RSA PRESS

[美] Steve Burnett
Stephen Paine 著

冯登国 周永彬 张振峰 李德全 等译

RSA Security's Official Guide To

CRYPTOGRAPHY

密码工程

实践指南

了解安全的数据加密技术的工作原理

保护网络上的机密信息

通过本书随附的CD-ROM获得当前正式的密码技术标准

清华大学出版社
http://www.tup.tsinghua.edu.cn

麦格劳-希尔教育出版集团
http://www.mheducation.com

密码工程实践指南

[美]Steve Burnett & Stephen Paine 著
冯登国 周永彬 张振峰 李德全 等译

清华大学出版社
麦格劳-希尔教育出版集团

(京)新登字 158 号

密码工程实践指南
Steve Burnett & Stephen Paine: **RSA Security's Official Guide to Cryptography**
EISBN: 0-07-213139-X

书　　名: 密码工程实践指南
译　　者: 冯登国　周永彬　张振峰　李德全　等译
出 版 者: 清华大学出版社(北京清华大学学研大厦,邮编 100084)
http://www.tup.tsinghua.edu.cn
责任编辑: 汤斌浩
印 刷 者: 北京牛山世兴印刷厂
发 行 者: 新华书店总店北京发行所
开　　本: 787×960 1/16　**印张**: 24.5　**字数**: 487 千字
版　　次: 2001 年 10 月第 1 版　2001 年 10 月第 1 次印刷
书　　号: ISBN 7-900637-18-4
印　　数: 0001～6000
定　　价: 53.00 元

序

自从20世纪70年代网络出现以来，电子工作空间的边界日益模糊。尤其是进入90年代，随着Internet及其相关技术的应用日益普及，随着电子商务的基础设施跨越传统的局域网和广域网，人们必须认识并着手面对这样的现实：电子工作空间不再处于自己的完全控制之中。

当企业开放了他们的网络，允许用户从外部访问其内部系统时，企业信息的界限就消失了。在这种环境下，对在网络上传输的各种信息提供安全性保障就变得十分关键。美国RSA信息安全(RSA Security)公司在电子安全业界享负盛名，是在电子安全领域最值得信赖的公司，它致力于开发双因素用户认证、加密和公开密钥管理系统，为有志开拓电子商务的企业建立安全稳妥的基础建设。

RSA信息安全公司的产品及技术以开放和标准为主，让企业只需就现有应用软件和网络系统执行最少的修订工作，即可轻易结合到企业的网络环境中。这些方案及技术不仅可协助企业安全地推行应用软件，更可沿用企业对现有基建设施的投资。RSA信息安全公司致力于发展网络安全的三大核心领域——公钥基础设施、认证技术以及加密技术。

但直到目前为止，广大用户对信息安全的认识和了解还远远不够，对信息安全的严重性也没有足够的重视，导致现在各种信息安全事故不断发生。因此，为了普及信息安全的相关概念、技术和知识，RSA信息安全公司也十分重视通过图书这种媒介来为广大读者和用户提供帮助。这套《RSA信息安全系列丛书》就是由RSA信息安全公司的专家撰写的，向读者介绍信息安全相关技术的科普性质读物。

《公钥基础设施：实现与管理电子安全》

随着安全性日益受到重视，认证技术和公开密钥密码系统逐步出台，在今后数年中，许多大型机构都将在整个公司范围内实施公开密钥及认证系统。而实施公开密钥密码系统就需要具备公钥基础设

施(PKI),以及为确保人事、程序及系统安全而对数字证书及加密技术进行管理所需的服务。本书就向读者展示了如何通过使用 PKI 技术,在电子商务中实现交易的安全性和实施客户信任。本书从对密码学的介绍入手,解释了用于创建公钥基础设施的各项技术,并概述了在 B2B 和 B2C 环境下实施 PKI 所需要的步骤。

《密码工程实践指南》

在网络成为人们工作生活中所必不可少的工具时,如何在网络传输和电子交易中确保信息的安全性、保密性、完整性呢?这就需要用到密码学的知识。但由于过去密码学的应用通常是与间谍活动、军事秘密联系在一起的,因此总给人一种神秘、高深的感觉。本书的目的就是希望通过一些浅显的语言和介绍,向有兴趣的读者揭开密码学的这层神秘面纱。书中解释了两种密码技术——对称密钥和公开密钥,并说明了它们之间的区别和当前的相关标准和实现,同时还通过不同的实际案例分析了应用密码技术成败的关键。

《IPSec:VPN 的安全实施》

通过在一个虚拟专用网上实现 IPSec,就可以确保最高级别的网络安全。本书解释了 IP 安全协议、实现这些协议的方法以及 VPN 互操作性。书中不仅介绍了 IPSec 的技术组成及其基础机构,还通过一个实际的例子,详细说明了 VPN 客户端以及安全网关的配置方法。本书可以说是目前市场上关于 IPSec 的图书中最权威的著作之一。

