21世纪 高等学校信息安全专业规划教材

密码学原理及应用技术

(第2版)

张健 任洪娥 陈宇 编著

清华大学出版社

21世纪高等学校信息安全专业规划教材

密码学原理及应用技术

（第2版）

张　健　任洪娥　陈　宇　编著

清华大学出版社
北京

内 容 简 介

密码学技术是网络安全和信息安全中的关键技术，其主要目标是实现保密性、完整性和不可否认性。本书介绍了密码算法及其在诸多方面的应用，内容包括分组密码体制、公钥密码体制、序列密码体制等算法以及密码学在网络安全、电子邮件、电子商务和图像加密中的应用等。全书语言简练，通俗易懂，重点突出。

本书是作者在多年教学和科研工作基础上形成的，可以作为高等学校计算机、通信工程、信息安全等专业的本科生和硕士生教材，也可以供从事相关领域的研究人员及工程技术人员参考。

图书在版编目(CIP)数据

密码学原理及应用技术/张健，任洪娥，陈宇编著. --2 版. --北京：清华大学出版社，2014
21 世纪高等学校信息安全专业规划教材
ISBN 978-7-302-35245-7

Ⅰ. ①密…　Ⅱ. ①张… ②任… ③陈…　Ⅲ. ①密码－理论－高等学校－教材　Ⅳ. ①TN918.1

中国版本图书馆 CIP 数据核字(2014)第 014273 号

责任编辑：郑寅堃　薛　阳
封面设计：杨　兮
责任校对：焦丽丽
责任印制：沈　露

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954
印 装 者：北京嘉实印刷有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　印　　张：12.75　　字　　数：309 千字
版　　次：2011 年 7 月第 1 版　2014 年 5 月第 2 版　　印　　次：2014 年 5 月第1 次印刷
印　　数：1～2000
定　　价：25.00 元

产品编号：056916-01

出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取、甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到了整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人才。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革，适应社会对信息安全人才的培养需求，教材内容坚持基本理论的扎实和清晰，反映基本理论和原理的综合应用，在其基础上强调工程实践环节，并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，在选择教材内容和编写体系时注意体现素质教育、创新能

力与实践能力的培养,为学生知识、能力、素质协调发展创造条件。

(3) 实施精品战略,突出重点。规划教材建设把重点放在专业核心(基础)课程的教材建设上;特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版,逐步形成精品教材;提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

(4) 支持一纲多本,合理配套。专业核心课和相关基础课的教材要配套,同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化,基本教材与辅助教材、教学参考书,文字教材与软件教材的关系,实现教材系列资源的配套。

(5) 依靠专家,择优落实。在制定教材规划时依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时,要引入竞争机制,通过申报、评审确定主编。书稿完成后认真实行审稿程序,确保出书质量。

繁荣教材出版事业,提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量,希望有志于教材建设的教师能够加入到我们的编写队伍中来。

21世纪高等学校信息安全专业规划教材

联系人:魏江江 weijj@tup.tsinghua.edu.cn

前　言

随着通信和计算机技术的快速发展以及经济全球化应用的推动，互联网表现出了极大的使用方便性和信息传递的快捷性，这使得人们对信息网络的依赖程度越来越大。人们在传递信息的同时，信息的安全性自然成为所关心的重要问题。

密码学作为实现网络信息安全的核心技术，在保障网络信息安全的应用中具有重要意义。

作者根据多年教学经验和科研经验，在学习和总结国内外相关文献的基础上，完成了本书的撰写工作。

本书对第1版中的错误之处进行了修订，同时增加了对密码算法的安全分析，在很多的细节部分进行了完善。本书的特色是用通俗易懂的语言，对密码学的基本概念和基本原理进行准确阐述，并配合适当的例题进行深入研究。同时力图反映出密码学应用方面的一些新进展，包括密码学在网络、电子邮件、电子商务以及图像加密上的应用。

