

<<现代密码学理论与实践>>

图书基本信息

书名：<<现代密码学理论与实践>>

13位ISBN编号：9787505399259

10位ISBN编号：750539925X

出版时间：2004-1

出版时间：电子工业出版社

作者：毛文波

页数：477

字数：800000

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>

## <<现代密码学理论与实践>>

### 内容概要

很多密码方案与协议，特别是基于公钥密码体制的，有一些基础性或所谓的“教科书式密码”版本，这些版本往往是很多密码学教材所包含的内容。

本书采用了一种不同的方式来介绍密码学——更加注重适于应用的密码学方面。

它解释了那些“教科书式密码”版本仅适合于理想世界的原因，即数据是随机的、坏人的表现不会超过预先的假定。

本书通过展示“教科书式密码”版本的方案、协议、和系统在各种现实应用场合存在着很多攻击，来揭示“教科书式密码”版本在现实生活中的不适用性。

本书有选择性的介绍了一些实用的密码方案、协议和系统，其中多数已成为了标准或事实上的标准，对其进行了详细的研究，解释了其工作原理，讨论了其实际应用，并且常会以建立安全性形式证明的方式来考察它们的强（实用）安全性。

另外，本书还完整地给出了学习现代密码学所必备的理论基础知识。

本书可作为高院校计算机专业研究生或高年级本科生的教材，也可供密码安全架构师、工程人员、开发人员以及管理人员参考。

## <<现代密码学理论与实践>>

### 作者简介

Wenbo Mao, 1993年获英国格拉斯哥Strathclyde大学计算机科学博士。  
1992年到1994年在英国Manchester大学做博士后研究期间, 与C.Boyd博士对密码协议和协议形式的分析进行了深入研究并做出了贡献。  
后加入HP公司做高级技术成员, 在英国的Bristol研究实验室的可信赖系统实验室

## &lt;&lt;现代密码学理论与实践&gt;&gt;

## 书籍目录

第一部分 引言 第1章 一个简单的通信游戏 1.1 一个通信游戏 1.2 描述密码系统和协议的准则 1.3 本章小结 习题 第2章 防守与攻击 2.1 引言 2.2 加密 2.3 易受攻击的环境 (Dolev?Yao威胁模型) 2.4 认证服务器 2.5 认证密钥建立的安全特性 2.6 利用加密的认证密钥建立协议 2.7 本章小结 习题 第二部分 数学基础 标准符号 第3章 概率论和信息论 3.1 引言 3.2 概率论的基本概念 3.3 性质 3.4 基本运算 3.5 随机变量及其概率分布 3.6 生日悖论 3.7 信息论 3.8 自然语言的冗余度 3.9 本章小结 习题 第4章 计算复杂性 4.1 引言 4.2 图灵机 4.3 确定性多项式时间 4.4 概率多项式时间 4.5 非确定多项式时间 4.6 非多项式界 4.7 多项式时间不可区分性 4.8 计算复杂性理论与现代密码学 4.9 本章小结 习题 第5章 代数学基础 5.1 引言 5.2 群 5.3 环和域 5.4 有限域的结构 5.5 用椭圆曲线上的点构造群 5.6 本章小结 习题 第6章 数论 6.1 引言 6.2 同余和剩余类 6.3 欧拉 $\phi$ 函数 6.4 费马定理、欧拉定理、拉格朗日定理 6.5 二次剩余 6.6 模一个整数的平方根 6.7 Blum整数 6.8 本章小结 习题 第三部分 基本的密码学技术 第7章 加密——对称技术 第8章 加密——非对称技术 第9章 理想情况下基本公钥密码函数的比特安全性 第10章 数据完整性技术 第四部分 认证 第11章 认证协议——原理篇 第12章 认证协议——实践篇 第13章 公钥密码的认证框架 第五部分 建立安全性的形式化方法 第14章 公钥密码体制的形式化强安全性定义 第15章 可证明安全的有效公钥密码体制 第16章 强可证明安全的数字签名方案 第17章 分析认证协议的形式化方法 第六部分 密码学协议 第18章 零知识协议 第19章 回到“电话掷币”协议 第20章 结束语参考文献

<<现代密码学理论与实践>>

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>