以后根据技术的发展和读者的需要,我们还会陆续推出《RSA 信息安全系列丛书》的新选题。

《RSA 信息安全系列丛书》的简体中文版版权由清华大学出版社引进,由清华大学出版社第六编辑室组织翻译、出版。在此向参与此套丛书翻译、出版工作的所有译者、编辑和其他人士表示感谢。

RSA 信息安全公司
中国办事处
http://www.rsasecurity.com
2001 年 10 月

译者序

密码技术是信息安全中的关键技术，它的有效使用可以极大地提高网络的安全性。为了有效地将密码技术集成到产品和系统之中，开发者和工程师们需要了解密码技术。将密码技术集成到产品和系统之中，就涉及到多层次人员都需要了解密码技术，如销售人员、购买者、管理者和律师等。这就要求有一本能够介绍密码技术的基本概念和用途的简明教程。Steve Burnett 所著的《密码工程实践指南》一书正是一本能满足这种需求的很好的科普读物。它一方面描述了当今世界上最广泛应用的密码的基本概念，另一方面可以使读者了解密码学是做什么的，怎么用的。我们认为，本书是密码学方面的一本很好的入门书，它可以不知不觉地将读者带进具有神秘色彩的密码学殿堂，从而揭开密码学的神秘面纱。我们相信本书一定会对密码工程实践有所裨益。

参加本书各章的翻译人员如下：前言、第 4 章、第 11 章和第 12 章由张振峰博士翻译，第 1 章和第 2 章由张兴兰博士和徐震博士翻译，第 3 章、第 6 章、第 7 章、第 8 章、第 9 章和附录 B 由周永彬博士翻译，第 5 章、第 10 章和附录 A、附录 C 由李德全博士翻译。全书最后由冯登国研究员统稿和审校。

本书的出版得到了国家 973 项目（编号：G1999035802）和国家杰出青年科学基金（编号：60025205）的支持，在此表示感谢。

感谢清华大学出版社第六编辑室的汤斌浩、赵彤伟等编辑为本书的出版提出的宝贵意见。最后，感谢所有帮助和支持我们的人。

译　者

2001 年 8 月于北京

鸣谢

ALX300 由 Compaq 计算机公司特许。

ikey2000 CryptoSwift 加速器由 Rainbow 技术公司特许。

Java 环由 Dallas Semiconductor 公司特许。

Box Blue 加速器和卡阅读器由 nCipher 公司特许。

Luna CA3—Photos 由 Chrysalis-ITS 公司特许。

Smarty 智能卡阅读器由 SmartDisk 公司特许。

RSA SecurID 卡和令牌由 RSA 信息安全公司特许。

BioMouse Plus 由美国 Biometric 公司特许。

XyLoc 邻近卡由 Ensure 技术公司特许。

Trusted Time 产品由 Datum 公司特许。

前言

欢迎阅读 RSA Press 出版的第二本书——RSA 信息安全公司的《密码工程实践指南》。

Internet 与人们日常生活的联系越来越密切，网络安全也迫在眉睫。任何一个参与在线活动的组织必须评估和控制与他们的活动相关的网络安全风险。有效地使用密码技术是网络安全风险控制策略的核心。本书指导一个组织（企业或事业单位等）正确、可靠地使用密码学网络安全技术，以保护该组织最宝贵的资产——数据——的保密性、安全性和完整性。

随着重要的技术、商业和法律事件频频发生，密码学进入了一个令人振奋的时代。本书能帮助读者更好地了解这些事件背后的技术问题。

2001 年 1 月，美国政府宣布彻底放松对强密码出口的限制。这一决定允许美国公司现在可以同世界上其他国家的公司在密码商业上竞争。本书所讨论的许多算法以前在美国被视为机密，受到严格的出口限制。

2000 年 9 月，RSA 算法的专利——据说是密码学中最重要的专利——到期了。现在任何一个公司或者个人都可以实现这个算法，这进一步增加了这一计算机史上最广为传播的技术的知名度。

2000 年 10 月，美国国家标准与技术研究所宣布了高级加密标准（Advanced Encryption Standard，AES）优胜者的选择程序，这是一个由两位比利时研究人员发明的称为 Rijndael 的算法。AES 算法的目的是取代古老的、越来越容易受到攻击的数据加密标准（Data Encryption Standard，DES）算法。在近期内，AES 有望成为该类算法中应用最为广泛的算法。

以密码学为基础的网络安全技术出现了很多新的选择，安全技术工业在短期内也得到了蓬勃发展。从密码学硬件的新发展到公开密钥基础设施中个人智能卡的使用，这些工业继续扩大了网络安全风险解决方案的可选择范围。本书在网络安全的核心密码技术方面为读者提供了坚实的基础，包括前面提到的 RSA、AES 和 DES 以及