全书共分为13章，第1章至第8章的主要内容是密码学的基本原理及其算法；第9章至第13章是密码学在其他领域的应用。

第1章主要介绍密码学的基本概念及发展历史；第2章对古典密码的相关理论做了介绍；第3章详细介绍了密码学所用到的数字基础知识；第4章对经典的分组加密体制DES做了详细的分析，同时介绍了目前的加密标准AES；第5章对非对称密码体制RSA和椭圆密码体制做了细致的分析；第6章介绍了序列密码的相关内容；第7章介绍了数字签名的原理及基本算法；第8章对密钥的安全管理做了分析。

第9章是密码学在网络安全及无线网络中的应用；第10章是密码学在图像加密中的应用；第11章是密码学在智能IC卡上的应用；第12章是密码学在电子邮件上的应用；第13章是密码学在电子商务上的应用。

本书第1～3章由任洪娥编写，第8、第9章由陈宇编写，张健负责其余章节的编写和全书的统稿。

为配合本课程的教学需要，本教材为教师配有习题参考答案，可发E-mail(ZhengYK@tup.tsinghua.edu.cn)联系索取。

作者要特别感谢参考文献中所列各位作者,是他们的独到见解为本书提供了宝贵的资料及丰富的写作源泉。限于作者的水平和学识,书中难免存在疏漏和错误之处,诚望读者不吝赐教,以便修正,让更多读者受益。

最后,谨向每一位关心和支持本书编写工作的各方面人士表示感谢!

作 者

2013年10月

目　录

第1章　密码学概述

随着计算机网络的不断发展，全球信息化已成为人类发展的大趋势。但由于计算机网络具有联结形式多样性、终端分布不均匀性和网络的开放性、互联性等特征，致使网络易受黑客、怪客、恶意软件和其他攻击，所以网络上信息的安全和保密是一个至关重要的问题。对于军用的自动化指挥网络和银行等传输敏感数据的计算机网络系统而言，其信息的安全和保密尤为重要。在众多安全方法中，密码学是非常重要的一个保密措施。

1.1　密码学与网络信息安全

1.1.1　网络信息安全

网络必须有足够强的安全措施，否则网络将是个无用、甚至会危及国家安全的网络。无论是在局域网还是在广域网中，都存在着自然和人为等诸多因素的脆弱性和潜在威胁。故此，网络的安全措施应能全方位地针对各种不同的威胁和脆弱性，这样才能确保网络信息的保密性、完整性和可用性。

1. 网络安全的含义

网络安全就是网络上的信息安全，涉及的领域很广。网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因为偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断，包括以下含义。

(1) 网络运行系统安全；

(2) 网络上系统信息的安全；

(3) 网络上信息传播的安全，即信息传播后果的安全；

(4) 网络上信息内容的安全。

网络安全具有以下5个要素。

(1) 可用性，授权实体有权访问数据；

(2) 机密性，信息不暴露给未授权实体或进程；

(3) 完整性，保证数据不被未授权修改；

(4) 可控性，控制授权范围内的信息流及操作方式；

(5) 可审查性，对出现的安全问题提供依据与手段。

网络安全的内容如下。

(1) 物理安全；

(2) 网络安全；

(3) 传输安全；

(4) 应用安全；

(5) 用户安全。

2. 网络信息面临的威胁

计算机网络所面临的威胁大体可分为两种。一是对网络中信息的威胁；二是对网络中设备的威胁。影响计算机网络的因素很多，有些因素可能是有意的，也可能是无意的；可能是人为的，也可能是非人为的；可能是外来黑客对网络系统资源的非法使用。归结起来，针对网络安全的威胁主要有三个方面。

(1) 人为的无意失误。如操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的账号随意转借他人或与别人共享等都会给网络安全带来威胁。

(2) 人为的恶意攻击。这是计算机网络所面临的最大威胁，敌手的攻击和计算机犯罪就属于这一类。此类攻击又可以分为以下两种。一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；另一类是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄露。

(3) 网络软件的漏洞和“后门”。网络软件不可能是百分之百无缺陷和无漏洞的，然而，这些漏洞和缺陷恰恰是黑客进行攻击的首选目标，曾经出现过黑客攻入网络内部的事件，这些事件大部分就是因为安全措施不完善所招致的苦果。另外，软件的“后门”都是软件公司的设计编程人员为了自便而设置的，一般不为外人所知，但一旦“后门”打开，其造成的后果将不堪设想。

