

<<密码学>>

图书基本信息

书名：<<密码学>>

13位ISBN编号：9787040280456

10位ISBN编号：7040280450

出版时间：2009-11

出版时间：高等教育出版社

作者：金晨辉等著

页数：382

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>

## &lt;&lt;密码学&gt;&gt;

## 内容概要

《密码学》由中国人民解放军信息工程大学密码学课程组在长期教学过程中所使用的内部讲义完善而成，定位于介绍密码学的基本原理和基本方法，通过该书的学习，读者可以系统地掌握密码学的基本原理、基本方法和基本技术。

全书共包括10章和1个附录。

第1章介绍了密码学的基本概念和基本编码原理。

第2章介绍了shannon保密理论和计算复杂性理论。

第3、4章分别介绍了序列密码和分组密码的基本原理和方法。

第5、6和7章分别介绍了公钥密码、数字签名和杂凑函数的基小理论和方法。

第8章和第9章分别介绍了认证技术、随机数的产生与检验方法。

第10章介绍了密钥管理和密钥分配协议的理论与方法。

附录介绍了相关的数学知识。

为适应不同层次读者的需要，并使他们接触更多的密码学知识，《密码学》有意增加了许多相关内容。

在具体的教学实施过程中，可根据需要对有关内容进行选择。

小书既可作为本科生的教材，也可作为硕士研究生和密码研究人员的入门教材。

## 书籍目录

第1章 密码学概述1.1 引言1.2 密码学的基本概念1.2.1 密码编码学1.2.2 密码分析学1.2.3 密钥管理学1.3 密码的基本编码原理1.3.1 移位密码1.3.2 代替密码1.4 代替密码分析1.4.1 语言的内在规律1.4.2 单表代替密码分析1.4.3 多表代替密码分析习题参考文献第2章 保密理论2.1 信息论简介2.1.1 随机事件的信息量和概率分布的熵2.1.2 熵的基本性质2.1.3 联合熵、条件熵和互信息2.2 Shannon保密理论2.2.1 理论上的保密性2.2.2 密码体制的唯一解码量2.3 计算复杂性理论2.3.1 实际保密性2.3.2 算法和问题2.3.3 算法的计算复杂性2.3.4 问题的复杂性习题参考文献第3章 序列密码3.1 伪随机序列的常规特性3.1.1 周期序列和最终周期序列3.1.2 伪随机性的Golomb三假设3.2 序列密码的基本模型3.2.1 序列密码的一般模型3.2.2 无明文反馈的模型3.2.3 明密文反馈模型3.2.4 自同步密码模型3.3 有限域上的线性反馈移存器3.3.1 有限域上的n级递归序列3.3.2 线性反馈移存器简介3.3.3 m序列的密码特性3.3.4 m序列的还原特性3.3.5 基于除法电路设计的LFSR3.4 Walsh谱理论3.4.1 复数值函数的Walsh谱理论3.4.2 Boole函数的Walsh谱理论3.4.3 Bent函数3.4.4 多输出Boole函数的平衡性判定定理3.4.5 函数复合与函数求和的Walsh谱计算3.5 序列密码的基本编码技术3.5.1 前馈模型3.5.2 非线性滤波模型3.5.3 非线性组合模型3.5.4 滤波一组合模型3.5.5 钟控模型3.5.6 有记忆变换模型3.6 RC4序列密码算法3.7 A5序列密码算法3.7.1 A5-1序列密码算法3.7.2 A5-2序列密码算法习题参考文献第4章 分组密码4.1 分组密码概述4.2 分组密码的基本设计原则4.2.1 安全原则4.2.2 实现原则4.3 分组密码的整体结构4.3.1 S-P网络4.3.2 Feistel模型4.4 数据加密标准4.4.1 背景4.4.2 DES算法4.4.3 DES的简单分析4.4.4 DES的安全性4.4.5 多重DES4.5 穷举攻击4.5.1 穷举攻击的基本方案4.5.2 穷举攻击的实现方案4.6 差分密码分析4.6.1 差分密码分析概述4.6.2 DES的差分密码分析4.7 线性密码分析4.7.1 对DES算法f函数的线性逼近4.7.2 线性逼近方程的建立4.8 国际数据加密算法4.8.1 IDEA算法4.8.2 IDEA的简单分析4.9 高级加密标准4.9.1 背景4.9.2 数学基础4.9.3 状态和状态矩阵4.9.4 AES算法4.9.5 AES的简单分析4.10 分组密码的工作模式4.10.1 电码本模式4.10.2 密码分组链接模式4.10.3 密码反馈模式4.10.4 输出反馈模式4.10.5 尾分组处理方法习题参考文献第5章 公钥密码技术5.1 RSA公钥密码体制5.1.1 RSA公钥密码体制介绍5.1.2 大素数生成算法5.1.3 RSA的实现5.2 RSA密码体制的安全性分析5.2.1 因子分解的进展及实用算法5.2.2 对RSA的其他攻击5.2.3 共模RSA体制的安全性分析5.2.4 RSA参数的选择5.3 基于离散对数问题的公钥密码5.3.1 有限域上的离散对数问题5.3.2 ElGamal公钥密码算法5.3.3 Diffie-Hellman密钥交换协议5.4 椭圆曲线公钥密码体制5.4.1 椭圆曲线的定义5.4.2 椭圆曲线群上的离散对数问题5.4.3 椭圆曲线上的公钥密码习题参考文献第6章 数字签名6.1 RSA数字签名方案6.1.1 RSA数字签名方案6.1.2 RSA数字签名的同态性6.1.3 RSA数字签名与加密的结合6.2 ElGamal数字签名方案6.2.1 ElGamal数字签名方案6.2.2 ElGamal数字签名方案的安全性分析6.2.3 ElGamal数字签名方案的变型6.2.4 数字签名标准DSS6.2.5 椭圆曲线数字签名算法(ECDSA)参考文献第7章 杂凑函数7.1 杂凑函数的性质及应用7.2 杂凑函数的基本攻击方法7.3 基于分组密码的杂凑函数设计7.4 MD5杂凑函数7.5 SHA杂凑函数习题参考文献第8章 认证技术8.1 消息认证8.1.1 对称密码体制实现的消息认证8.1.2 杂凑函数实现的消息认证8.1.3 公钥密码体制实现的消息认证8.2 身份认证8.2.1 弱身份认证8.2.2 强身份认证8.3 认证技术的应用8.3.1 人机认证8.3.2 产品防伪习题参考文献第9章 随机数的产生与检验9.1 随机数的描述9.2 随机数和伪随机数的产生方法9.3 随机数的检验方法9.3.1 正态分布和 $\chi^2$ 分布9.3.2 假设检验9.3.3 5种基本检验(5项常规统计检验)习题参考文献第10章 密钥管理10.1 密钥管理的内容10.1.1 密钥的概念10.1.2 密钥的分配10.1.3 密钥的维护10.2 密钥的分层和分散管理10.2.1 密钥的分层管理10.2.2 密钥的分散管理10.3 密钥分配技术10.3.1 密钥分配的体系结构10.3.2 密钥分配协议10.4 公钥基础设施的基本原理10.4.1 PKI的一些基本概念10.4.2 公钥证书的生成过程10.4.3 证书的结构及实现原理10.4.4 证书的验证过程习题参考文献附录 数学基础知识附录1 概率论和统计检验基础附录2 数论基础附录3 代数基础参考文献

#### 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>