<<信息安全与密码学>>

图书基本信息

书名：<<信息安全与密码学>>

13位ISBN编号：9787302139584

10位ISBN编号：730213958X

出版时间：2007-1

出版时间：清华大学

作者：徐茂智

页数：271

<<信息安全与密码学>>

内容概要

《信息安全与密码学》介绍信息安全与密码的基础理论与基本应用。
信息安全的核心得密码学，所以密码学也是《信息安全与密码学》的重点。
全书由绪论、信息安全初步、信息安全技术、传统密码学、公钥密码算法、Hash函数、计算复杂性理论、零知识证明与比特承诺、基于身份的公钥密码学、数学签名、密钥管理和密码学中的基本数学知识（附录）组成，共11章及一个附录。
所涉及的内容基本了涵盖了现代密码学的基本概念、基本算法，以及信息安全的基本知识。
附录是对数论基本知识，以及群、环、域等一些基本代数概念的简单介绍。
《信息安全与密码学》每章配有习题，便于检验加深学生对所学内容的理解和掌握。
《信息安全与密码学》可作为数学、计算机科学、通信、电子工程等相关专业的本科高年级学生或研究生一个学期课程的教材或参考书。

<<信息安全与密码学>>

书籍目录

<<信息安全与密码学>>

编辑推荐

本书介绍信息安全与密码学的基础理论与基本应用。
信息安全的核心是密码学，所以密码学也是本书的重点。
全书由绪论、信息安全初步、信息安全技术、传统密码学、公钥密码算法、Hash函数、计算复杂性理论、零知识证明与比特承诺、基于身份的公钥密码学、数字签名、密钥管理和密码学中的基本数学知识(附录)组成，共11章及一个附录。
所涉及的内容基本上涵盖了现代密码学的基本概念、基本算法．以及信息安全的基本知识。
附录是刘数论基本知识，以及群、环、域等一些基本代数概念的简单介绍。
本书每章均配有习题，便于检验和加深学生对所学内容的理解和掌握。
本书可作为数学、计算机科学、通信、电子工程等相关专业的本科高年级学生或研究生一个学期课程的教材或参考书。

<<信息安全与密码学>>

版权说明