国外计算机科学教材系列

PEARSON Prentice Hall

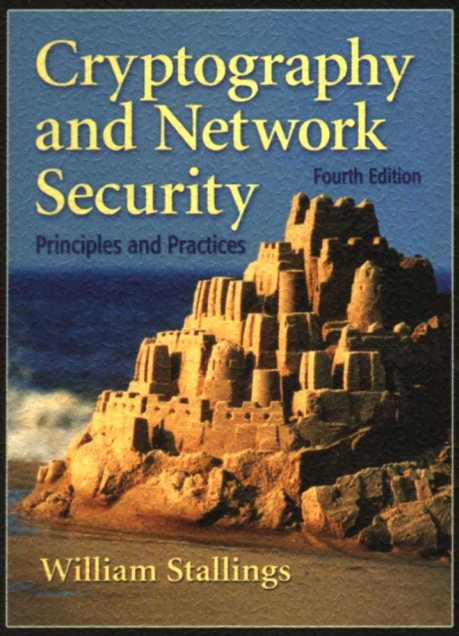
William Stallings

密码编码学与网络安全

—— 原理与实践（第四版）

Cryptography and Network Security

Principles and Practices, Fourth Edition



[美] William Stallings 著
孟庆树 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
http://www.phei.com.cn

权威作者 经典力作

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（第四版）

Cryptography and Network Security

Principles and Practices

Fourth Edition

[美] William Stallings 著

孟庆树 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：对称密码部分讨论了对称密码的算法和设计原理；公钥加密和散列函数部分讨论了公钥密码的算法和设计原理、报文认证码和散列函数的应用等；网络安全应用部分讨论了系统层的安全问题，包括电子邮件安全、IP安全以及Web安全等；系统安全部分讨论了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等。第四版与第三版相比，新增了Whirlpool，CMAC，DDoS以及CCITSE等内容，并对简化的AES，PKI等内容做了扩充。此外，对于基本内容的讲述方法也有许多变化和更新，并新增加了100多道习题。

本书可作为信息类专业高年级本科生与低年级研究生的教材，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：01-2006-0891

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4版/（美）斯托林斯（Stallings, W.）著；孟庆树等译.
北京：电子工业出版社，2006.11
（国外计算机科学教材系列）
书名原文：*Cryptography and Network Security: Principles and Practices, Fourth Edition*
ISBN 7-121-03341-0
Ⅰ.密… Ⅱ.①斯… ②孟… Ⅲ.①电子计算机-密码-编码理论-教材
②计算机网络-安全技术-教材 Ⅳ.①TP309.7 ②TP393.08
中国版本图书馆CIP数据核字（2006）第126231号

责任编辑：李秦华
印　　刷：
装　　订：北京市京科印刷有限公司
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
开　　本：787×1092　1/16　　印张：31.5　　字数：909千字
印　　次：2006年11月第1次印刷
定　　价：49.80元

凡所购买电子工业出版社的图书有缺损问题，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。邮购电话：（010）88254888。

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。

服务热线：（010）88258888。

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损害，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已成为世人关注的社会问题，并成为信息科学技术领域中的研究热点。

信息安全技术与产业已成为我国信息科学技术中的重点发展领域。目前，许多大专院校都开设了信息安全专业或开设了信息安全课程，迫切需要一本合适的教科书。为此，电子工业出版社组织我们于 2004 年翻译出版了《密码编码学和网络安全——原理与实践》(第三版)这本优秀的教科书。这本书翻译出版后得到了广大读者的厚爱，许多著名大学都采用它作为教材，为我国信息安全人才培养和传播信息安全知识发挥了重要作用。

2006 年原书作者又出版了该书的第四版。在第四版中，作者对原书部分内容做了调整和更新。在密码学方面增加了简化 AES，新的分组密码工作模式 CMAC。去掉了有关 MD5，SHA-1，RIPEMD-160 方面的内容，增加了一种基于分组密码的新散列(hash)函数 Whirlpool 和 SHA-512。在网络安全方面增加了公钥基础设施(PKI)。在系统安全方面增加了分布式拒绝服务攻击(DDOS)和信息技术安全评估通用准则。此外，作为对本书内容的补充，在本书的网站上新设了 6 个附录。

