第一图书网, tushu007.com

<<密码学原理与实践>>

图书基本信息

书名：<<密码学原理与实践>>

13位ISBN编号：9787505384651

10位ISBN编号：7505384651

出版时间：2003-1

出版时间：电子工业出版社

作者：Douglas R.Stinson；冯

页数：278

字数：480000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

内容概要

本书是密码学领域的经典著作，被世界上的多所大学用做指定教科书。
本书在第1版的基础上进行了细致和严谨的修改，将重点集中放在密码学研究的核心问题上，从应用离散数学的角度对密码学进行了系统阐述。
全书共分7章，从古典密码学开始，继而介绍了Shannon的信息论在密码学中的应用，然后进入现代密码学部分，先后介绍了加密技术、数据加密标准（DES）、高级加密标准（ADES）、公钥密码学、单向Hash函数、数字签名等，在内容的选择上既突出了广泛性，又注重对要点的深入探讨。
书中对于数学背景知识的讲授采取“即学即用”的方式，将基础知识与算法描述有机地穿插在一起，使读者对算法的理解更加深刻和精确；同时，相关的定义、定理、引理、证明都阐释得非常清晰，读者完全可以感受到一种逻辑上的美感。
每一章后都附有大量的练习题，这既利于读者对书中内容的总结和应用，又是对兴趣、思维和智力的挑战。

本书适合于作为计算机科学、数学等相关学科的密码学课程的教材或教学参考书，同时也是密码学研究的必备参考书。

作者简介

本书作者Douglas R.Stinson 博士：加拿大Waterloo大学教授，“ Jounrnal of Combinatorial Design ”期刊的主编。
他的研究领域包括密码学、网络和分布式系统、算法和计算复杂性、组合结构的构造及在计算机和密码学中的应用。

书籍目录

第1章 古典密码学 1.1 几个简单的密码体制 1.2 密码分析 1.3 注释与参考文献 练习第2章 Shannon理论 2.1 引言 2.2 概率论基础 2.3 完善保密性 2.4 熵 2.5 熵的性质 2.6 伪密钥和惟一解距离 2.7 乘积密码体制 2.8 注释与参考文献 练习第3章 分组密码与高级加密标准 3.1 引言 3.2 代换-置换网络 3.3 线性密码分析 3.4 差分密码分析 3.5 数据加密标准 3.6 高级加密标准 3.7 工作模式 3.8 注释与参考文献 练习第4章 Hash函数 4.1 Hash函数与数据完整性 4.2 Hash函数的安全性 4.3 迭代Hash函数 4.4 消息认证码 4.5 无条件安全消息认证码 4.6 注释与参考文献 练习第5章 RSA密码体制和整数因子分解 5.1 公钥密码学简介 5.2 更多的数论知识 5.3 RSA密码体制 5.4 素性检测 5.5 模n的平方根 5.6 分解因子算法 5.7 对RSA的其他攻击 5.8 Rabin密码体制 5.9 RSA的语义安全 5.10 注释与参考文献 练习第6章 基于离散对数问题的公钥密码体制第7章 签名方案练习参考文献

第一图书网, tushu007.com

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com