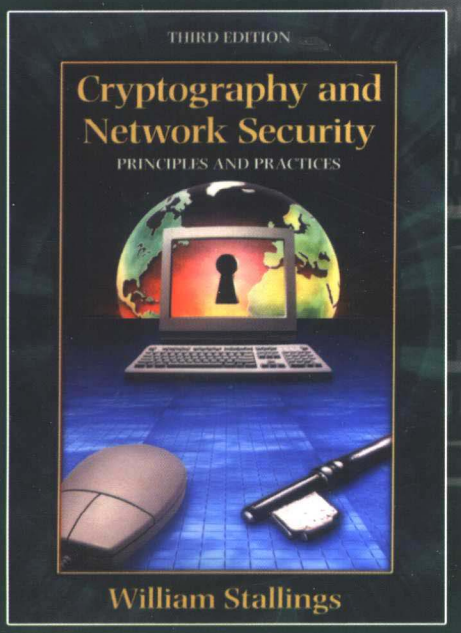
国外计算机科学教材系列

密码编码学与网络安全

——原理与实践（第三版）

Cryptography and Network Security

Principles and Practices, Third Edition



[美] William Stallings 著
刘玉珍 王丽娜 傅建明 等译
张焕国 审校

PEARSON Prentice Hall
PHEI
電子工業出版社
Publishing House of Electronics Industry
http://www.phei.com.cn

国外计算机科学教材系列

密码编码学与网络安全

——原理与实践（第三版）

Cryptography and Network Security
Principles and Practices
Third Edition

[美] William Stallings 著

刘玉珍 王丽娜 傅建明 等译

张焕国 审校

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内容简介

本书系统地介绍了密码编码学与网络安全的基本原理和应用技术。全书主要包括下列四个部分。传统密码部分详细讨论了传统密码算法和设计原理，包括使用传统密码来保证秘密性。公钥密码和hash函数部分详细讨论了公钥密码算法和设计原理、消息认证码和hash函数的应用，以及数字签名和公钥证书。网络安全部分讨论了系统层的安全问题，包括入侵者和病毒造成的威胁及相应的对策、防火墙和可信系统的应用。本书第三版与第二版相比，在继续广泛涵盖密码编码学与网络安全领域内容的同时，新增了有限域、高级加密标准（AES）、RC4密码、CTR模式等内容，并对椭圆曲线密码部分的内容做了很多扩充。此外，对于基本内容的讲述方法也有许多变化和更新。本书内容全面，讲述深入浅出，便于理解，尤其适合于课堂教学和自学，是一本难得的好书。特别是本书后面讨论的网络安全在现实世界中的应用，包括已经实现的和正在使用的提供网络安全的实际应用。

本书可作为研究生和高年级本科生的教材，也可供从事信息安全、计算机、通信、电子工程等领域的科技人员参考。

版权贸易合同登记号　图字：01-2002-5703

图书在版编目（CIP）数据

密码编码学与网络安全：原理与实践：第三版/（美）斯托林斯（Stallings, W.）著；刘玉珍等译.
-北京：电子工业出版社，2004.1
（国外计算机科学教材系列）
书名原文：Cryptography and Network Security: Principles and Practices, Third Edition
ISBN 7-5053-9395-2

Ⅰ.密...　Ⅱ.①斯...　②刘...　Ⅲ.①电子计算机-密码-理论　②计算机网络-安全技术
Ⅳ.①TP309.7　②TP393.08

中国版本图书馆CIP数据核字（2003）第108188号

责任编辑：谭海平
印　　刷：北京兴华印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路173信箱　邮编：100036
经　　销：各地新华书店
开　　本：787×1092　1/16　　印张：32　字数：819千字
印　　次：2004年8月第2次印刷
定　　价：49.00元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换；若书店售缺，请与本社发行部联系。
联系电话：（010）68279077。质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

出 版 说 明

21世纪初的5至10年是我国国民经济和社会发展的重要时期，也是信息产业快速发展的关键时期。在我国加入WTO后的今天，培养一支适应国际化竞争的一流IT人才队伍是我国高等教育的重要任务之一。信息科学和技术方面人才的优劣与多寡，是我国面对国际竞争时成败的关键因素。