为了使广大读者能够读到新版本，电子工业出版社又组织我们翻译出版了本书。

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。他编写出版了 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 5 次获得了(美国)教材和著作家协会(Textbook and Academic Authors Assiciation)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。全书主要包含以下四个部分。第一部分为传统密码，详细讨论了传统密码算法和设计原理，以及使用传统密码确保秘密性的方法与技术。第二部分为公钥密码和散列函数，详细讨论了公钥密码算法和设计原理、消息认证码和散列函数的应用，以及数字签名。第三部分为网络安全，讨论了公钥基础设施、电子邮件安全、IP 安全和 Web 安全。第四部分为系统安全，讨论了系统层的安全问题，包括入侵和病毒造成的威胁与相应的对策、恶意软件以及防火墙。

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。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。

本书的前言、第 0 章到第 4 章、第二部分和附录由孟庆树翻译，第 5 章到第 7 章由王张宜翻译，第三部分由傅建明翻译，第四部分由王丽娜翻译，全书由张焕国统稿和校审。

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。

符　号

符　号	表达式	意　义
D, K	D(K, Y)	用密钥 K 和对称算法解密密文 Y
D, PR_a	D(PR_a, Y)	用 A 的私钥 PR_a 和非对称算法解密密文 Y
D, PU_a	D(PU_a, Y)	用 A 的公钥 PU_a 和非对称算法解密密文 Y
E, K	E(K, X)	用密钥 K 和对称算法加密明文 X
E, PR_a	E(PR_a, X)	用 A 的私钥 PR_a 和非对称算法加密明文 X
E, PU_a	E(PU_a, X)	用 A 的公钥 PU_a 和非对称算法加密明文 X
K		密钥
PR_a		用户 A 的私钥
PU_a		用户 A 的公钥
C, K	C(K, X)	消息 X 的消息认证码,密钥为 K
GF(p)		阶为 p 的有限域,p 为素数,域定义为 Z_p 及其上模 p 的算术运算
GF(2^n)		阶为 2^n 的有限域
Z_n		小于 n 的非负整数集合
gcd	gcd(i, j)	最大公因子,整除 i 和 j 的最大正整数
mod	$a \bmod m$	a 除以 m 的余数
mod, $\equiv$	$a \equiv b \pmod m$	$a \bmod m = b \bmod m$
mod, $\not\equiv$	$a \not\equiv b \pmod m$	$a \bmod m \neq b \bmod m$
dlog	$\mathrm{dlog}_{a,p}(b)$	以 a 为底的 b 的对数,模 p 运算
ϕ	$\phi(n)$	欧拉函数,小于 n 且和 n 互素的正整数个数
Σ	$\sum_{i=1}^{n} a_i$	$a_1 + a_2 + \cdots + a_n$
Π	$\prod_{i=1}^{n} a_i$	$a_1 \times a_2 \times \cdots \times a_n$
$\mid$	$i \mid j$	i 除得尽 j,即 i 除 j 的余数为零
$\mid, \mid$	$\mid a \mid$	a 的绝对值
$\parallel$	$x \parallel y$	级联 x 和 y
$\approx$	$x \approx y$	x 约等于 y
$\oplus$	$x \oplus y$	单比特变量时是异或运算,多比特变量时是按位异或运算
$\lfloor, \rfloor$	$\lfloor x \rfloor$	小于等于 x 的最大整数
$\in$	$x \in S$	元素 x 属于集合 S
$\longleftrightarrow$	$A \longleftrightarrow (a_1, a_2, \cdots, a_k)$	整数 A 和整数序列(a_1, a_2, $\cdots$, a_k)对应

前　言

在当前全球电子互联互通的时代，由于病毒、黑客、电子窃听和电子欺诈，使得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这些系统所存储和传输的信息。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。

本书的目标

本书的目标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，在需要时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

本书适合于学术和专业人员使用。作为教科书，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。本书的内容包括了IAS2 安全机制、NET4 安全和 IT311 中的内容（IAS2 和 NET4 是信息技术知识体系的两个核心领域，而 IT311 是密码学的高级教程）。

本书也可作为参考用书或作为自学教材。

本书的组织

本书由如下四部分组成：

第一部分：对称密码[①]。详细讨论了传统加密算法和设计原理，包括使用传统加密来保证保密性。

① 原书此处为“传统密码”（Conventional Encryption），在业界一般认为“传统密码”就是“对称密码”，为与正文相符，我们将其统一为“对称密码”——编者注。

