第一图书网, tushu007.com

<<密码学基础>>

图书基本信息

书名：<<密码学基础>>

13位ISBN编号：9787560620848

10位ISBN编号：7560620841

出版时间：2008-8

出版时间：西安电子科技大学出版社

作者：范九伦 等 著

页数：174

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

前言

密码学有着悠久而神秘的历史，最早的密码技术可以追溯到古罗马时代。
1949年，Claude Shannon在Bell System Technical Journal上发表的论文“The Communication Theory of Secrecy Systems”，标志着密码学研究进入了崭新的时代。
20世纪70年代以来，分组密码和公钥密码技术得到了迅速发展，取得了丰富的研究成果，也被广泛应用于信息安全的各个领域。
随着互联网技术和计算机技术的发展和普及，越来越多的人认识到密码学的重要性。
为了能为在校本科生学习密码学提供内容较新、论述较系统的教材，也能为相关领域的科研人员提供一本内容充实、具有一定实用性的参考书，我们编写了《密码学基础》这本教材。
本书系统介绍了密码学的基本原理，在此基础上详细介绍了密码学中的基本算法及其应用，详细介绍了当前广泛应用的密码算法及其理论基础，并对其安全性进行了相应的分析。
本书内容以当前广泛应用的密码技术为主，重点放在密码学研究的核心问题上，既突出了广泛性，又注重对主要知识内容的深入讨论。
本书的每一章后都附有相应的习题，便于读者对书中的内容进行总结和应用，同时也对思维和智力进行相应的锻炼。
作为示例，本书给出了常用的基本加密算法——DES和RSA算法的C语言程序。
本书主要供信息安全、网络工程、计算机科学与技术、通信工程等本科专业的高年级学生使用。
学习该课程的学生需要具备高等数学和线性代数的基础知识，同时应该掌握基本的编程技术和数据结构的基本知识。
通过对本课程的学习，学生可以掌握基本的密码学算法原理，对加／解密技术具备一定的实际应用能力。
为了便于学生学习和理解本课程，我们以结论性的方式在附录A中给出了学习密码学需要具备的数论基础知识。
对于已经具备相关数论知识的学生，这一部分内容可以作为了解内容；对于不具备相关数论基础知识的学生，这一部分内容可以作为自学内容。
本书计划课时为48～64学时，其中对密码学基础知识的介绍大约需要48学时，具有扩展性的知识用*号给出了标记。
在讲授本书的过程中，建议根据课时量和授课对象来选择和组织相关内容。

第一图书网, tushu007.com

内容概要

本书系统地介绍了密码学的基本原理、基本算法，并对算法的安全性进行了相应的分析。主要内容包括古典密码、分组密码、序列密码、Hash函数、公钥密码、数字签名、密钥管理和计算复杂性等。