当前，正值我国高等教育特别是信息科学领域的教育调整、变革的重大时期，为使我国教育体制与国际化接轨，有条件的高等院校正在为某些信息学科和技术课程使用国外优秀教材和优秀原版教材，以使我国在计算机教学上尽快赶上国际先进水平。

电子工业出版社秉承多年来引进国外优秀图书的经验，翻译出版了“国外计算机科学教材系列”丛书，这套教材覆盖学科范围广、领域宽、层次多，既有本科专业课程教材，也有研究生课程教材，以适应不同院系、不同专业、不同层次的师生对教材的需求，广大师生可自由选择和自由组合使用。这些教材涉及的学科方向包括网络与通信、操作系统、计算机组织与结构、算法与数据结构、数据库与信息处理、编程语言、图形图像与多媒体、软件工程等。同时，我们也适当引进了一些优秀英文原版教材，本着翻译版本和英文原版并重的原则，对重点图书既提供英文原版又提供相应的翻译版本。

在图书选题上，我们大都选择国外著名出版公司出版的高校教材，如Pearson Education培生教育出版集团、麦格劳－希尔教育出版集团、麻省理工学院出版社、剑桥大学出版社等。撰写教材的许多作者都是蜚声世界的教授、学者，如道格拉斯·科默（Douglas E. Comer）、威廉·斯托林斯（William Stallings）、哈维·戴特尔（Harvey M. Deitel）、尤利斯·布莱克（Uyless Black）等。

为确保教材的选题质量和翻译质量，我们约请了清华大学、北京大学、北京航空航天大学、复旦大学、上海交通大学、南京大学、浙江大学、哈尔滨工业大学、华中科技大学、西安交通大学、国防科学技术大学、解放军理工大学等著名高校的教授和骨干教师参与了本系列教材的选题、翻译和审校工作。他们中既有讲授同类教材的骨干教师、博士，也有积累了几十年教学经验的老教授和博士生导师。

在该系列教材的选题、翻译和编辑加工过程中，为提高教材质量，我们做了大量细致的工作，包括对所选教材进行全面论证；选择编辑时力求达到专业对口；对排版、印制质量进行严格把关。对于英文教材中出现的错误，我们通过与作者联络和网上下载勘误表等方式，逐一进行了修订。

此外，我们还将与国外著名出版公司合作，提供一些教材的教学支持资料，希望能为授课老师提供帮助。今后，我们将继续加强与各高校教师的密切联系，为广大师生引进更多的国外优秀教材和参考书，为我国计算机科学教学体系与国际教学体系的接轨做出努力。

电子工业出版社

教材出版委员会

译 者 序

随着计算机与数据通信网络的高速发展和广泛应用，社会对计算机和数据通信网络的依赖越来越大。如果计算机和数据通信网络的安全受到危害，将会危及国家安全，引起社会混乱，造成重大损失。因此，确保计算机和数据通信网络的安全成为世人关注的社会问题，并成为计算机科学技术的热点领域。

为了适应信息科学技术发展的这一新特点，我国政府和科技界已将信息安全技术列为今后一段时期的重点发展领域。许多大专院校都开办了信息安全专业，开设了信息安全课程，因此迫切需要一本合适的教课书。为此，电子工业出版社组织我们翻译出版了这本优秀的教科书。

本书的作者 William Stallings 先后获得了 Notre Dame 电气工程学士学位和麻省理工学院计算机科学博士学位。他编辑出版了 48 本计算机网络和计算机结构领域的书籍，在帮助人们了解计算机网络和计算机结构的技术发展方面做出了卓越的贡献。William Stallings 的著作不仅学术造诣很高，而且十分实用，连续五次获得了教材和著作家协会颁发的优秀计算机科学和工程教材奖。

本书系统地介绍了密码编码学和网络安全的基本原理和应用技术。全书主要包含下列四个部分：传统密码部分详细讨论了传统密码算法和设计原理，包括使用传统密码来保证秘密性；公钥密码和 hash 函数部分详细讨论了公钥密码算法和设计原理、消息认证码和 hash 函数的应用，以及数字签名和公钥证书；网络安全实现部分讨论了重要的网络安全工具和应用软件；系统安全部分讨论了系统层的安全问题，包括入侵者和病毒造成的威胁及相应的对策、防火墙和可信系统的应用。

