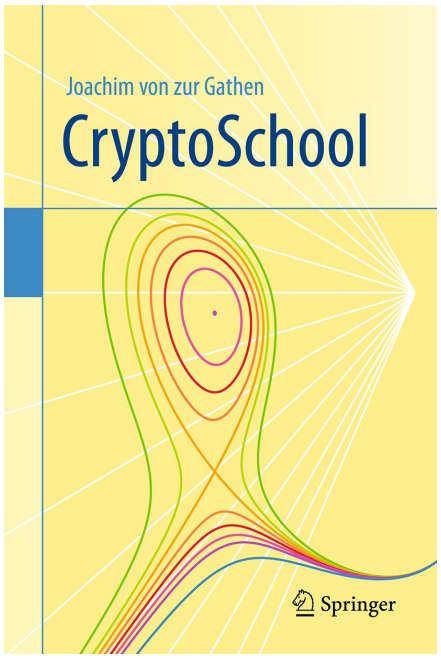


1st ed. 2015, XII, 876 p. 186 illus., 97 illus. in color.

## Printed book

Hardcover

34,99 € | £27.99 | $44.99
[1]37,44 € (D) | 38,49 € (A) | CHF 41,50

Softcover

34,99 € | £30.99 | $44.99
[1]37,44 € (D) | 38,49 € (A) | CHF 41,50

## eBook

29,74 € | £23.99 | $34.99
[2]29,74 € (D) | 29,74 € (A) | CHF 33,00

Available from your library or springer.com/shop

## MyCopy [3]

Printed eBook for just
€ | $ 24.99
springer.com/mycopy

Joachim von zur Gathen

# CryptoSchool

- **Basic and advanced cryptographic methods with complete underpinnings**
- **Modern approach with security reductions throughout the text**
- **Colorful history of cryptography with over 100 illustrations, half of them in color**
- **Suitable for beginners**

This book offers an introduction to cryptology, the science that makes secure communications possible, and addresses its two complementary aspects: cryptography——the art of making secure building blocks——and cryptanalysis——the art of breaking them. The text describes some of the most important systems in detail, including AES, RSA, group-based and lattice-based cryptography, signatures, hash functions, random generation, and more, providing detailed underpinnings for most of them. With regard to cryptanalysis, it presents a number of basic tools such as the differential and linear methods and lattice attacks. This text, based on lecture notes from the author's many courses on the art of cryptography, consists of two interlinked parts. The first, modern part explains some of the basic systems used today and some attacks on them. However, a text on cryptology would not be complete without describing its rich and fascinating history. As such, the colorfully illustrated historical part interspersed throughout the text highlights selected inventions and episodes, providing a glimpse into the past of cryptology. The first sections of this book can be used as a textbook for an introductory course to computer science or mathematics students. Other sections are suitable for advanced undergraduate or graduate courses. Many exercises are included. The emphasis is on providing reasonably complete explanation of the background for some selected systems.