<<应用密码学>>

图书基本信息

书名：<<应用密码学>>

13位ISBN编号：9787560623450

10位ISBN编号：756062345X

出版时间：2009-12

出版时间：西安电子科技大学出版社

作者：张仕斌 等 著

页数：267

前言

21世纪以来，随着信息化在全球的快速发展，信息系统及其运行的安全性与社会经济发展和公众利益的关系越来越密切；同时，传统的社会活动不断向网络空间延伸扩展，网络空间中的竞争与对抗越来越尖锐、复杂。
这些因素已经构成了重要的国家安全问题，关系到一个国家的政治、经济、文化、科技和国防安全。

密码技术是信息安全技术的内核和基石，这方面的任何重大进展，都有可能改变信息安全技术的走向。
同时，密码技术的技巧和方法自始至终深刻影响着整个信息安全技术界的发展和突破。
密码技术作为信息安全技术的核心，在保障网络信息安全的应用中具有重要的意义，而对典型密码学算法的掌握又是快速实现信息安全的捷径。

本书是作者结合自身多年的教学和科研工作实践经验、在广泛调研和充分论证并参考众多国内外有关网络信息安全和应用密码学文献的基础上，通过教学实践，为高等院校信息安全、密码学、应用数学、通信工程、计算机、电子商务等相关专业的本科生和研究生编写的一本专业教材。
在本书的编写中，始终遵循这样一个目标：为网络与信息安全领域提供一本既可以作为教学用书，也可以作为专业技术人员参考书的实用教材。

作者力求本书能体现以下特色：　　★先进性：本书给出一些具有代表性而且比较重要的例子，描述了当前及未来具有很强应用前景的对称密码体制与非对称密码体制在密码芯片、移动通信、电子商务和工业等领域中的应用，以及典型的密码算法的应用（如数字签名、身份识别和电子货币等）。

★易学性：在内容安排上力求深入浅出、条理清晰，尽量使各章内容相互独立，以便读者学习时可以跳过自己不需要的章节，而不影响其它章节的理解。

★实用性：在讲述应用密码学基本概念、基本理论之前，介绍了与密码学基本理论、基本概念相关的数论知识，弥补了其它密码学专著忽略密码学相关数学知识的不足。
通过阅读本书，读者可以对密码学涉及到的所有数学知识有一个比较全面的了解，有助于加深读者对密码学的理解。

★典型性：通过必要的实例和典型密码算法的基本工作原理及其应用方法对密码学进行较系统、深入的介绍，密码算法的选取和例题设置等方面都体现出广泛的代表性和典型性，为读者快速掌握和应用密码学的核心概念、方法与技术提供了便利。

★实践性：本书的附录部分是密码学算法应用的课程设计，通过课程设计的实践既增强了学生对密码算法的理解与掌握，同时也锻炼了他们将实践与理论相结合的能力。

本书的编排从教学适用性出发，特别重视读者对应用密码学知识的系统理解和有针对性地重点掌握关键内容；在体系结构、语言表达、内容选取和应用举例等方面都做了特别的考虑，因此本书也适于自学。

<<应用密码学>>

内容概要

《应用密码学》是作者在多年的教学与科研实践的基础上，按照高等院校的培养目标和基本要求，为实施教学改革，使密码学技术面向应用实践，而编写的一本应用密码学技术基础教材。《应用密码学》在全面讲解密码学基本知识和阐述密码理论的同时，还介绍了大量的算法，阐述了部分算法的安全性以及密码学发展的新方向；为了强化密码算法的理解、掌握与应用，《应用密码学》还介绍了一些典型密码算法的应用以及密码算法的课程设计；每章后都配有相应的习题以实现学与练的统一。

全书共11章，主要内容包括密码学基础知识、古典密码、对称密码、序列密码、非对称密码、Hash函数、数字签名、身份认证技术、密钥管理技术、密码学的新方向、密码学的应用等。《应用密码学》内容丰富详实、构思新颖、突出适用，既可作为普通高等院校信息安全、密码学、应用数学、通信工程、计算机、电子商务等相关专业的本科生或研究生的教学用书，也可作为相关领域技术人员的参考书。