本书第三版与第二版相比，在继续广泛涵盖密码学与网络安全领域内容的同时，新增了有限域、高级加密标准（AES）、RC4 密码、CTR 模式等内容，并对椭圆曲线密码部分的内容做了很多扩充。除此之外，对于基本内容的讲述方法也有许多变化和更新。

本书内容全面，讲述深入浅出，便于理解，尤其适合于课堂教学和自学，是一本难得的好书。特别是本书后面讨论的网络安全在现实世界中的应用，包括已经实现的和正在使用的提供网络安全的实际应用。本书可作为研究生和高年级本科生的教材，也可供从事信息安全、计算机、通信、电子工程等领域的科技人员参考。

本书前言、第 1 章和第二部分由刘玉珍翻译，第一部分由曾祥勇、王张宜翻译，第三部分及附录由傅建明翻译，第四部分由王丽娜翻译，全书由张焕国统稿和审校。

由于译者的专业知识和外语水平有限，书中错误在所难免，敬请读者指正，译者在此先致感谢之意。

前　言

在当前全球电子互连互通的时代，由于病毒、黑客、电子窃听和电子欺诈，使得信息安全性在任何时候都十分重要。第一，由于计算机系统的大量增加以及计算机系统通过网络互联，使得组织和个人越来越依赖于存储的信息和利用计算机系统传输的信息。这样就需要保护数据和资源不被泄露，保证数据和消息的真实性，保护系统不受基于网络的攻击。第二，密码和网络安全的学科已经成熟，这样可开发出方便实用的应用软件来加强网络安全。由于这两种发展趋势，本书所讨论的内容就显得十分重要。

本书的目的

本书的目的是概述密码编码学和网络安全的原理和应用。前两部分讨论密码编码学和网络安全技术，阐述网络安全的基本内容。其他部分讨论网络安全的应用，包括已经实现或正用于提供网络安全的实用应用软件。

因此本书涉及多个学科。特别地，要想理解本书讨论的某些技术的精髓，必须要有数论的基本知识和概率论中的某些结果。然而本书试图自成体系，不仅给出了必需的数论知识，而且让读者对这些知识有直观的理解。采用的方法是，在需要的时候才引入这些背景知识。这样有助于读者理解讨论这些知识的动机，作者认为这种方法比把所有的数学知识一次性全部放在本书开头要好。

本书适用的对象

本书适合于教师和专业人员使用。本书可作为计算机科学、计算机工程、电气工程专业本科生密码编码学和网络安全方面课程的教材，学时为一学期。本书也可作为参考用书或作为自学教材。

本书的组织

本书由四个部分组成：

1. **传统密码**：详细讨论了传统密码算法和设计原理，包括使用传统密码来保证秘密性。
2. **公钥密码和 hash 函数**：详细讨论了公钥密码算法和设计原理，该部分还讨论了消息认证码和 hash 函数的应用，以及数字签名和公钥证书。
3. **网络安全实现**：讨论了重要的网络安全工具和应用软件，包括 Kerberos、X.509v3、PGP、S/MIME、IP Security、SSL/TLS 和 SET。
4. **系统安全**：讨论了系统层的安全问题，包括入侵者和病毒造成的威胁及相应的对策、防火墙和可信系统的应用。

另外,本书还给出了术语表、常用的首字母缩略词表和参考文献。每一章中都有课后习题、思考题和关键术语表、推荐读物和网址。

在每一部分开头,按章详细介绍了该章的主要内容。

教师和学生的 Internet 服务

本书的网页可给学生和教师提供支持,该网页包括一些相关的站点、以 PDF 格式存储的本书中出现的图片和表格、有关本书的 Internet 邮件列表的签名信息。该网页是 WilliamStallings.com/Crypto3e.html。Internet 邮件列表的建立使得使用本书的教师可以相互或与作者交换信息、建议或讨论问题。若发现印刷或其他错误,则在 WilliamStallings.com 处可找到本书的勘误表。另外在计算机科学专业学生资源网址 WilliamStallings.com/StudentSupport.html 提供了有关计算机专业学生和专业人员的信息和链接。

