HZ BOOKS
华章教育

计 算 机 科 学 丛 书

WILEY

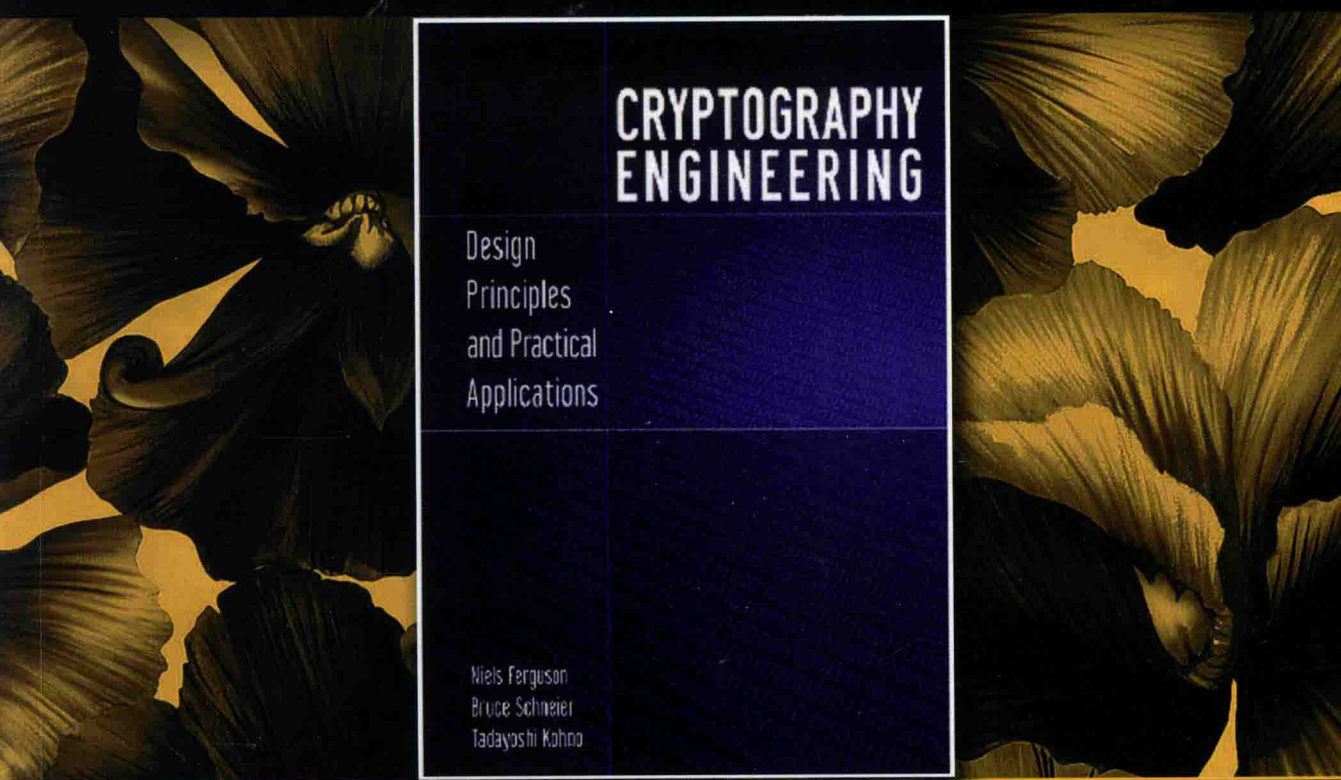
密码工程

原理与应用

尼尔斯·弗格森（Niels Ferguson）
[美] 布鲁斯·施奈尔（Bruce Schneier） 著 赵一鸣 沙朝锋 李景涛 译
大仓河野（Tadayoshi Kohno）

