《Introduction to cryp》

图书基本信息

书名：《Introduction to cryptography对密码学的介绍》

13位ISBN编号：9780387207568

10位ISBN编号：0387207562

出版时间：2004-7

出版社：Springer Verlag

作者：Johannes Buchmann

页数：335

《Introduction to cryp》

内容概要

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 thereforeshould 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 knowledgewho 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. Johannes A. Buchmann is Professor of Computer Science and Mathematics at the Technical University of Darmstadt, andan Associate Editor of the Journal of Cryptology. In 1985, he receiveda Feodor Lynen Fellowship of the Alexander von Humboldt Foundation. He has alsoreceived the most prestigious award in science in Germany, the Leibniz Award of the German Science Foundation (Deutsche Forschungsgemeinschaft).

《Introduction to cryp》

书籍目录

《Introduction to cryp》

版权说明