

<<计算机密码应用基础>>

图书基本信息

书名：<<计算机密码应用基础>>

13位ISBN编号：9787030084361

10位ISBN编号：7030084365

出版时间：2005-1

出版时间：高教分社

作者：朱文余，孙琦

页数：200

字数：231000

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>

<<计算机密码应用基础>>

内容概要

本书是在四川大学密码学公共选修课所用的讲义基础上编写而形成的。内容涉及密码学中几大“核心”领域，包括分组密码、香农理论、序列密码、公钥密码以及他们的应用，其中还涉及必要的数学知识。

本书可供高等院校计算机系、无线电系、数学系等专业用作密码学教材或参考书，也可供从事计算机科学、通信理论、密码学等工作的科技人员参考。

<<计算机密码应用基础>>

书籍目录

第一章 简单密码体制及分析 1.1 密码学的基本概念 1.2 一些简单密码体制与它的破译 1.2.1 置换密码 1.2.2 单表代替密码 1.2.3 单表代替密码的统计分析 1.2.4 多表代替密码 1.2.5 对Vigenere密码的分析 1.2.6 代数密码 1.2.7 Hill加密算法 1.2.8 关于Hill密码的已知明文攻击 习题第二章 分组密码 2.1 DES数据加密标准 2.1.1 DES加密算法 2.1.2 DES加密的一个例子 2.2 FEAL密码 2.3 IDEA密码系统 2.4 分组密码的应用技术 习题第三章 香农理论 3.1 密码体制的概率分布 3.2 熵 3.3 条件熵 3.4 多余度和唯一解码量 3.5 完全保密体制 习题第四章 序列密码和移位寄存器 4.1 引言 4.2 序列密码的一般原理 4.3 线性移位寄存器 4.4 线性移位寄存器的一元多项式表示 4.5 m序列的伪随机性 4.6 m序列密码的破译 4.7 非线性序列 习题第五章 RSA公钥密码体制 5.1 概论 5.2 计算复杂性理论 5.2.1 算法复杂性 5.2.2 问题复杂性和NP完全问题 5.3 必备的数论知识 5.3.1 同余方程和中国剩余定理 5.3.2 欧几里得算法 5.3.3 Wilson定理 5.3.4 欧拉函数 5.3.5 平方剩余和Jacobi符号 5.4 RSA公钥系统 5.4.1 RSA加密算法 5.4.2 RSA安全性讨论 5.5 RSA公钥密码体制的一种改进方案 5.5.1 RSA公钥密码体制的一种潜在弱点 5.5.2 RSA公钥体制改进方案 5.5.3 RSA改进方案的安全性分析 5.5.4 改进方案举例 5.6 大素数的产生 5.7 因数分解 5.7.1 Fermat因数分解法 5.7.2 连分数因式分解法 5.7.3 用圆锥曲线分解整数 5.7.4 P-1方法 5.8 对RSA体制中小指数的攻击 5.9 Rabin密码体制 5.10 RSA在有限域 F_p 上多项式上的推广 5.10.1 F_p 上的多项式 5.10.2 RSA在 F_p 上的多项式上的推广 习题第六章 其它公钥密码体制 6.1 背包公钥系统 6.2 群论中有关概念和结果 6.3 离散对数公钥密码体制 6.4 离散对数问题的算法 6.5 概率公钥体制 6.6 关于 F_p 上的椭圆曲线 6.7 $E(F_q)$ 中密码体制与明文嵌入方法 6.8 有限域 F_p 上圆锥曲线的公钥密码系统 6.9 双密钥公开钥密码体制 6.10 公钥密码系统的应用 习题第七章 数字签名 7.1 利用公开密钥密码获得数字签名 7.2 利用传统密码获得数字签名 7.3 美国数字签名标准DSS 7.4 不可否认的签名协议 习题参考文献

<<计算机密码应用基础>>

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>