<<密码编码学与网络安全>>

图书基本信息

书名：<<密码编码学与网络安全>>

13位ISBN编号：9787121152504

10位ISBN编号：7121152509

出版时间：2012-1

出版时间：电子工业出版社

作者：William Stallings

页数：540

译者：王张宜,杨敏,杜瑞颖 等译,张焕国 审校

前言

序　　随着信息科学技术的高速发展和广泛应用，社会逐步信息化。
在信息化社会中，通信、计算机和消费电子的结合，产生了Internet、信息高速公路或全球信息基础设施（GII），构成了人类生存的信息环境，即信息空间（Cyberspace）。
在信息空间中，计算机和网络在军事、金融、工业、商业、人们的生活和工作等方面的应用越来越广泛，社会对计算机和网络的依赖越来越大，如果计算机和网络系统的信息安全受到破坏将导致社会的混乱并造成巨大损失。
　　我们应当清楚，人类社会中的安全可信与信息空间中的安全可信是休戚相关的。
对于人类生存来说，只有同时解决了人类社会和信息空间的安全可信，才能保证人类社会的安全、和谐、繁荣和进步。
　　因此，确保信息空间、计算机和网络系统的信息安全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。
　　发展我国信息安全技术与产业的关键是人才，而培养人才的关键是教育。
目前，我国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2006年翻译出版了《密码编码学与网络安全——原理与实践（第四版）》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。
　　2010年原书作者又出版了该书的第五版。
在第五版中，作者对原书的内容和组织结构都做了较大的调整和更新。
　　1.在书的组织结构方面做了如下调整：　　① 在密码学方面增加了第三部分：密码学数据完整性算法。
专门讨论密码算法中涉及数据完整性的内容，包括密码学Hash函数，消息认证码和数字签名。
　　② 增加了第四部分：相互信任。
集中讨论了信息系统中的实体相互信任问题，包括密钥管理和用户认证。
　　③ 首次采用了在线内容，包括在线章和在线附录。
将第六部分：系统安全、第七部分：法律与道德、附录C至附录Q放到网站上，读者可以上网阅读学习为使本书的中文版读者能读到原书的完整内容，特地翻译了原书的在线内容［第20章至第23章，以及附录C至附录Q。
这些内容的中文版已上载至华信教育资源网（http：//www.hxedu.com.cn），有兴趣的读者可免费下载］，从而为中文读者提供了一本完整的中文图书——编者注。
。
这样可以节约书的篇幅，降低书的成本。
　　④ 将伪随机数产生与序列密码集成为独立的一章。
类似单独列章的还有传输层安全等。
在以前的版本中，这些相关内容分散在各章中。
这样将相关联的内容集成为一章，便于读者学习掌握。
　　2.在内容方面进行了许多修改，并增加了一些新内容。
如对于欧几里得算法、AES、分组密码工作模式、伪随机数、Hash函数和消息认证码、密钥管理和分配、远程用户认证、IPsec等内容进行了修改，并新增了ElGamal加密和数字签名、SHA-3、认证加密、联合身份认证、HTTPS、安全框架SSH、域密钥身份认证邮件DKIM、无线网络安全、法律与道德、在线附录、Sage示例与问题等方面的新内容。
　　3.作为对本书内容的补充，增加了15个附录。
这些附录为感兴趣的读者提供了更深入、更广泛的补充材料。
这是以前的版本中所没有的。

4.首次使用开源免费的Sage计算机代数系统，使学生们能够亲手进行各种密码算法的实验。

为了使广大读者能够读到新版书，电子工业出版社又组织我们翻译出版了本书的第五版。

《密码编码学与网络安全——原理与实践》一书的作者William Stallings先后获得了Notre Dame电气工程学士学位和MIT计算机科学博士学位。

他累计编写出版了48本计算机网络和计算机体系结构领域的书籍，在计算机网络和计算机体系结构的学术交流和教育方面做出了卓越的贡献。

其中《密码编码学与网络安全——原理与实践》就是其中最成功的一本书籍。

William Stallings的著作不仅学术造诣很高，而且十分实用，先后11次获得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教材奖。

