中国计算机学会
学术著作丛书

密码学与计算机网络安全

卿斯汉 著

清华大学出版社
广西科学技术出版社

中国计算机学会学术著作丛书

密码学与计算机网络安全

卿斯汉 著

清华大学出版社
广西科学技术出版社

(京)新登字 158 号

内 容 简 介

本书是一部关于密码学和计算机网络安全的专著。全书共分 16 章，全面介绍了密码学和计算机网络安全的基本理论和关键技术。主要内容包括：密码学的基本概念，传统密码学，公开钥密码学，分组密码、序列密码以及 Rabin 密码、概率加密密码、量子密码等，IDEA 算法、美国 AES 候选算法、欧洲密码计划 NESSIE 候选算法，数字签名，密码协议，零知识证明技术，认证协议、BAN 逻辑、SVO 逻辑以及 BAN 类逻辑的形式化分析，黑客攻击分析，入侵检测，防止修改主页，防火墙，网络监视系统，安全电子邮件系统和安全操作系统等。

本书题材广泛，内容新颖，深入浅出，实例丰富，包括密码学和计算机网络安全领域的最新研究成果，同时也包括了作者近年来的科研成果。

本书可供计算机、信息、通信、密码、数学等专业的工程技术人员和高等院校相关专业师生参考。

书　名：密码学与计算机网络安全
作　者：卿斯汉　著
出版者：清华大学出版社　广西科学技术出版社
（北京清华大学学研大厦，邮编 100084）
http：// www. tup. tsinghua. edu. cn
印刷者：清华大学印刷厂
发行者：新华书店总店北京发行所
开　本：787×1092 1/16　**印张**：17.5　**字数**：411 千字
版　次：2001 年 7 月第 1 版　2001 年 7 月第 1 次印刷
书　号：ISBN 7-302-04379-5/TP・2571
印　数：0001～5000
定　价：28.00 元

序

信息化和网络化是当今世界经济与社会发展的大趋势，也是推进我国国民经济和社会现代化的关键环节。信息资源的深入开发利用以及政府管理、企业生产经营、社会公共服务、金融财税等的信息化、网络化已在全国迅猛展开；全社会广泛应用信息技术，计算机与网络应用的普及和提高，为人们普遍关注。与此同时，由于计算机网络所具有的开放性与共享性，其安全性也成为人们日益关切的问题。在世界范围内，对计算机网络的攻击手段层出不穷，网络犯罪日趋严重。在一些网络应用发展较快的国家，都已遭受到很大威胁和损失。我国信息化、网络化建设在技术与装备上对别国的极大依赖性，使网络安全问题尤为突出。因此，增强全社会安全意识，普及计算机网络安全教育，提高计算机网络安全技术水平，促进计算机网络安全的自主研发创新，改善计算机网络的安全状况，实为当务之急。

本书作者卿斯汉教授长期从事信息安全科研工作，是我国著名的信息安全专家，在信息安全领域具有深厚的学术造诣。本书着重从密码学与计算机网络安全两方面立论，密码学是计算机网络安全的基础，而计算机网络安全的内容涵盖尤广，二者紧密结合，可使读者对计算机网络安全有一个清晰完整的概念。

对密码学，本书全面介绍传统密码学、公开钥密码学、分组密码、序列密码、量子密码、数字签名、密码协议、零知识证明技术等内容，并对 20 世纪末密码学的重大事件（如美国 AES 候选算法、欧洲密码大计划－NESSIE 等）作了介绍和评述。

在计算机网络安全方面，本书以较大篇幅阐明认证协议、BAN 类逻辑及其形式化分析、黑客攻击、入侵检测、防火墙、网络监视系统、安全电子邮件系统、安全操作系统等重要内容，并特别强调了计算机网络安全体系的重要性，着重指出：没有整体安全设计和安全部署，即无计算机网络安全可言，这一观点很值得从事计算机网络安全工作者的重视。