很多其他的技术，然后在此基础上探讨了这些技术在实际应用和边沿技术中的用途。

虽然本书的确讨论了密码学的数学基础，但是其主要目的仍在于这些技术在熟知的现实生活中的应用。本书运用系统分析法探讨了如何把密码学应用到网络安全中，说明了网络安全所提供的保护程度是保护链中最薄弱的环节。

我们希望读者能喜欢本书以及 RSA Press 出版的其他图书。欢迎读者提出批评和建议。关于 RSA 信息安全公司的更多信息，请访问网站 www. rsasecurity. com；关于 RSA Press 的情况可以访问 www. rsapress. com。

Burt Kaliski
RSA 实验室主任，首席科学家
bkaliski@rsasecurity. com

致谢

首先我要感谢 Stephen Paine。他整理了初始的提议和大纲。后来为了使本书更优秀，他调整了本书的结构。是他计划了本书，我只是动手写作而已。

Osborne/McGraw Hill 的两位编辑 Besty Hardinger 和 Lee-Ann Pickrell 给了我们很多建议（大多数被接收），使得本书的语言更优美，更具有可读性，内容也更加流畅。本书封面有 Stephen Paine 和我的名字，但我认为这两位编辑应当受到感谢。

RSA 的 Blake Dournaee 花了很多时间校阅了本书。如果不是他，我们会因为他所发现的不少错误而窘迫。当然本书仍然难免有错误，这完全是 Stephen 和我的责任。

许多人帮助我们得到了实例。Reynold 数据恢复公司的 Mark Tession 和 4Sites Internet Services 的 Dennis Vanatta 为我们在第 1 章中所讨论的数据恢复提供了信息和屏幕图。Oracle 公司的 Mary Ann Davidsone 和 Matt Robshaw 帮我整理了第 2 章中的例子。RSA 的 Peter Rostin 和 Nino Marino 提供了 Keno 例子。

Osborne/McGraw Hill 的人员说我们在致谢上有完全的发言权，所以在此我需要感谢那些在本书中没有给我帮助但在我的职业生涯中给予我帮助的人们。若不是 Intergraph 的 Dave Neff，我想我不会成为如此出色的编程人员，也不可能在 RSA 取得如此成功，更不可能有机会被推荐来撰写本书。RSA 的工程技术副总 Victor Chang 雇用了我，让我参与了密码学领域和工业中各种各样有意义的工作，为我提供了 RSA 工程师这样一个很好的工作位置。RSA 实验室的天才们，特别是 Burt Kaliski 和 Matt Robshaw 向我传授了至今所知的大多数密码术。RSA 的工程师们，特别是 Dung Huynh 和 Pao-Chi Hwang 教给了我所有的密码学编码。

—Steve Burnett

我首先要感谢 Steve Burnett。我可以断定若不是他同意和我合作共同写作本书，一开始我可能就放弃了。

当然我应该感谢 RSA Press，感谢他们给了我和 Steve Burnett 这个机会来写此书。我还要感谢 Steve Elliot、Alex Corana、Betsy Hardinger、LeeAnn Pickrell 以及所有其他的 Osborne/McGraw Hill 雇员们帮我们完成本书。

Jessica Nelson 和 Blake Dournaee 为本书提供了技术校对，你们作了很出色的工作——感谢你们。特别要感谢 RSA 信息安全公司的 Mohan Atreya 和 Scott Maxwell；他们两位给予了本书很好的主意和技术投入。

感谢 RSA 信息安全公司的朋友们，感谢你们在我写作本书的那段时间里给予的忍耐和理解。

特别感谢 Jerry Mansfield，一个很好的朋友，他教给我如何面对人生。最后，感谢我家人的支持。

—Stephen Paine

序言

应用开发者从不习惯于对他们的产品增加安全性，因为他们的购买者并不关心这个问题。为产品增加安全意味着更高的开销，却不会有助于销售。如今，客户对许多产品要求加以安全保护。2000年2月16日，(美国)联邦调查局发表了如下的国会声明：

“1999年美国有1亿多个Internet用户。预计到2003年底这个数字在美国将达到1.77亿，全世界将达到5.02亿。电子商务已经作为美国经济中的一个新部分出现了，1999年销售额超过了1 000亿美元；预计到2003年电子商务会突破1万亿美元。”

同时，计算机安全研究所(Computer Security Institute，CSI)报告了不断增加的计算机犯罪：“在我们的调查中，55%的回复者曾被入侵者的恶意行为骚扰过。”了解到这个情况，你会确信发展中的公司需要安全产品。