Cryptography Engineering

Design Principles and Practical Applications



机械工业出版社
China Machine Press

计 算 机 科 学 丛 书

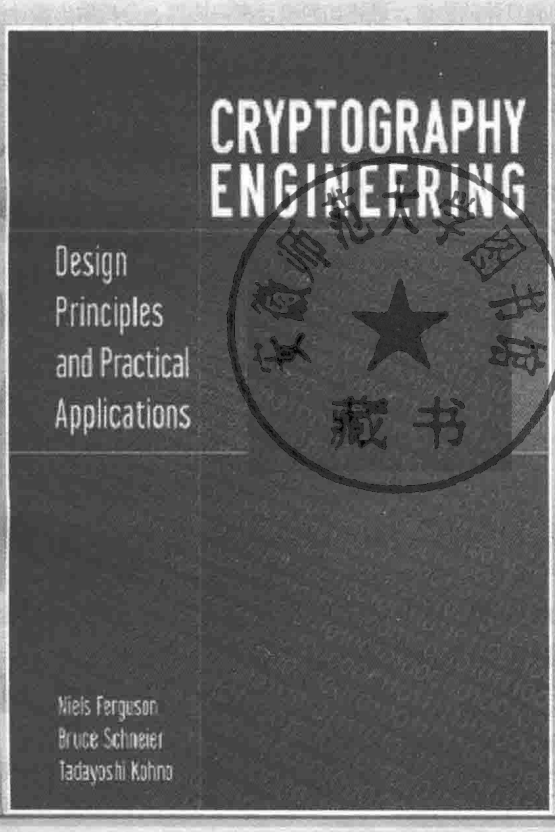
密码工程

原理与应用

尼尔斯·弗格森（Niels Ferguson）
[美] 布鲁斯·施奈尔（Bruce Schneier） 著 赵一鸣 沙朝锋 李景涛 译
大仓河野（Tadayoshi Kohno）

Cryptography Engineering

Design Principles and Practical Applications



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

密码工程：原理与应用 /（美）尼尔斯·弗格森（Niels Ferguson）等著；赵一鸣等译．
—北京：机械工业出版社，2017.7
（计算机科学丛书）
书名原文：Cryptography Engineering: Design Principles and Practical Applications

ISBN 978-7-111-57435-4

I. 密… II. ① 尼… ② 赵… III. 密码学 IV. TN918.1

中国版本图书馆 CIP 数据核字（2017）第 167697 号

本书版权登记号：图字 01-2010-4825

本书深入地探讨明确具体的协议，讲述如何设计密码协议，分析做出设计决策的原因，并指出其中可能存在的陷阱，从而帮助读者像密码学家一样思考。本书分为五部分，第一部分对密码学进行概述，第二到四部分分别讲述消息安全、密钥协商、密钥管理方面的内容，第五部分介绍标准和专利等其他问题。

本书可作为高等院校计算机安全和密码学相关专业的教材或教学参考书，也可作为应用密码工程的自学指南。

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）
责任编辑：迟振春　　责任校对：殷　虹
印　　刷：中国电影出版社印刷厂　　版　　次：2018 年 1 月第 1 版第 1 次印刷
开　　本：185mm × 260mm　1/16　　印　　张：16
书　　号：ISBN 978-7-111-57435-4　　定　　价：79.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

文艺复兴以来，源远流长的科学精神和逐步形成的学术规范，使西方国家在自然科学的各个领域取得了垄断性的优势；也正是这样的优势，使美国在信息技术发展的六十多年间名家辈出、独领风骚。在商业化的进程中，美国的产业界与教育界越来越紧密地结合，计算机学科中的许多泰山北斗同时身处科研和教学的最前线，由此而产生的经典科学著作，不仅擘划了研究的范畴，还揭示了学术的源变，既遵循学术规范，又自有学者个性，其价值并不会因年月的流逝而减退。

近年，在全球信息化大潮的推动下，我国的计算机产业发展迅猛，对专业人才的需求日益迫切。这对计算机教育界和出版界都既是机遇，也是挑战；而专业教材的建设在教育战略上显得举足轻重。在我国信息技术发展时间较短的现状下，美国等发达国家在其计算机科学发展的几十年间积淀和发展的经典教材仍有许多值得借鉴之处。因此，引进一批国外优秀计算机教材将对我国计算机教育事业的发展起到积极的推动作用，也是与世界接轨、建设真正的世界一流大学的必由之路。