讲授密码编码学和网络安全的计划

对许多教师来说,密码编码学或信息安全课程的一个重要组成部分就是制定一个或一系列计划,使得学生有机会亲手实践,以加深从课本中学到的知识。本书在很大程度上对该课程的讲授计划提供支持。教师手册不仅包含如何布置和安排计划,而且还包括一系列涵盖本书内容的推荐教学计划:

- **研究计划**:一系列指导学生研究 Internet 有关课题以及撰写研究报告的课外研究课题。
- **程序设计计划**:一系列涵盖大部分课程内容且可在任何平台上用任何适当的语言实现的程序设计项目。
- **课外阅读/报告**:每一章在参考文献中都包含有论文列表,可让学生阅读并写出简短报告。

第三版新增内容

本书第二版出版后的四年中,该领域仍处于不断的变革之中。该新版中,我试图在继续广泛涵盖本领域内容的同时,增加这些新的变化。进行本次修订之初,本书由许多讲授该领域课程的教授仔细审阅过。而且,许多研究该领域的专业人员也审阅过某些章节。这使得许多地方的叙述变得清晰、紧凑,对插图也进行了改进,而且增加了许多新的"现场试验"问题。

除了这些为改进教学法和用户友好性所做的修改以外,还有一些实质性的变化贯穿本书,最主要包括下列几个方面:

- **新增内容——高级加密标准(AES)**:该领域在过去四年中发生的最重要的事件莫过于采用了高级加密标准(AES)。设计该传统加密算法是为了替代 DES 和三重 DES。该算法可能很快会成为最为广泛使用的传统加密算法。本书新增了对 AES 的详细讨论。
- **新增内容——有限域**:AES 和椭圆曲线密码学都使用有限域。本书新增加了一章,简洁且清晰地描述了该领域中那些必不可少的概念。
- **新增内容——RC4 密码**:RC4 是使用最为广泛的流密码。它是为网络浏览器和服务器

间通信而定义的 SSL/TLS(安全套接层/传输层安全)标准的一部分,它也用于 WEP(Wired Equivalent Privacy)协议中,该协议是 IEEE 802.11 无线 LAN 标准的一部分。

- **新增内容——CTR 模式**:NIST 最近批准了分组密码加密的计数器模式,以适应对加密速度要求高的应用。
- **扩充内容——椭圆曲线密码学**:ECC 是一种愈来愈重要的、愈来愈被广泛使用的公钥技术,因此本书对 ECC 部分的内容做了很多扩充。

致谢

本次修改得益于许多人的审阅,他们花费了大量的时间和精力。下列这些人员审阅了所有或大部分手稿:Martha Sloan(Michigan Tech)、Xiangyang Li(Illinois Institute of Technology)、Ed Fernandez(Florida Atlantic University)、Dan Warren(Naval Postgraduate School)、Phillip Enslow(Georgia Tech)和 Cetin Koc(Oregon State)。

我还要感谢那些详细审阅其中某一章的人员:Steve Tate、Breno de Medeiros、Daniel Kifer、Sam Staton、Thiébaut Mochel、Mads Sig Ager Jensen、Alexey Kudravtsev、Stefan Katzenbeisser 和 Iulian Dragos。Joan Daemen 审阅了关于 AES 的章节。

下列人员在教师手册中的课程计划方面做了工作:Henning Schulzrinne(Columbia University)、Cetin Kaya Koc(Oregon State University)和 David Balenson(Trusted Information Systems and George Washington University)。

同时,我还要感谢那些在家庭作业方面做了工作的人员:Luke O'Connor;MITRE 的 Joseph Kusmiss;Stratus 的 Carl Ellison;Shunmugavel Rajarathinam;Jozef Vyskoc,他在 Sherlock Holmes 问题上做了很好的工作。