3. 主要攻击与威胁手段

(1) DoS。使目标系统或网络无法提供正常服务。DoS(Denial of Service)，也就是“拒绝服务”的意思。最基本的DoS攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务，如图1-1所示。基本过程是：首先攻击者向服务器发送众多的带有虚假地址的请求，服务器发送回复信息后等待回传信息，由于地址是伪造的，所以服务器一直等不到回传的消息，分配给这次请求的资源就始终不能被释放。在这种反复发送伪地址请求的情况下，服务器资源最终会被耗尽。

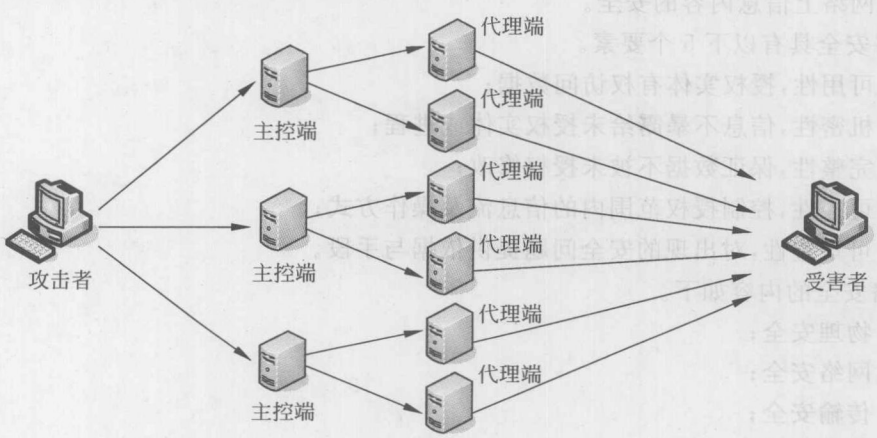

图1-1 DoS攻击

(2) 扫描探测。系统弱点探察。

(3) 口令攻击。弱口令。

(4) 获取权限,提升权限。猜/crack root 口令、缓冲区溢出、利用 NT 注册表、访问和利用高权限控制台、利用启动文件、利用系统或应用 Bugs。

(5) 插入恶意代码。病毒、特洛伊木马(BO)、后门、恶意 Applet。

(6) 网络破坏。主页篡改、文件删除、毁坏 OS、格式化磁盘。

(7) 数据窃取。敏感数据拷贝、监听敏感数据传输——共享媒介/服务器监听/远程监听 RMON。

(8) 伪造、浪费与滥用资源。

(9) 篡改审计数据。删除、修改、权限改变、使审计进程失效。

(10) 安全基础攻击。防火墙、路由、账户修改,文件权限修改。

1.1.2　密码学在网络信息安全中的作用

在现实世界中,安全是一个相当简单的概念。例如,房子门窗上要安装足够坚固的抗变形材料以阻止窃贼的闯入;安装报警器是阻止入侵者破门而入的进一步措施;当有人想从他人的银行账户骗取钱款时,出纳员会要求其出示相关身份证明也是为了保证存款安全;签署商业合同时,需要双方在合同上签名以产生法律效力也是保证合同的实施安全。

在数字世界中,安全以类似的方式工作着。机密性就像大门上的锁,它可以阻止非法者闯入用户的文件夹读取用户的敏感数据或盗取钱财。数据完整性提供了一种当某些内容被修改时,可以使用户得知的机制,相当于报警器。这些思想是密码技术在保护信息安全方面所起作用的具体体现。

密码是一门古老的技术,但自密码技术诞生直至第二次世界大战结束,对于公众而言,密码技术始终处于一种未知的保密状态,常与军事、机要、间谍等工作联系在一起,让人在感到神秘之余,又有几分畏惧。信息技术的迅速发展改变了这一切,随着计算机和通信技术的迅猛发展,大量的敏感信息常通过公共通信设施或计算机网络进行交换,特别是 Internet 的广泛应用、电子商务和电子政务的迅速发展,越来越多的个人信息需要严格保密,如银行账号、个人隐私等。正是这种对信息的机密性和真实性的需求,密码学才逐渐揭去了神秘的面纱,走进公众的日常生活中。