机械工业出版社华章公司较早意识到“出版要为教育服务”。自 1998 年开始，我们就将工作重点放在了遴选、移译国外优秀教材上。经过多年的不懈努力，我们与 Pearson，McGraw-Hill，Elsevier，MIT，John Wiley & Sons，Cengage 等世界著名出版公司建立了良好的合作关系，从他们现有的数百种教材中甄选出 Andrew S. Tanenbaum，Bjarne Stroustrup，Brian W. Kernighan，Dennis Ritchie，Jim Gray，Afred V. Aho，John E. Hopcroft，Jeffrey D. Ullman，Abraham Silberschatz，William Stallings，Donald E. Knuth，John L. Hennessy，Larry L. Peterson 等大师名家的一批经典作品，以“计算机科学丛书”为总称出版，供读者学习、研究及珍藏。大理石纹理的封面，也正体现了这套丛书的品位和格调。

“计算机科学丛书”的出版工作得到了国内外学者的鼎力相助，国内的专家不仅提供了中肯的选题指导，还不辞劳苦地担任了翻译和审校的工作；而原书的作者也相当关注其作品在中国的传播，有的还专门为其书的中译本作序。迄今，“计算机科学丛书”已经出版了近两百个品种，这些书籍在读者中树立了良好的口碑，并被许多高校采用为正式教材和参考书籍。其影印版“经典原版书库”作为姊妹篇也被越来越多实施双语教学的学校所采用。

权威的作者、经典的教材、一流的译者、严格的审校、精细的编辑，这些因素使我们的图书有了质量的保证。随着计算机科学与技术专业学科建设的不断完善和教材改革的逐渐深化，教育界对国外计算机教材的需求和应用都将步入一个新的阶段，我们的目标是尽善尽美，而反馈的意见正是我们达到这一终极目标的重要帮助。华章公司欢迎老师和读者对我们的工作提出建议或给予指正，我们的联系方法如下：

华章网站：www.hzbook.com
电子邮件：hzjsj@hzbook.com
联系电话：（010）88379604
联系地址：北京市西城区百万庄南街 1 号
邮政编码：100037

华章科技图书出版中心

译 者 序

Cryptography Engineering: Design Principles and Practical Applications

随着信息科学技术的高速发展和广泛应用，人类社会进入信息时代。信息技术改变着人们的生活和工作方式，同时也使得信息存在着严重的不安全性、危险性及脆弱性，更容易被窃听、篡改和破坏，信息安全问题越来越成为全社会关注的焦点，并成为制约信息技术应用发展的主要瓶颈之一。密码学作为实现信息安全的核心技术，在保障信息安全的应用中具有基础性的意义，已成为信息安全应用领域人员必须了解的基础知识。近年来国内外出版了大量适合学习和了解密码学的系列书籍，从各个层面为人们展示了密码学的基本概念、基本理论和实用技术。但多数密码学书籍通常侧重于密码算法的设计以及密码协议的工作过程，而对“如何在构建信息安全系统时正确实现密码协议”介绍较少。事实上，如果在实际使用中出现问题，对信息系统的安全造成的损害可能会更大。

由 Niels Ferguson、Bruce Schneier 和 Tadayoshi Kohno 编写的这本书，让读者像密码工程师一样思考，体会将加密技术构建到产品中的技术，并领悟应用过程中的技术变化。本书涵盖了密码学的所有主要领域，对明确具体的协议的实现问题进行了深入的分析，并且每章的应用实例和动手练习利于读者更好地理解密码学知识。本书明确描述了密码学的现实约束，侧重探讨如何设计并实现一个安全的密码系统。

本书三位作者在设计和构建密码系统方面都有丰富的实践经验，Niels Ferguson 参与设计了著名密码算法 Twofish，Bruce Schneier 已在安全领域出版了 14 部著作，包括著名的《应用密码学》，Tadayoshi Kohno 是华盛顿大学的教授，他们三位还是 Skein 散列函数设计团队的成员。他们对密码算法设计到使其成功工作所需的基础设施实现上的各个环节都十分清楚，因此本书对用密码算法构建安全信息系统具有极强的指导价值，是有关密码协议设计与实现的不可多得的参考书，也适合相关课程作为教材使用。鉴于本书的特点，在出版社邀请我翻译本书时，我欣然答应。我拿到书后认真阅读并做了摘记，深有启发，深深认同书中的观点：密码学研究中，通常关注密码算法的安全性问题，而很少关注算法实现过程中的问题，较少考虑密码算法用来构建安全的信息系统过程中可能存在的安全隐患（这种隐患不是算法本身所造成的，而是在实现过程中可能出现的问题）。