第二部分：公钥密码和散列函数。详细讨论了公钥密码算法和设计原理，还讨论了消息认证码和散列函数的应用，以及数字签名和公钥证书。

第三部分：网络安全应用。讨论了重要的网络安全工具和应用软件，包括 Kerberos，X.509v3 证书，PGP，S/MIME，IP Security，SSL/TLS 和 SET。

第四部分：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、推荐读物和网站。

在每一部分的开头，按章详细介绍了该部分各章的主要内容。

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网站、以 PDF 格式存储的本书中出现的图片、表格和幻灯片。该网页为 WilliamStallings.com/Crypto/Crypto4e.html。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，计算机科学专业学生资源网WilliamStallings.com/StudentSupport.html 为计算机专业学生和专业人员提供了有关的文档、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订一个或一系列计划，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部署和安排计划，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。
- **实验室练习：**就本书中的概念进行编程和做实验的系列计划。
- **书面作业：**每一章中推荐了一些书面作业。
- **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。

第四版新增内容

在本书第三版出版后的三年中，该领域仍处于不断的变革之中。在第四版中，作者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“现场测试”习题。

除了这些为改进教学法和方便用户所做的修改以外，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：

- **简化 AES**:一个用于教学目的的简化版本 AES(Advanced Encryption Standard,高级加密标准),使学生更容易掌握 AES 的本质。
- **Whirlpool**:一个基于对称分组密码的全新且重要的安全散列算法。
- **CMAC**:一种新的分组密码工作模式。CMAC(Cipher-based Message Authentication Code,基于密文的消息认证码)基于对称分组密码对消息进行认证。
- **公钥基础设施(PKI)**:这是本书中的一个重要主题。
- **分布式拒绝服务攻击(DDoS)**:DDoS 攻击近年来越来越值得关注。
- **信息技术安全评估通用准则**:通用准则已经成为体现安全要求、产品评估及实现评估的国际框架。
- **在线附录**:作为对本书内容的补充,本书的网站上有 6 个附录。

另外,本书的许多其他内容也进行了更新和修改。

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:Danny Krizanc (Wesleyan University), Breno de Medeiros (Florida State University), Roger H. Brown (Rensselaer at Hartford), Cristina Nita-Rotarul (Purdue University), 以及 Jimmy McGibney (Waterford Institute of Technology)。

我还要感谢那些详细审阅其中某一章的人员:Richard Outerbridge, Jorge Nakahara, Jeroen van de Graaf, Philip Moseley, Andre Correa, Brian Bowling, James Muir, Andrew Holt, Décio Luiz Gazzoni Filho, Lucas Ferreira, Dr. Kemal Bicakci, Routo Terada, Anton Stiglic, Valery Pryamikov 和 Yongge Wang。

Joan Daemen 审阅了关于 AES 的章节,Vincent Rijmen 审阅了有关 Whirlpool 的内容,而 Edward F. Schaefer 审阅了有关简化 AES 的内容。

下列人员为第四版的课外作业做了很多工作:Joshua Brandon Holden (Rose-Hulman Institute of Technology), Kris Gaj (George Mason University)和 James Muir (University of Waterloo)。

Purdue 大学的 Sanja Rao 和 Ruben Torres 为教师手册里的实验室练习做了很多工作。下列人员为教师手册中的课程计划做了工作:Henning Schulzrinne(Columbia University),Cetin Kaya Koc(Oregon State University)和 David Balenson(Trusted Information Systems and George Washington University)。

最后,我要感谢负责本书出版的工作人员 Rose Kernan, Sarah Parker, Tracy Dunkelberger 和 Patricia M. Daly。

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,即使没有这些帮助,我也会选择所有这些内容。

目　录

第二部分 公钥密码和散列函数

第三部分 网络安全应用

第四部分 系统安全

第0章 读者导引

本书及其配套网站涵盖了很多的内容。下面为读者介绍一下概况。

0.1 本书概况

在第0章和第1章之后，本书由如下四部分组成：

第一部分：对称密码。提供了有关对称加密算法的综述，包括传统和现代加密算法。重点放在两个最为重要的算法上，即数据加密标准(DES)和高级加密标准(AES)。这部分还讨论了消息认证和密钥管理。

第二部分：公钥密码和散列函数。给出了公钥密码算法的综述，包括RSA (Rivest-Shamir-Adelman)密码和椭圆曲线密码。该部分还讨论了公钥密码算法的应用，如数字签名和密钥交换。