<<应用密码学>>

书籍目录

第1章 绪论1.1 信息安全概述1.2 信息安全模型1.3 密码学在信息安全中的作用1.4 密码学的基本知识1.4.1 密码学的发展简史1.4.2 密码学的基本概念1.4.3 保密通信模型1.4.4 密码体制的构成及其分类1.5 密码体制的安全性1.5.1 密码分析1.5.2 密码体制的安全性习题1第2章 古典密码体制2.1 古典密码学中的基本运算2.1.1 代替密码2.1.2 换位密码2.1.3 转轮机2.2 隐写术2.3 移位密码技术2.4 仿射密码技术2.5 维吉尼亚密码技术2.6 弗纳姆密码技术2.7 希尔密码技术2.8 古典密码体制的安全性分析2.8.1 移位密码安全性分析2.8.2 仿射密码安全性分析习题2第3章 分组密码体制3.1 分组密码概述3.2 分组密码的原理3.3 数据加密标准（DES）3.3.1 DES算法概述3.3.2 DES算法描述3.3.3 DES的各种变形算法3.4 高级加密标准（AES）3.4.1 算法中的数学基础知识3.4.2 AES算法描述3.4.3 基本运算3.4.4 基本变换3.4.5 密钥扩展3.4.6 解密过程3.4.7 具体实例3.5 SMS4密码算法3.5.1 SMS4描述3.5.2 算法流程3.5.3 密钥扩展算法3.5.4 具体实例3.6 其他典型的对称密码体制简介3.6.1 RC6对称密码体制3.6.2 Twofish对称密码体制3.7 对称密码体制的工作模式3.7.1 ECB电子码本模式3.7.2 CBC密码分组链接模式3.7.3 CFB密码反馈模式3.7.4 OFB输出反馈模式3.7.5 CTR计数器模式3.8 对称密码算法的应用习题3第4章 序列密码体制4.1 密码学中的随机数4.1.1 随机数的使用?：4.1.2 伪随机数产生器4.1.3 基于密码算法的随机数产生器4.1.4 伪随机数的评价标准4.2 序列密码的概念及模型4.3 线性反馈移位寄存器4.4 非线性序列简介4.5 常用的序列密码算法4.5.1 A5序列密码算法4.5.2 SEAL序列密码算法4.5.3 RC4序列密码算法习题4第5章 非对称密码体制5.1 概述5.2 数学基础5.2.1 中国剩余定理5.2.2 离散对数5.2.3 平方剩余5.2.4 勒让得符号5.2.5 素数的产生5.2.6 椭圆曲线5.2.7 有限域上的椭圆曲线5.3 非对称密码体制概述5.3.1 非对称密码体制的原理5.3.2 非对称密码体制的设计准则5.3.3 非对称密码体制的分类5.4 RSA密码算法5.4.1 RSA发展简史5.4.2 RSA算法描述5.4.3 RSA算法举例5.4.4 RSA算法的安全性及常用攻击5.4.5 RSA算法的实现5.5 ElGamal密码算法5.5.1 ElGamal算法描述5.5.2 ElGamal算法举例5.5.3 ElGamal算法的常用攻击5.6 椭圆曲线密码体制5.6.1 椭圆曲线密码体制简介5.6.2 椭圆曲线上的Eli3amal密码体制5.6.3 算法举例5.7 RSA、ElGamal及椭圆曲线密码比较5.8 其他非对称密码体制简介习题5第6章 认证理论与技术——Hash函数6.1 认证与认证系统6.2 散列算法概述6.2.1 散列算法的概念及结构6.2.2 散列算法的发展现状6.3 Hash散列算法6.3.1 MD5散列算法6.3.2 SHA-1散列算法6.3.3 Hash散列算法的应用6.4 散列算法的攻击现状6.4.1 生日悖论问题6.4.2 生日攻击6.5 消息认证6.5.1 消息认证的基本概念6.5.2 HMAC6.5.3 消息认证的应用习题6第7章 认证理论与技术—— 数字签名7.1 数字签名概述7.2 数字签名的原理及分类7.2.1 数字签名的原理7.2.2 数字签名的分类7.3 数字签名算法7.3.1 RSA数字签名7.3.2 ElGamal数字签名7.4 数字签名标准（DSS）7.4.1 DSA的描述7.4.2 DSA举例7.5 其他专用数字签名方案7.6 盲签名方案7.6.1 基于整数分解难题的盲签名7.6.2 基于离散对数难题的盲签名7.6.3 盲签名的应用习题7第8章 认证理论与技术——身份认证技术8.1 认证模型及认证协议8.1.1 认证及认证模型8.1.2 认证协议8.2 身份认证技术8.2.1 口令认证技术8.2.2 IC卡认证技术8.2.3 个人特征识别技术8.3 基于零知识证明的身份认证技术8.3.1 零知识证明基本概念8.3.2 基于零知识的身份认证技术8.4 Kerberos身份认证技术8.4.1 Kerberos身份认证技术简介8.4.2 Kerberos的工作原理8.4.3 Kerberos域间的认证8.5 X.5 09认证技术8.5.1 数字证书8.5.2 X.5 09认证过程习题8第9章 密钥管理技术9.1 密钥管理概述9.2 密钥的结构和分类9.2.1 密钥的结构9.2.2 密钥的分类9.3 密钥管理9.4 密钥托管技术9.4.1 密钥托管技术简介9.4.2 密钥托管系统的组成9.5 密钥协商与密钥分配9.5.1 密钥协商9.5.2 密钥分配9.5.3 PKI技术简介习题9第10章 密码学的新方向10.1 量子密码学10.1.1 量子密码学简介10.1.2 量子密码学原理10.1.3 量子密钥分配协议10.1.4 量子密码学面临的挑战及发展趋势10.2 基于混沌理论的密码体制10.2.1 混沌理论的基本概念10.2.2 混沌序列的产生及其随机序列10.2.3 混沌密码体制10.2.4 应用示例10.3 其他新密码体制简介习题10第11章 密码学的应用11.1 密码学在电子商务中的应用11.1.1 电子商务系统面临的安全威胁11.1.2 电子商务系统的安全需求11.1.3 电子商务的安全体系结构11.1.4 电子商务的交易协议11.2 密码学在数字通信中的应用11.2.1 第三代移动通信系统（3G）安全特性与机制11.2.2 WiMAX无线网域安全问题11.3 密码学在工业网络控制中的应用习题11附录应用密码学课程设计参考文献