感谢我的学生丁圣龙、朱晗、刘雨阳、冯超逸在我所做摘记基础上做了部分扩充工作，使得翻译工作得以延续，之后李景涛老师、沙朝锋老师和我对全书进行了完整翻译，最后我对全书进行了审定和修改。由于译者的知识和翻译水平有限，对于本书中出现的错误，恳请广大读者批评指正。

本书翻译过程中，得到了出版社负责本书编辑出版工作的相关人员的支持和鼓励，他们工作认真，一丝不苟，为出版付出了大量辛勤劳动，在此表示衷心的感谢！

赵一鸣

2017 年 10 月

大多数图书涵盖了“密码学是什么？”——现在的密码是如何设计的，以及现有的密码协议（如 SSL / TLS）是如何工作的。 Bruce Schneier 的早期著作《应用密码学》（Applied Cryptography）[⊖]就是这样。这样的书对于任何密码领域的人都是非常有价值的参考书，但与现实中密码工程师和安全工程师的需求有差距。密码工程师和安全工程师不仅需要知道当前的密码协议如何工作，还需要知道如何正确地使用密码。

要知道如何使用密码，人们必须学会像密码学家一样思考。本书旨在帮助你实现这一目标。我们通过深入的讨论做到这一点——对明确具体的协议进行深入的设计和分析，而不是对密码学中的所有协议进行泛泛的探讨。我们手把手地教你设计密码协议，分享我们做出某些设计决策的原因，并指出其中可能存在的陷阱。

通过学习如何像密码学家一样思考，你还将学习如何成为更聪明的密码使用者。你将能够查看现有的加密工具包，理解其核心功能，并了解如何使用它们。你还将更好地理解加密技术所涉及的挑战，以及如何克服这些挑战。

本书也是学习计算机安全的一本指导书。在许多方面，计算机安全是密码学的超集。计算机安全和密码学都是关于设计和评价以某些方式表现的对象（系统或算法）的，甚至在有对手的情况下。在本书中，你将学习如何在加密技术的背景下思考对手的行为。一旦知道如何像对手一样思考，你就可以将这种思维方式扩展到一般的计算机系统安全上。

历史

这本书基于 Niels Ferguson 和 Bruce Schneier 编著的《实用密码学》（Practical Cryptography），并由 Tadayoshi Kohno（Yoshi）增补内容修改而成。Yoshi 是华盛顿大学计算机科学与工程系教授，也是 Niels 和 Bruce 之前的同事。Yoshi 以《实用密码学》作为基础，将其修改为适合课堂使用和自学，同时保持了 Niels 和 Bruce 的原书主旨。

教学大纲

本书可以用作应用密码工程的自学指南，也可以用作教材。可以在关于计算机安全的一季度或一学期的课程中使用本书，例如作为 6 周或 10 周的密码学课程的基础教材，如果时间允许，还可以增加高级材料。为了方便课堂使用，我们提供以下几种可能的教学大纲。

下面的教学大纲适合于 6 周的课程。对于这一课程，假设第 1 章的内容在一般的计算机安全的更广泛背景下单独讨论，此处不考虑。

第 1 周：第 2 ～ 4 章；
第 2 周：第 5 ～ 7 章；
第 3 周：第 8 ～ 10 章；
第 4 周：第 11 ～ 13 章；
第 5 周：第 14 ～ 17 章；

