

<<现代密码学基础>>

图书基本信息

书名：<<现代密码学基础>>

13位ISBN编号：9787563506514

10位ISBN编号：7563506519

出版时间：2004-6

出版时间：北京邮电大学出版社

作者：章照止编

页数：280

字数：401

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>

## <<现代密码学基础>>

### 内容概要

本书全面深入地介绍了现代密码学的基础理论。

全书共分15章和1个附录。

内容包括密码学研究的基本问题、古典密码学、密码学的信息论基础和计算复杂性理论基础、单向函数和伪随机序列生成器的严格理论、序列密码、分组密码和公钥密码、字签名、杂凑函数、身份识别、认证码、密钥管理和零知识证明，附录的内容包括本书用到的代数学和初等数论方面的基础知识，每章还包括注记和习题。

本书注意了严格理论和直观描述的配合，在介绍经典密码体制的同时，注意从中总结出一般的原则和方法及基本工具，并注重介绍一些新的密码体制。

本书是为信息安全专业编写的专业基础课教材，适用于高等院校信息安全本科专业的学生以及计算机应用、信息工程、应用数学等相关本科专业的学生，同时也可供从事信息安全工作的科技人员以及相关专业的研究生参考。

## <<现代密码学基础>>

### 书籍目录

第1章 引论 密码学研究的基本问题 密码学的广泛应用 本书选材的组织与安排 习题一第2章 古典密码学 古典密码体制 古典密码体制分析 习题二第3章 密码学的信息论基础 保密系统的数学模型 信息量和熵 完善保密性 理论安全性和实际安全性 习题三第4章 密码学的计算复杂性理论基础 问题与算法的复杂性 问题的计算复杂性分类 习题四第5章 单向函数 一般单向函数 单向函数族 单向函数族的其他性质 单向函数的硬核 习题五第6章 伪随机序列生成器 计算不可区分性 伪随机序列生成器的定义和性质 伪随机序列生成器的构造 用伪随机序列生成器构造伪随机函数 伪随机置换的构造 习题六第7章 序列密码第8章 分组密码第9章 公钥密码学第10章 数字签名第11章 杂凑 (Hash) 函数第12章 身份识别方案第13章 认证码第14章 密钥管理第15章 零知识证明

<<现代密码学基础>>

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>