第三部分：网络安全应用。讨论了应用密码算法和安全协议为网络和Internet提供安全。涉及的主题包括用户认证、电子邮件、IP安全和Web安全。

第四部分：系统安全。讨论了保护计算机系统免受安全威胁的安全工具问题，这些威胁包括入侵、病毒和蠕虫。该部分还介绍了防火墙技术。

本书中介绍的众多密码算法、网络安全协议和应用，许多都已经成为标准。其中最为重要的是由Internet RFC定义的Internet标准以及由美国国家标准技术局(NIST)发布的联邦信息处理标准(FIPS)。附录A讨论了标准制订的过程并列出了本书引用过的一些标准。

0.2 导读

0.2.1 主题

本书的内容分为如下三大类：

- **密码学**：研究确保信息的秘密性和真实性的技术。密码学的两个主要分支是密码编码学和密码分析学。密码编码学研究如何设计上述技术，密码分析学研究如何对抗上述技术以恢复信息，或者伪造信息，使得信息的接收者认为是真的。
- **网络安全**：该领域讨论如何将密码算法用于网络协议和网络应用。
- **计算机安全**：本书中我们用该术语来表示防止入侵(如黑客)和恶意软件(如病毒)的计算机安全。一般来说，需要保护的计算机通常连接在网络上，而大量的威胁也来自于网络。

本书的前两部分讨论两种不同的加密码方法：对称加密算法和公钥或非对称加密算法。在对称算法中，双方使用单个共享的密钥。公钥算法使用两个密钥：一方只知道私钥，而另一方只知道公钥。

0.2.2 主要内容的顺序

本书包含了很多的内容，对于希望简短地阅读本书的教师和学生，有很多的机会可以这么做。

若想全面了解前两部分的内容,则应该逐章依次阅读。除了高级加密标准(AES)之外,第一部分的内容不需要任何特别的数学背景知识。为了理解 AES,有必要对有限域有所了解。而理解有限域则需要素数和模算术的一些基本背景知识。相应地,在第 5 章使用它们之前,我们在第 4 章中包含了这些数学预备知识。因此,如果准备跳过第 5 章,那么跳过第 4 章也没有问题。

第 2 章中介绍了这一部分其他章中都有用的一些概念。然而,对于那些只对现代密码学感兴趣的读者来说,这一章可以很快跳过。第 3 章和第 5 章分别讨论了两个最重要的对称密码算法:DES 和 AES。第 6 章讨论了另外两个有趣的算法,它们都有商业应用。如果对这两个算法不感兴趣,也可以跳过这一章。

对于第二部分,惟一需要补充的数学背景知识是数论,这将在第 8 章讨论。那些跳过第 4 章和第 5 章的读者应该首先复习一下 4.1 节至 4.3 节的内容。

两个使用得最广的通用公钥密码算法是 RSA 和椭圆曲线密码,RSA 更为人们所接受。读者也许会希望跳过第 10 章中有关椭圆曲线密码的内容,至少是初次阅读时会如此。在第 12 章中,Whirlpool 和 CMAC 的重要性稍微低一些。

第三部分和第四部分彼此独立,阅读顺序可以随意。这两部分都需要读者对第一部分和第二部分的基本内容有所了解。

0.3 Internet 和 Web 资源

Internet 和 Web 上有许多支持本书的资源,以便读者可以跟踪该领域的发展。

0.3.1 支持本书的网站

为支持本书,作者制作了一个专用网页——WilliamStallings.com/Crypto/Crypto4e.html。该网页包含有如下内容:

- **有用的网站**:按章的顺序给出了通往其他网站的链接,这些网站包括本节和全书列出的网站。
- **勘误表**:我们会维护和按需更新勘误表。请读者将发现的错误通过电子邮件告诉我们。书中已有的勘误表位于 WilliamStallings.com。
- **图**:以 PDF 格式给出了本书中的所有图形。
- **表**:以 PDF 格式给出了本书中的所有表格。
- **幻灯片**:按章组织的一套幻灯片。
- **密码编码学和网络安全教程**:含有指向基于本书课程主页的链接。这些主页有助于教师组织课程。

作者还维护了一个计算机科学学生资源网站——WilliamStallings.com/StudentSupport.html。该网站的目的是为计算机科学的学生和专业人士提供文档、信息和链接。链接和文档分为如下四类:

- **数学**:包括基本的数学复习、排队论分析初步读物、数字系统初步读物以及很多通向其他数学网站的链接。
- **如何做的问题**:给出了一些有关如何做课外作业、写技术报告、准备技术汇报的建议和指导。