⊖ 本书已由机械工业出版社翻译出版，书号为 978-7-111-44533-3，定价为 79.00 元。——编辑注

第 6 周：第 18 ～ 21 章。

以下大纲是针对 10 周的密码学课程。

第 1 周：第 1 和 2 章；

第 2 周：第 3 和 4 章；

第 3 周：第 5 和 6 章；

第 4 周：第 7 和 8 章；

第 5 周：第 9 和 10 章；

第 6 周：第 11 和 12 章；

第 7 周：第 13 和 14 章；

第 8 周：第 15 ～ 17 章；

第 9 周：第 18 ～ 20 章；

第 10 周：第 21 章。

以下大纲适用于 12 周的课程，可以增加密码学或计算机安全的高级材料。

第 1 周：第 1 和 2 章；

第 2 周：第 3 和 4 章；

第 3 周：第 5 和 6 章；

第 4 周：第 7 章；

第 5 周：第 8 和 9 章；

第 6 周：第 9（续）和 10 章；

第 7 周：第 11 和 12 章；

第 8 周：第 13 和 14 章；

第 9 周：第 15 和 16 章；

第 10 周：第 17 和 18 章；

第 11 周：第 19 和 20 章；

第 12 周：第 21 章。

本书有几种类型的练习，建议你尽可能多地完成这些练习。其中包括传统的练习，旨在测试你对加密技术的理解。但是，由于我们的目标是帮助你学习如何在真实系统中考虑加密，所以还引入了一组非传统练习（参见 1.12 节）。密码学不是孤立存在的，而是由其他硬件和软件系统、人、经济、伦理、文化差异、政治、法律等组成的更大生态系统的一部分。非传统练习是明确设计的，以促使你在真实系统和周边生态系统的上下文中考虑加密。这些练习提供了将本书的内容直接应用到真实系统中的机会。此外，通过这些练习，随着学习的推进，你将看到自己的知识不断增加。

其他信息

虽然我们努力使本书没有错误，但是无疑错误不可避免。我们为本书维护了在线勘误表，使用此勘误表的方法如下。

- 阅读本书之前，请访问 http://www.schneier.com/ce.html 并下载当前的更正列表。
- 如果你在书中发现错误，请检查其是否已在列表中。如果它不在列表中，请发邮件到 cryptographyengineering@schneier.com。我们将把错误添加到在线列表中。

希望你有一个学习密码学的美好旅程。密码学是一个奇妙和迷人的主题，希望你从本书中学到很多东西，并且像我们一样享受密码工程。

致谢

非常感谢密码学和安全社区，如果没有他们在推进这一领域研究上所做的努力，本书是不可能出现的。本书还反映了我们作为密码学家的知识和经验，非常感谢我们的同行和导师帮助我们形成对密码学的理解。

感谢 Jon Callas、Ben Greenstein、Gordon Goetz、Alex Halderman、John Kelsey、Karl Koscher、Jack Lloyd、Gabriel Maganis、Theresa Portzer、Jesse Walker、Doug Whiting、Zooko Wilcox-O'Hearn 和 Hussein Yapit，他们对本书的早期版本给出了非常有价值的反馈意见。

本书的部分内容是在华盛顿大学的本科生计算机安全课程教学中得到发展和完善的，感谢所有学生和助教。特别感谢 Joshua Barr、Jonathan Beall、Iva Dermendjieva、Lisa Glendenning、Steven Myhre、Erik Turnquist 和 Heather Underwood，他们对本书提出了具体意见和建议。

感谢 Melody Kadenko 和 Julie Svendsen 在整个编写过程中的所有行政支持。感谢 Beth Friedman 对手稿所做的文字编辑。最后，感谢 Carol Long、Tom Dinse 和整个 Wiley 团队，他们鼓励我们准备本书，并一直给予我们帮助。

我们也感谢生活中所有其他人在幕后默默无闻地工作，使我们写成了本书。

2009 年 10 月

《实用密码学》前言

Cryptography Engineering: Design Principles and Practical Applications

在过去十年中，加密技术事实上对数字系统的安全性造成的损害更多，而不是更好地增强了它。密码学在20世纪90年代早期作为互联网的安全保障登上了世界舞台。一些人认为密码学是一个伟大的技术均衡器，一个将有最低的隐私保障需求的个人与最需要安全性保障的国家情报机构放在同样地位的数学工具。有些人认为，当政府失去在网络上当警察的能力时，它会成为国家垮台的武器。其他人认为它是毒贩和恐怖分子的可怕的完美工具，他们能够利用它非常安全地进行沟通。即使是那些具有更现实态度的人也认为密码学是一种能够在这个新的在线世界中实现全球商业化的技术。