本书系统地介绍了密码学与网络安全的基本原理和应用技术。

全书主要包含以下7个部分。

第一部分：对称密码，介绍了古典和现代对称密码算法，重点介绍数据加密标准（DES）和高级加密标准（AES）。

此外，还讨论了伪随机数和流密码。

第二部分：非对称密码，给出了数论基础、RSA密码、椭圆曲线密码和其他公钥密码。

第三部分：密码学中的数据完整性算法，介绍了密码学Hash函数、消息认证码和数字签名。

第四部分：相互信任，介绍了密钥管理和密钥分配，以及用户认证协议。

第五部分：网络与因特网安全，讨论了传输层安全、无线网络安全、E-mail安全和IP安全等内容。

第六部分：系统安全，讨论了非法入侵、恶意软件和防火墙技术。

第七部分：法律与道德，讨论了与计算机和网络安全相关的法律和道德问题。

《密码编码学与网络安全——原理与实践（第五版）》一书内容丰富，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。

本书的第一部分由杨敏和孟庆树翻译，第二部分由王后珍翻译，前言和第三部分由王张宜翻译，第四部分由陈晶翻译，第五部分由杜瑞颖翻译，第六部分和第七部分由彭国军翻译。

本书的附录C、E、F、G、H、I由杨敏翻译，附录A、B、D、K、N、M由王张宜翻译，附录J由王后珍翻译，附录L由陈晶翻译，附录O、P、Q由杜瑞颖翻译。

全书由张焕国统稿和审校。

研究生陈新姣、王丹、梁玉、郑美凤及叶青晟等参与了翻译书稿的整理工作。

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。

译者于武汉大学珞珈山　　2011年6月

<<密码编码学与网络安全>>

内容概要

本书系统介绍了密码编码学与网络安全的基本原理和应用技术。
全书主要包括以下七个部分：对称密码部分讨论了对称加密的算法和设计原则；公钥密码部分讨论了公钥密码的算法和设计原则；密码学中的数据完整性算法部分讨论了密码学Hash函数、消息验证码和数字签名；相互信任部分讨论了密钥管理和认证技术；网络与因特网安全部分讨论了应用密码算法和安全协议为网络和Internet提供安全；法律与道德问题部分讨论了与计算机和网络安全相关的法律与道德问题。
本书的第五版与第四版相比，书中的内容和组织结构都做了较大的调整，增加了许多新内容，并首次采用了在线内容和使用Sage计算机代数系统。

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

作者简介

作者：(美国)斯托林斯 (William Sallings) 编译：王张宜 杨敏 杜瑞颖 等 注释 解说词：张焕国

<<密码编码学与网络安全>>

书籍目录

章节摘录

编辑推荐

《密码编码学与网络安全:原理与实践(第5版)》：在全球实现了电子化连接，充满病毒、黑客、电子窃听、电子欺诈的年代，安全是一个极其重要的主题。
《密码编码学与网络安全:原理与实践(第5版)》针对密码编码学和网络安全，从原理和实践两方面提供了实用的知识。
《密码编码学与网络安全:原理与实践(第5版)》适合用做密码编码学、计算机安全、网络安全专业的本科生或研究生一学期课程的教材。
在讲解密码编码学和网络安全的实用知识时，《密码编码学与网络安全:原理与实践(第5版)》还为教师和学生提供了大量的支持材料。
涵盖最新的主题，扩充了分组密码模型的内容，包含认证加密，优化并扩展了AES的讲解，扩展了伪随机数发生器的内容新增联合身份（federated identity）、HTTPS. SSH以及无线网络安全的内容，全面重写并更新了IPsec，新增关于法律和伦理的一章，使用Sage计算机代数系统演示密码编码学算法，关于密码编码学算法的全面比较，对认证和数字签名的完整比较，统一、全面地论述了相互信任的主题，比如密钥管理和用户认证，针对电子邮件安全同时介绍了PGP和S/MIME。
访问《密码编码学与网络安全:原理与实践(第5版)》的配套网站，可获得学生和教师资源，包括测试库（Testbank）、PowerPoint教案、教师用习题解答手册、教师用项目手册，书中的图和表、Java样本程序、实验室练习模板、附加的PowerPoint教案、勘误表、安全与密码编码学论坛、密码编码学演示、各章的链接、在线内容（包括在线章节和附录、重要的页面、支持文档、Sage代码例子等）。
为使《密码编码学与网络安全:原理与实践(第5版)》的中文版读者能读到原书的完整内容，特地翻译了原书的在线内容[第20章至第23章，以及附录C至附录Q。
这些内容的中文版已上载至华信教育资源网，有兴趣的读者可免费下载]，从而为中文读者提供了一本完整的中文图书。

<<密码编码学与网络安全>>

版权说明