book explains the basic methods of modern cryptography. It is written for readers with only basic mathematical knowledge who are interested in modern cryptographic algorithms and their mathematical foundation. Several exercises are included following each chapter. This revised and extended edition includes new material on the AES encryption algorithm, the SHA-1 Hash algorithm, on secret sharing, as well as updates in the chapters on factoring and discrete logarithms.

2nd ed. 2004, XVI, 338 p.

Printed book

Softcover

64,99 € | £54.99 | $79.99

[1]69,54 € (D) | 71,49 € (A) | CHF 77,00

eBook

53,49 € | £43.99 | $59.99

[2]53,49 € (D) | 53,49 € (A) | CHF 61,50

Available from your library or springer.com/shop

MyCopy [3]

Printed eBook for just

€ | $ 24.99

springer.com/mycopy

Error[en_EN | Export.Bookseller.MediumType | SE]