在这么多帮助面前,我几乎没有什么可以居功自傲的。但我可以自豪地说,没有这些帮助,我也会选择所有这些内容。

目　录

第一部分　对称密码

第二部分 公钥加密与hash函数

第三部分　网络安全应用

第四部分　系统安全性

第1章 引 言

最近几十年中，企业对**信息安全**的需求经历了两个重要变革。在广泛使用数据处理设备之前，企业主要是依靠物理和行政手段来保证重要信息的安全。采用的物理手段如将重要的文件放在上锁的文件柜里，采用的行政手段如对雇员的检查制度。

很显然，由于计算机的应用，需要有自动工具来保护存于计算机中的文件和其他信息。对于共享系统，如时间共享系统，以及通过公共电话网、数据网或 Internet 可访问的系统，尤其如此。用来保护数据和阻止黑客的工具一般称为**计算机安全**。

影响安全的第二个变革是，分布式系统、终端用户与计算机之间以及计算机与计算机之间传送数据的网络和通信设施的应用。在信息传输时，需要有网络安全措施来保护数据传输。事实上，术语**网络安全**容易引起误解，因为实际上所有的商业、政府和学术组织都将其数据处理设备与互联网相连，该互联网称为 internet[①]，并使用术语 **internet 安全**。

上述两种形式的安全没有明确的界限。例如，对信息系统最常见的攻击就是计算机病毒，它可能已先感染磁盘，然后才加载到计算机上，从而进入系统；也可能是通过 internet 进入系统。无论是哪一种情况，一旦病毒驻留在计算机系统中，就需要内部的计算机安全工具来检查病毒并恢复数据。

本书主要讨论 internet 的安全，包括阻止、防止、检测和纠正信息传输中出现的安全问题的措施，所涉及的内容相当广泛。为使读者对本书中讨论的领域有所了解，我们先举出几个有关安全问题的例子：

1. 用户 A 向用户 B 传送文件，该文件包含不能泄密的敏感信息（如工资单），用户 C 无权读取文件，但能够监视传输过程并截获该文件。
2. 网络管理员 D 向计算机 E 传输一条消息，命令计算机 E 更新权限文件以允许新用户可访问 E。用户 F 截获并修改该消息，如增加或删除一些用户，然后将消息转发给 E，而 E 误以为是管理员 D 发来的消息并更新权限文件。
3. 用户 F 也可以不截获消息，而是按自己的意愿构造消息并发送给 E，同样 E 误以为是管理员 D 发来的消息并更新权限文件。
4. 雇员事先未得到警告就被解雇。管理人员向服务器系统发送消息以注销该雇员的账号。账号注销后，服务器将通知贴到该雇员的文件中以确认注销。该雇员可以截获并延时这条消息，直至他有足够的时间访问服务器来获取敏感信息，然后再转发这条消息，以确认注销账号。雇员的这些活动在相当长的时间内不会被察觉。
5. 顾客向股票经纪人发送消息，请求完成各种交易。后来，这些投资失败而顾客否认发送过该消息。

---

① internet（“i”小写时）是指任何网络互联，如企业内部网就是 internet 的一个示例；Internet（“I”大写时）是指企业构造其 internet 时所使用的设施之一。

尽管上述举例不能穷尽所有可能的安全威胁类型，但足以表明网络安全所关注的范围。Internet 的安全同样错综复杂。理由如下：

1. 安全涉及到通信和网络，它不是像初次接触这个领域的人想像的那样简单。对网络安全的要求看起来似乎很明显。的确，对安全服务的绝大多数要求都可用自明其意的词语来描述，如保密性、认证、真实性和完整性等。但是，实现满足这些要求的安全机制却非常复杂。要想理解这些安全机制，需要进行缜密的推理。
2. 倘若让你设计一个安全机制或算法，你必须考虑各种各样的潜在攻击。很多情况下，从一个与设计完全不同的角度和方法出发，可能使攻击成功。这些方法都利用了你设计的机制中存在的意想不到的弱点。
3. 根据第二点，设计安全机制的过程通常采用逆向思维：不是从对安全性的要求出发来确定需要哪些安全措施，而是从可能有哪些攻击方法出发来确定需要哪些安全措施。
4. 倘若已经设计好了安全机制，接下来就是要确定在哪里使用这些安全机制，包括物理位置（在网络的什么地方）和逻辑位置（如像 TCP/IP 这样的网络协议的哪一层）。
5. 安全机制所使用的算法和协议通常不止一个。这些协议和算法需要通信双方使用一些秘密信息（如加密密钥），这就出现了对秘密信息的产生、分配、保护等问题。它们所依赖的通信协议可能会使得设计安全机制的过程复杂化。例如，安全机制需要对通信时间进行限制，而任何协议和网络都存在不确定且不可预知的通信时延，因此可能使这种限制毫无意义。

