

<<密码学导引>>

图书基本信息

书名：<<密码学导引>>

13位ISBN编号：9787111124788

10位ISBN编号：7111124782

出版时间：2003-12-1

出版时间：机械工业出版社

作者：Paul Garrett

页数：389

译者：吴世忠

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>

<<密码学导引>>

内容概要

本书着重介绍现代密码学的加密思想及其实现方法，内容涉及数论、概率论、抽象代数、加密算法的思想及复杂度理论。

本书介绍了密码学的历史沿革，剖析了古典的加密算法为何会被现代的加密算法所取代，展望了密码编码领域的发展，为古典和现代密码体系提供了数学理论基础，还给出了一些针对各种加密算法的密码分析方法。

本书适合作为高校计算机安全与信息安全专业密码学导论的简明教材，也可供对密码学、数论和计算机数论有兴趣的技术人员参考。

作者简介

Paul Garrett : 1973年21岁时获普渡大学硕士学位, 1977年于普林斯顿大学获博士学位, 之后在耶鲁大学任教。

1979 ~ 1981年在加州大学伯克利分校获得美国国家科学基金会资助的博士后奖学金, 1979年成为斯坦福大学副教授, 自1982年起, Paul Garrett开始在明尼苏达大学授课, 1987

<<密码学导引>>

书籍目录

出版者的话 专家指导委员会译者简介 译者序 前言 引言 第1章 简单密码 第2章 概率 第3章 置换 第4章 严格的密码 第5章 概率问题 第6章 现代对称密码 第7章 整数 第8章 希尔密码 第9章 复杂度 第10章 公钥密码算法 第11章 素数 第12章 $\text{mod } p$ 的根 第13章 模合数的根 第14章 弱乘法性 第15章 二次互反定理 第16章 伪素数 第17章 群 第18章 协议概述 第19章 环、域、多项式 第20章 分圆多项式 第21章 随机数发生器 第22章 群的更多知识 第23章 伪素性证明 第24章 因式分解攻击 第25章 现代因式分解攻击 第26章 有限域 第27章 离散对数 第28章 椭圆曲线 第29章 有限域的更多知识 附录A 相关公式 附录B 部分习题答案 附录C 常用数表

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>