这本专著的撰写前后历时 5 年有余，反映了密码学和计算机网络安全的新发展和新趋势，并结合作者的最新科研成果，是一部符合时代需求的佳作。我深信，本书的出版，必将对我国信息化、网络化事业产生积极影响并作出重要贡献。

中国科学院院士

张效祥

2001 年 4 月

序　　言

计算机是当代发展最为迅猛的科学技术，其应用几乎已深入到人类社会活动和生活的一切领域，大大提高了社会生产力，引起了经济结构、社会结构和生活方式的深刻变化和变革，是最为活跃的生产力之一。计算机本身在国际范围内已成为年产值达2500亿美元的巨大产业，国际竞争异常剧烈，预计到本世纪末将发展为世界第一大产业。计算机科技具有极大的综合性质，与众多科学技术相交叉而反过来又渗入更多的科学技术，促进它们的发展。计算机科技内容十分丰富，学科分支生长尤为迅速，日新月异，层出不穷。因此在我国计算机科技尚比较落后的情况下，加强计算机科技的传播实为当务之急。

中国计算机学会一直把出版图书刊物作为学术活动的重要内容之一。我国计算机专家学者通过科学实践，做出了大量成果，积累了丰富经验与学识。他们有撰写著作的很大积极性，但相当时期以来计算机学术著作由于印数不多，出版往往遇到不少困难，专业性越强越有深度的著作，出版难度越大。最近清华大学出版社与广西科学技术出版社为促进我国计算机科学技术及产业的发展，推动计算机科技著作的出版工作，特设立“计算机学术著作出版基金”，以支持我国计算机科技工作者撰写高水平的学术著作，并将资助出版的著作列为中国计算机学会的学术著作丛书。我们十分重视这件事，并已把它列为学会本届理事会的工作要点之一。我们希望这一系列丛书能对传播学术成果、交流学术思想、促进科技转化为生产力起到良好作用，能对我国计算机科技发展具有有益的导向意义，也希望我国广大学会会员和计算机科技工作者，包括海外工作和学习的神州学人们能积极投稿，出好这一系列丛书。

中国计算机学会

1992年4月20日

出版说明

近年来，随着微电子和计算机技术渗透到各个技术领域，人类正在步入一个技术迅猛发展的新时期。这个新时期的主要标志是计算机和信息处理的广泛应用。计算机在改造传统产业、实现管理自动化、促进新兴产业的发展等方面都起着重要作用，它在现代化建设中的战略地位愈来愈明显。计算机科学与其他学科的交叉又产生了许多新学科，推动着科学技术向更广阔的领域发展，正在对人类社会产生深远的影响。

科学技术是第一生产力。计算机科学技术是我国高科技领域的一个重要方面。为了推动我国计算机科学及产业的发展，促进学术交流，使科研成果尽快转化为生产力，清华大学出版社与广西科学技术出版社联合设立了“计算机学术著作基金”，旨在支持和鼓励科技人员，撰写高水平的学术著作，以反映和推广我国在这一领域的最新成果。

计算机学术著作出版基金资助出版的著作范围包括：有重要理论价值或重要应用价值的学术专著；计算机学科前沿探索的论著；推动计算机技术及产业发展的专著；与计算机有关的交叉学科的论著；有较大应用价值的工具书；世界名著的优秀翻译作品。凡经作者本人申请，计算机学术著作出版基金评审委员会评审通过的著作，将由该基金资助出版，出版社将努力做好出版工作。

基金还支持两社列选的国家高科技重点图书和国家教委重点图书规划中计算机学科领域的学术著作的出版。为了做好选题工作，出版社特邀请中国计算机学会、中国中文信息学会帮助做好组织有关学术著作丛书的列选工作。