本书主要供信息安全、网络工程、计算机科学与技术、通信工程等本科专业的 高年级学生使用，也可供相关专业的教学、科研和工程技术人员参考。

<<密码学基础>>

书籍目录

第1章古典密码1.1密码学的基本概念1.2几种典型的古典密码体制1.2.1棋盘密码1.2.2移位密码1.2.3代换密码1.2.4维吉尼亚密码1.2.5仿射密码1.2.6置换密码1.2.7Hill密码1.3古典密码的统计分析习题第2章分组密码2.1分组密码的设计准则2.1.1Feistel分组密码的基本结构2.1.2F函数的设计准则2.2数据加密标准——DES2.2.1DES的描述2.2.2DES的分析2.2.3多重DES2.3高级数据加密标准——AES2.3.1AES的描述2.3.2AES的分析2.4国际数据加密标准——IDEA2.5RCS算法2.6分组密码的安全性及工作模式2.6.1分组密码的安全性2.6.2分组密码的工作模式习题第3章序列密码3.1序列密码的基本原理3.1.1序列密码的设计思想3.1.2序列随机性能评价3.2反馈移位寄存器3.2.1线性反馈移位寄存器3.2.2LFSR输出序列的周期与随机性3.3基于LFSR的密钥流生成器3.4非线性反馈移位寄存器习题第4章Hash函数4.1Hash函数与随机预言模型4.1.1Hash函数4.1.2随机预言模型4.2迭代Hash函数4.3MD4.3.1MD44.3.2MD54.4SHA-14.5MD5与SHA-1的比较4.6消息认证码(MAC)4.6.1基于分组密码的MAC4.6.2基于序列密码的MAC习题第5章公钥密码5.1公钥密码体制的基本原理5.1.1公钥密码的基本思想5.1.2公钥密码算法应满足的要求5.2背包算法5.2.1背包问题5.2.2背包算法的描述5.2.3背包算法的安全性5.3RSA算法5.3.1RSA算法的描述5.3.2RSA算法的安全性5.3.3RSA算法的参数选择5.4Rabin算法5.4.1求解数模下的平方根问题5.4.2Rabin算法描述5.4.3Rabin算法的修正5.5ElGamal算法5.5.1离散对数问题5.5.2ElGamal算法的描述5.5.3ElGamal算法的安全性5.6椭圆曲线算法5.6.1椭圆曲线的定义与性质5.6.2椭圆曲线算法的描述5.6.3椭圆曲线算法的特性习题第6章数字签名6.1数字签名的基本原理6.1.1数字签名的基本概念6.1.2数字签名的特性6.1.3数字签名的实现方法6.2RSA数字签名6.2.1RSA数字签名算法6.2.2RSA数字签名算法的安全问题6.3Rabin数字签名6.3.1Rabin数字签名算法6.3.2Rabin数字签名算法的安全问题6.4ElGamal数字签名6.4.1ElGamal数字签名算法6.4.2针对ElGamal数字签名算法的可能攻击6.5数字签名标准——DSS6.5.1DSS的数字签名算法6.5.2DSA算法的安全问题6.6不可否认的签名习题第7章密钥管理7.1密钥管理的生命周期7.2单钥体制的密钥管理7.2.1密钥的分类7.2.2密钥分配的基本方法7.2.3层次式密钥控制7.2.4分布式密钥控制7.3公钥体制的密钥管理7.3.1公开密钥的分发7.3.2用公钥加密分配单钥体制的会话密钥7.3.3Diffie-Hellman密钥交换与中间人攻击7.4秘密共享7.4.1Lagrange插值多项式门限方案7.4.2矢量门限方案7.4.3高级门限方案7.4.4有骗子情况下的密钥共享方案习题第8章计算复杂性8.1确定性多项式时间8.1.1算法效率分析8.1.2问题的难度8.2非确定多项式时间8.3概率多项式时间8.4多项式时间不可区分性习题附录A数论基础A.1素数与互素A.2同余与模运算A.3欧拉(Euler)定理A.4几个有用的算法A.5中国剩余定理A.6模为素数的二次剩余A.7Zp上的离散对数附录BDES算法程序源代码附录CRSA算法程序源代码参考文献

章节摘录

第1章　古典密码　　古典密码（Classical Cipher)是现代密码的基础。
本章在简要介绍密码学基本概念的基础上，介绍一些典型和古典密码体制，通过对古典密码学进行分析，给出密码分析学的基本概念和原理。
1.1　密码学的基本概念　　密码学有着悠久而神秘的历史，人们很难对密码学的起始时间给出准确的定义。
一般认为人类对密码学的研究与应用已经有几千年的历史，该学科一直广泛应用于军事领域。
密码学正式一门科学的理论基础应该首推1949年美国科学家Shannon的一篇文章《保密通信的信息理论》，他在研究保密机的基础上，蝗出了将密码建立在解某个已知数学难题基础上的观点。
20世纪70年代，以公钥密码体制的提出和数据加密标准DES的问世为标志，现代密码学开始蓬勃发展。
随着计算机技术和网络技术的发展，互联网的普及和网上业务的大量开展，人们更加关注密码学，更加依赖密码技术。
保密是密码学的核心。
密码学的基本目的是面对攻击者Oscar,在被称为Alice和Bob的通信双方之间应用不安全的信道进行通信时，设法保证通信安全。
密码学研究对通信双方要传输的信息进行何种保密变换以防止未被授权的第三方对信息的窃取。
此外，密码技术还可以用来进行信算鉴别、数据完整性检验、数字签名等。
在通信过程中，Alice和Bob也分别被称为信息的发送方和接收方。
Alice要发送给Bob的信息称为明文（Plaintext）。

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