章节摘录

1）计算机所面临的主要安全威胁　　随着个人计算机的普及，个人计算机也已成为黑客攻击的目标之一，就其安全威胁而言，主要涉及以下几个方面。

（1）计算机病毒：是当前最常见、最主要的威胁，几乎每天都有计算机病毒产生。

计算机病毒的主要危害体现在破坏计算机文件和数据，导致文件无法使用，系统无法启动；消耗计算机CPU、内存和磁盘资源，导致一些正常服务无法进行，出现死机、占用大量的磁盘空间；有的还会破坏计算机硬件，导致计算机彻底瘫痪。

（2）木马：是一种基于远程控制的黑客工具，也称为“后门程序”。

木马作为一种远程控制的黑客工具，主要危害包括窃取用户信息（比如计算机或网络账户和密码、网络银行账户和密码、QQ账户和密码、E-mail账户和密码等），携带计算机病毒（造成计算机或网络不能正常运行，甚至完全瘫痪），或被黑客控制，攻击用户计算机或网络。

（3）恶意软件：是指一类特殊的程序，是介于计算机病毒与黑客软件之间的软件的统称。

它通常在用户不知晓也未授权的情况下潜入系统，具有用户不知道（一般也不许可）的特性，激活后将影响系统或应用的正常功能，甚至危害或破坏系统。

其主要危害体现在非授权安装（也被称为“流氓软件”）、自动拨号、自动弹出各种广告界面、恶意共享和浏览器窃持等。

当前，恶意软件的出现、发展和变化给计算机及网络系统带来了巨大的危害。

2）网络所面临的主要安全威胁　　相对于个人计算机而言，网络所面临的安全威胁除具有计算机所面临的三种常见的威胁之外，主要是由于网络的开放性、网络自身固有的安全缺陷和网络黑客的入侵与攻击（人为的因素）等三个方面带来的安全威胁。

（1）网络的开放性：主要表现为由于网络业务都是基于公开的协议、连接的建立是基于主机上彼此信任的原则和远程访问，因而使得各种攻击无需到现场就能成功。

正是由于网络的开放性，使得在虚幻的计算机网络中网络犯罪往往十分隐蔽，虽然有时会留下一些蛛丝马迹，但更多的时候是无迹可寻。

（2）网络自身固有的安全缺陷：这是网络安全领域首要关注的问题，发现系统漏洞（安全缺陷）也是黑客进行入侵和攻击的主要步骤。

据调查，国内80%以上的网站存在明显的漏洞。

漏洞的存在给网络上的不法分子的非法入侵提供了可乘之机，也给网络安全带来了巨大的风险。

据美国CERT／CC统计，2006年总共收到系统漏洞报告8064个，平均每天超过22个（自1995年以来，漏洞报告总数已经达到30780个）。

这些漏洞的存在对广大互联网用户的系统造成了严重的威胁。

当前，操作系统的漏洞是我们面临的最大风险。

比如，Windows操作系统是目前使用最为广泛的系统，但经常发现存在漏洞。

过去Windows操作系统的漏洞主要被黑客用来攻击网站，对普通用户没有多大影响，但近年来一些新出现的网络病毒利用Windows操作系统的漏洞进行攻击，能够自动运行、繁衍、无休止地扫描网络和个人计算机，然后进行有目的的破坏。

比如“红色代码”、“尼姆达”、“蠕虫王”以及“冲击波”等。

随着Windows操作系统越来越复杂和庞大，出现的漏洞也越来越多，利用windows操作系统漏洞进行攻击造成的危害越来越大，甚至有可能给整个互联网带来不可估量的损失。

版权说明