热诚希望得到广大计算机界同仁的支持和帮助。

清华大学出版社
广西科学技术出版社
计算机学术著作出版基金办公室

1992 年 4 月

前　言

经过5年多的努力，这本书终于脱稿有望与读者见面了。自从与出版社签约5年来，因工作繁忙，未能静下心来一门心思地搞好本书的写作，故此拖拉至今，甚感有愧于出版社和广大读者的期待。现在，本书终于完成，不仅如释重负，而且有感于信息安全领域在这5年间的飞速发展，感慨良多。本书的前身是拙作"现代密码学引论"，写于1985年，我刚刚从美国作访问学者返回后不久。当时我应邀赴中国科学院成都计算机应用研究所讲学，全国各方面人士100余人踊跃参加，因此草草准备了一份讲义，约10万字。1986年，该讲义内部出版成书，此即为"现代密码学引论"。后来，该书成为若干所著名大学研究生的参考教材。

本书的基础虽然起源于该书，但做了大量的修改和增添。首先，密码学近年来飞速发展，特别是新的设计技术和新的分析技术不断涌现，以AES为代表，分组密码的设计和分析进入了一个新的时期；其次，密码学在计算机网络安全中的应用不断深入和发展。无论在安全电子邮件协议中，还是在VPN等有关应用中，都离不开密钥分配和密码算法。以密码学为基础的数字签名、密码协议更是应用范围广泛。认证协议、非否认协议、电子商务协议、PKI等，密码学在其中都起着举足轻重的作用。此外，计算机网络安全的领域越来越广，涉及操作系统安全、数据库管理系统安全、入侵检测、防火墙、安全Web服务器、智能卡安全系统、网络安全监视系统等各个方面。本书总结了作者亲自参与的第一线工作的若干成果，根据密码学和计算机网络安全的新发展和新趋势完成了本书的写作，希望将作者的一些体会与读者共享。

全书分为上下两篇，共16章。上篇是基础篇，主要讲述密码学，由1～10章组成，内容涉及：密码学的基本概念；传统密码学；公开钥密码学；分组密码、序列密码，以及Rabin密码、概率加密密码、量子密码等；数字签名；密码协议；零知识证明技术。此外，基础篇中还包括IDEA算法和美国AES候选算法等内容。最近出现的所谓"欧洲密码大计划"，亦即NESSIE(New European Schemes for Signatures, Integrity, and Encryption)密码计划，则在附录D中简要介绍。为使本书自成体系，在附录A、B和C中分别介绍了有关代数、计算复杂性理论和数论的有关基础知识，免去读者频繁查阅其他文献的麻烦。下篇是应用篇，主要介绍计算机网络安全，由11～16章组成，内容涉及：认证协议、BAN逻辑、SVO逻辑以及BAN类逻辑的形式化分析；黑客攻击分析；入侵检测；防止修改主页；防火墙；网络监视系统；安全电子邮件系统；安全操作系统等。

本书从写作到出版，都得到了中国科学院信息安全技术工程研究中心广大同仁的鼓励和支持。本书涉及的许多科研成果，是中心员工多年来共同努力的结晶，对此，作者特别感谢：倪惜珍研究员、冯登国研究员；吴文玲副研究员；刘文清、蒋建春、张磊、杨蕾、王贵林、贺也平等博士；赵晓亮、樊迟、周武、周典萃、张旺、司伟生等硕士。

在本书的写作和出版过程中，以及在作者长期从事信息安全的工作中，作者还得到张

效祥院士和肖国镇教授的一贯支持和帮助，作者在此表示深深的谢意。本书的出版得到清华大学出版社“计算机学术著作出版基金”的资助，同时还得到国家自然科学基金(60083007)和国家重点基础研究发展规划项目(G1999035810)的支持，在此表示感谢。作者也感谢清华大学出版社的责任编辑尹芳平编审为本书的顺利出版所付出的辛勤劳动。

本书面向相关专业的高年级本科生、硕士研究生和博士研究生，也可供广大教学、科研和工程技术人员参考。本书作者水平有限，不足之处恳请广大读者批评指正。

作者谨识于中国科学院信息安全技术工程研究中心

2000 年 12 月

目　　录

上篇　基　础　篇

下篇 应 用 篇

上　篇

基　礎　篇

第1章 引 论

1.1 计算机网络安全的基础——密码学

如果密码学还值得应用的话，就一定要用好它.