因此，需考虑的问题还有很多，这一章概述本书所要讨论的主要问题。首先讨论网络安全、服务和机制以及对网络的攻击类型，然后给出安全设施和安全机制的一般模型。

1.1 服务、机制和攻击

为了对系统的安全需求进行评估以及评价各种有关安全的产品和政策，负责安全的主管人需要用一些系统的方法来定义对安全的要求以及描述如何满足这些要求。一种方法是考虑信息安全的三个方面：

- **安全攻击**：任何危及系统信息安全的活动。
- **安全机制**：用来保护系统免受侦听、阻止安全攻击及恢复系统的机制。
- **安全服务**：加强数据处理系统和信息传输的安全性的一种服务。其目的在于利用一种或多种安全机制阻止安全攻击。

1.1.1 服务

我们先简单考虑一下上述三个方面，首先我们讨论安全服务。我们可以想到一些信息安全服务，如正常的与物理文本有关的某些服务。大多数人类活动，如商业、外交、军事以及人际交往等，都使用了文本，并且依赖交易双方对文本完整性的信赖。通常文件都有签名和日期，同时为防止它们被泄漏、篡改或破坏，要有公证和现场见证人，要被记录或被允许访问，等等。

因为信息系统已经越来越深入到我们的日常生活，电子信息在很多方面已经取代了传统的纸文本的作用。然而，以下这些方面使得电子信息有时不太方便：

1. 一般说来，要区分出纸文本的原件和复印件是可能的，然而电子信息只不过是一些二进制位串，无法区分所谓的原件和复印件。
2. 更改纸文本必然会留下一些物理痕迹，比如擦除可能导致表面粗糙或留下一个小槽，而在内存中改变一些二进制位却不会留下任何物理痕迹。
3. 所有与纸文本有关的证据都来自于文本本身的物理特征，比如手写签名、阴文或阳文的公证印章，等等；而电子信息若要进行此类认证，只能依靠本身所记录的二进制信息。

表1.1列举了传统纸文本的一些常见功能以及电子信息类似的功能。这些功能实际上是我们对电子信息所提出的安全性要求。

表1.1的内容太长，其本身不适合指导我们设计安全机制。计算机和网络安全的研究与开发着重于一些通用的安全服务，包括信息安全机制所要求的各种功能。我们将在下一节中探讨这些问题。

表1.1 部分常见的信息完整性功能[SIMM92]

• 身份证明	• 签注
• 认证	• 访问(外出权)
• 许可与/或证书	• 确认
• 签名	• 发生时间
• 见证人(公证)	• 认证软件——软件与/或文件
• 同时发生	• 投票
• 责任	• 所有权
• 收条	• 登记
• 发送方与/或接收方的证书	• 赞成/否决
	• 隐秘(秘密)

1.1.2 机制

没有哪一种安全机制能提供上述的所有安全服务。本书将讲述几种安全机制。然而，我们会注意到，许多安全机制都包含一种特殊的技术：密码技术。加密或类加密信息传输(如hash函数)是提供安全性最常用的手段。因此，本书集中讨论了密码技术的发展、应用和管理。

1.1.3 攻击

正如G. J. Simmons所指出的，信息安全是指如何阻止对信息系统中物理存在的信息的攻击，或在阻止失败后如何检测这些攻击并从中恢复信息，其中这些信息本身是没有意义的物理存在[SIMM92]。

表1.2列举了一些攻击的例子，在现实世界中有许多这种攻击，即组织或个人（或代表其雇员的组织）都需要对付的攻击。对组织的攻击随着环境的变化而变化。幸运的是，我们能够通过观察可能遇到的攻击类型，从不同的角度来处理该问题。这就是下一节所要讨论的主题。