密码技术是实现网络信息安全的核心技术,是保护数据最重要的工具之一。通过加密变换,将可读的文件变换成不可理解的乱码,从而起到保护信息和数据的作用,它直接支持机密性、完整性和非否认性。

今天,在计算机被广泛应用的信息时代,由于计算机网络技术的迅速发展,大量信息以数字形式存放在计算机系统里,信息的传输则通过公共信道。这些计算机系统和公共信道在不设防的情况下是很脆弱的,容易受到攻击和破坏,信息的失窃不容易被发现,而后果可能是极其严重的。如何保护信息的安全成为许多人感兴趣的迫切话题,作为网络安全基础理论之一的密码学引起了人们的极大关注,吸引着越来越多的科技人员投入到密码学领域的研究之中。

密码学尽管在网络信息安全具有举足轻重的作用,但密码学绝不是确保网络信息安全的唯一工具,它也不能解决所有的安全问题。同时,密码编码与密码分析是一对矛盾的关

系,它们在发展中始终处于一种动态平衡。

1.2 密码学的基本概念

密码学(cryptology)是研究密码系统或通信安全的一门科学。它主要包括两个分支,即密码编码学和密码分析学。密码编码学的主要目的是寻求保证消息保密性或认证性的方法。密码分析学的主要目的是研究加密消息的破译或消息的伪造。

采用密码技术可以隐蔽和保护需要保密的消息,使未授权者不能提取信息,这其中包含如下一些基本概念。

明文。被隐蔽的消息称做明文(plaintext)。

密文。隐蔽后的消息称做密文(ciphertext)或密报(cryptogram)。

加密。将明文变换成密文的过程称做加密(encryption)。

解密。由密文恢复出原明文的过程称做解密(decryption)。

密码员。对明文进行加密操作的人员称做密码员或加密员(cryptographer)。

加密算法。密码员在对明文进行加密时,采用的一组规则称做加密算法(Encryption Algorithm)。

接收者。传送消息的预定对象称做接收者(receiver)。

解密算法。接收者在对密文进行解密时,采用的一组规则称做解密算法(Decryption Algorithm)。

加密密钥和解密密钥。加密算法和解密算法的操作通常是在一组密钥(key)的控制下进行的,分别称为加密密钥(Encryption Key)和解密密钥(Decryption Key)。

密码体制分类。根据密钥的特点将密码体制分为对称和非对称密码体制(Symmetric Cryptosystem and Asymmetric Cryptosystem)两种。

对称密码体制又称单钥(one-key)或私钥(Private Key)或传统(classical)密码体制。非对称密码体制又称双钥(two-key)或公钥(Public Key)密码体制。

在私钥密码体制中,加密密钥和解密密钥是一样的或者彼此之间是容易相互确定的。在私钥密码体制中,按加密方式又将私钥密码体制分为流密码(Stream Cipher)和分组密码(Block Cipher)两种。

在流密码中将明文消息按字符逐位地进行加密。在分组密码中将明文消息分组(每组含有多个字符),逐组地进行加密。

在公钥密码体制中,加密密钥和解密密钥不同,从一个难于推出另一个,可将加密能力和解密能力分开。

截收者。在消息传输和处理系统中,除了合法的接收者外,还有非授权者。他们通过各种办法,如搭线窃听、电磁窃听、声音窃听等来窃取机密信息,称其为截收者(eavesdropper)。

密码分析。虽然不知道系统所用的密钥,但通过分析可能从截获的密文推断出原来的明文,这一过程称做密码分析(cryptanalysis)。从事这一工作的人称做密码分析员或密码分析者(cryptanalyst)。

被动攻击。对一个密码系统采取截获密文进行分析,这类攻击称做被动攻击(Passive