J. T. Martin

我们今天正处于密码学发生重大变革的时代.

W. Diffie 和 M. E. Hellman

突然，现代密码学从半军事的角落里解脱出来，一跃成为通信科学一切领域中的中心研究课题.

T. Beth

计算机网络与分布式系统的安全主要涉及高速电子信道中传输的数据和系统中存储的数据的安全问题，它包含两个主要内容：保密性，即防止非法地获悉数据；完整性，即防止非法地修改数据. 解决这个问题的基础是现代密码学.

如图 1.1 所示，两种形式的攻击威胁计算机网络通信的安全. 第一种是**被动窃听**(passive wiretapping)，通常系指非法搭线窃听，截取通信内容后进行密码分析，在计算机网络通信环境，这种攻击形式还可以用来监视网络通信的信号流，并确定通信双方的身份. 第二种是**主动窃听**(active wiretapping)，通常系指非法修改计算机网络中传输的报文，例如插入一条非法的报文、重发原先的报文、删除一条报文、修改一条报文，等等.

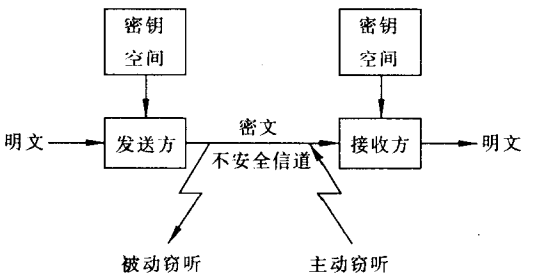

图 1.1 威胁计算机网络安全通信的两种形式

如图 1.2 所示，对于计算机系统中存储的数据有几种不同的安全威胁形式，**浏览**(browsing)系指通过搜索主存或输助存储器的方法非法获取数据，它类似于被动窃听，但二者之间有两个重大的差别：在计算机系统中存储的数据，其生命周期很长，因此，浏览比被动窃听构成的威胁更大；在被动窃听情形，无论能否访问系统，都无法防止对不安全信

道的这种形式的攻击. 在浏览情况下，仅当用户有访问系统的权限时才能够实现. **泄露**(leakage)系指非授权用户通过对数据的访问非法获取保密信息. **推理**(inference) 系指通过统计分析数据非法获取与个人有关的敏感数据，通常需要进行某种数学推导，例如：某系共有 10 位教员，平均工资为 890 元，如果其中只有一位女教员，又知道全体男教员的平均工资是 900 元，就可以推导出该女教员的实际工资：

$$10\times 890-9\times 900=8900-8100=800(\text{元})$$

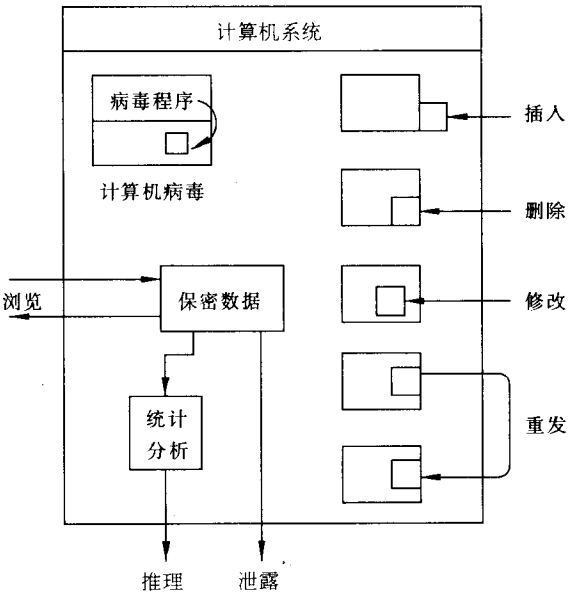

图 1.2 威胁计算机系统安全的几种形式

一般地，我们有如下公式：

$$X=KA_K-(K-1)A_{K-1},$$

其中：K 为全体教员数，A_K 和 A_{K-1} 分别为全体教员的平均工资和全体男教员的平均工资.