密码学是最重要的安全工具。为了有效地把密码集成到产品上，开发者和工程师们需要了解密码术。为了证明他们出售的产品是安全的，销售和市场人员需要了解密码术。购买这些产品的客户，无论是最终使用者还是合作代理商，也需要知道密码术，这样他们才能够做出最好的选择并且正确地使用这些产品。为了把密码正确地应用到他们的系统中，IT工作者们也需要懂得密码术。甚至是律师也得了解密码术，因为地方、州和联邦政府正在颁布新法律来界定实体保护公众的秘密信息的职责。

本书是对密码学的介绍。它不是关于密码的历史(虽然你会发现一些历史典故)。它不是一个编码指南，也不是一本罗列所有密码的基础定理和证明的数学书。它也没有包含密码的方方面面；然而，它描述了当今世界上最广泛应用的密码的基本概念。读完本书，你会了解计算机密码学是做什么的、怎么用的。例如：

- 你会知道分组密码和流密码的区别，知道何时使用它们(如果某人试图向你推销一种重复使用流密码密钥的应用软件，你会知道为什么不应该购买它)。
- 知道为什么你不应该对只用于签名的密钥实施密钥恢复。

- 了解 SSL 能做什么，知道为什么它不是能够解决所有问题的安全魔弹，虽然某些电子商务站点似乎是这样认为的。
- 知道一些公司是如何在他们的产品上有效地实现密码的。
- 知道某些公司如何未能很好地应用密码（聪明人从自己的错误中学习；卓越的人从别人的错误中学习）。

当然，从本书中你还可以学到很多别的知识。

第 1 章深入探讨了现今为什么需要密码学。第 2 章到第 5 章描述了密码的基本组成部分，例如对称密钥与公钥、口令加密和数字签名。在第 6 章到第 8 章，你会发现这些组件如何通过证书和协议来创建基础设施。第 9 章告诉你特殊的硬件设施如何加强安全性。第 10 章探讨了关于数字签名的法律问题。最后，第 11 章和第 12 章给出了一些公司失败或者成功使用密码的实际例子。

全书使用标准的计算机十六进制符号。例如我们可能把一个密钥写成如下的形式：

```
0x14C608B9  62AF9086
```

许多人知道它的含义，但是如果你不知道，请参阅附录 A。它介绍了计算机业界是如何用十六进制表示比特和字节的。其中也描述了 ASCII 码——计算机中字母、数字、符号的一种标准的表示方式。

第 6 章简单描述了 ASN.1 和 BER/DER 编码。如果想深入了解这一主题，请参阅附录 B。

附录 C 提供了本书所论述的许多主题的更详细的信息。这些详细资料对于理解本书正文中所给出的概念并不重要；但是对于想更多地了解当今密码是如何应用的读者来说，这个附录是很有趣的。

最后，本书所附的 CD 中包含了 RSA 实验室关于密码学的常见问题解答（FAQ）。FAQ 中有本书所给出的许多概念的更详细的信息。例如：FAQ 描述了很多的密码数学基础、关于出口的政治问题，也提供了术语表和参考文献。我们撰写本书的目的是向大多数人解释密码。如果想深入研究就请从该 FAQ 开始。

作者简介

Steve Burnett 在 Iowa 的 Grinnell 大学和 California 的 Claremont 研究生院取得数学学位，他的主要工作是把数学转换为计算机程序，他先是在 Intergraph 公司工作，现在在 RSA 信息安全公司。他目前是首席密码工程师，负责 RSA 的 BSAFE Crypto-C 和 Crypto-J 产品，这两种密码是用 C 语言和 Java 语言编写的通用密码软件开发工具包。Burnett 经常在工业会议和大学校园里作报告。

Stephen Paine Stephen Paine 大部分的职业生涯是在安全领域中工作——以前是在美国海军陆战队和 SUN Microsystems 工作。现在他是 RSA 信息安全公司的系统工程师，在那里他为世界上的公司和开发人员讲解安全概念，并且为客户和 RSA 雇员提供培训。

审校者简介

Blake Dournaee Blake Douranee 于 1999 年加入了 RSA 信息安全公司的开发者支援小组，主要为 BSAFE 密码工具包作支持和训练。之前他在 NASA Ames 研究中心的安全开发小组工作。他在 San Luis Obispo 的 California Polytechnic 州立大学取得了计算机科学学士学位，现在是 Massachusetts 大学的一位研究生。

Jessica Nelson Jessica Nelson 有很强的计算机安全背景。作为美国空军的一名官员，她是 12 Air Force/Southern Command Defensive Information Warfare分部的先锋。她结合计算机和通信安全编写用于国防部的信息战中的程序。她从 UCSD 毕业获得物理专业学位，曾与天体物理学家 Kim Griest 博士和 Sally Ride 博士一起工作。目前她是某个欧洲安全公司的西部技术销售的负责人。

目录