类似于主动窃听情形，对于在计算机系统中存储的数据或程序，威胁其完整性的形式也有以下几种：增加记录、删除记录、修改记录，等等. 特别地，众所知的计算机病毒和特洛伊木马程序会致使计算机系统瘫痪、数据丢失、造成灾难性的后果.

一般而言，为了保障分布式系统与计算机网络中传输与存储的数据的安全，通常采用四种不同的控制方法，即密码控制、存取控制、信息流控制和推理控制，此外，还包括备份与数据恢复等手段. 鉴于密码学在计算机网络安全中的关键作用，本书上篇着重介绍密码学的基本原理和主要内容.

1.2 历史的和现实的背景

当你发现写给朋友的信件中途被人截获并拆阅时，一定会很生气；在战争期间，如果

通信联络人员被敌方俘虏，密件中的情报泄露出去，后果就更不堪设想，诸如此类的事情，使人们自然而然地产生了“秘密书写”的念头. 我们可以将不愿意被无关的第三方所知道的内容用某种方法变换一下，使变换后的内容仅仅被有关的人员所理解，而在其他人眼里，这些东西则好像杂乱无章的“天书”，下面我们通过一个形象的例子予以说明. 在某些西方的古玩店里，许多商品旁边会摆放一些标签，但是上面写的并不是普通的标价，而是一些形如“ZZ”、“QPRA”之类的符号，然而，当你向店主询问商品价格时，他会在看一眼标签后马上告诉你准确的金额，原来这些顾客看不懂的符号正是店主自用的密码. 古玩店与一般的商店不同，常常不采用明码标价的方式，这是因为古玩的价格伸缩性很大，店主希望卖高价，但同时又需要知道成本是多少，从而保证在讨价还价时不会赔本，因此，他以密码的形式将成本价格记录在标签上，作为销售时的参考. 这种密码，由于只有店主一个人或店主和店员等少数人知道，因而可以用任何方式来编制，例如：他可以选取一个秘密的单词，使其与自然数对应如下：

C O M P L E X I T Y
0 1 2 3 4 5 6 7 8 9.

如果一个花瓶价值 $5321.00，则根据上述对应关系，可以在标签上注明 EPMO. 类似地，如果一张古画价值 $250.50，一把扇子价值 $7.46，就相应地在标签上标注 MECE，ILX，等等. 因为店主对每一种商品的价格有一个大约的估计，所以这种密码不考虑小数点的位置. 通常，我们把秘密单词 COMPLEXITY 称作密钥，其原因是：如果我们将整个密码系统比喻为一把锁，则掌握了这个秘密单词就等于得到了开锁的钥匙，从而可以窥视该密码系统的内部奥秘了.

早在 4000 多年以前，古埃及人就在墓志铭中使用过类似于象形文字那样奇妙的符号，这是史载的最早的密码形式. 公元前约 50 年，罗马皇帝朱利叶斯·凯撒(Julius Caesar)发明了一种用于战时秘密通信的方法，后来被称之为“凯撒密码”，他将字母按其自然顺序(即字母表的顺序排列)，最后一个字母与第一个字母相连. 将明文中的每个字母用其后面的第三个字母代替，就变成了密文. 例如：

s e n d h e l p

的凯撒密码是

V H Q G K H O S.

以英文为例，凯撒密码的代替表如图 1.3 所示.

明文字母表 a b c d e f g h i j k l m n o p q r s t u v w x y z
密文字母表 D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

图 1.3 凯撒密码字母代替表

注意：为清晰起见，在图 1.3 中我们用小写字母表示明文，用大写字母表示密文.

千百年来，人们运用自己的智慧创造出形形色色的编写密码的方法，下面介绍的几种是其中最简单的.