十年后，这一切都没有得到验证。尽管密码学普遍存在，但国际互联网的国界更加明显。检测和窃听犯罪通信的能力与数学相比，更多地涉及政治和人力资源。个人仍然没有机会去与强大和资金充足的政府机构对抗。全球商业的兴起与密码学的普遍性没有关系。

在大多数情况下，加密技术只是承诺给互联网用户一种假的安全感，而不是提供安全性。除了攻击者，这对任何人都不利。

产生这种现象的原因与密码学作为数学科学的关系较少，而与作为工程学科的关系很大。我们在过去十年中开发、实现和现场使用了很多加密系统。我们不擅长的是将加密安全的数学理论承诺转化为现实。事实证明这是困难的部分。

太多的工程师认为加密是一种“魔法粉末”，它们可以洒在硬件或软件上，使这些产品具有神秘的“安全”属性。太多的消费者阅读写着“加密”的产品说明，并相信同样的安全魔法粉末。审查人员只是去比较密钥长度这样的东西，并且以此为基础声明某种产品比另外一种更加安全。

决定安全性的永远都是最弱的那个环节，而密码学中的数学几乎从来不是最弱的环节。密码学的基础是重要的，但更重要的是如何实现和使用这些基础。争论一个密钥应该是112位还是128位长相当于一个巨大的木桩撞到地面，并希望攻击者正好跑到木桩下。你可以争辩该木桩是1英里[⊖]还是1.5英里高，但攻击者只是走在木桩附近。安全是一个密码学的栅栏，它是使密码学变得有效的东西。

过去十年的密码学书籍促成了这个魔法光环。一本接着一本的书宣传112位三重DES加密的优势，却没有说应该如何生成或使用它的密钥。一本接着一本的书都提出了复杂的协议，却没有提到使得这些协议工作所必需的业务和社会上的限制。一本接着一本的书将密码学解释为一个纯数学理想，却没有现实的约束，但恰恰是那些现实世界中的约束代表着密码学魔法的诺言与数字安全的现实之间的差异。

《实用密码学》也是一本关于密码学的书，但它是一本“贬损”密码学的书。我们的目标是明确描述密码学的现实约束，并谈论如何设计安全密码系统。在某些方面，这本书是Bruce Schneier第一本书《应用密码学》的续集，《应用密码学》是十年前首次出版的。然而，虽然《应用密码学》给出了密码学的广泛概述和加密技术可以提供的无数可能性，但是比较局限而且主题集中。我们不给你几十个选择，而是给你一个选项，告诉你如何正确实现它。

⊖ 1英里=1609.344米。

《应用密码学》显示了密码学作为数学科学的令人惊奇的可能性——什么是可能的，什么是可实现的，而《实用密码学》给设计和实现密码系统的人提供了具体的建议。

《实用密码学》是我们对弥合密码学的承诺和密码学的现实之间的差距所做的尝试。我们尝试通过这本书来教工程师如何使用加密来增加安全性。

我们有资格写这本书的原因是，我们两位都是经验丰富的密码学家。Bruce 以他的书《应用密码学》和《秘密和谎言》（Secrets and Lies）以及他的通讯“Crypto-Gram”而知名。Niels Ferguson 在阿姆斯特丹的 CWI（荷兰国家数学和计算机科学研究所）建立了加密支付系统，后来任职于一家名为 DigiCash 的荷兰公司。Bruce 设计了 Blowfish 加密算法，我们两人都在设计 Twofish 的团队中。Niels 的研究促成了当前这一代高效匿名支付协议的第一个例子。我们的学术论文数量加起来达到了三位数。

更重要的是，我们在设计和构建密码系统方面都有丰富的经验。从 1991 年到 1999 年，Bruce 的咨询公司 Counterpane Systems 为世界上一些最大的计算机和金融公司提供设计和分析服务。最近，Counterpane Internet Security 公司已经向全球的大公司和政府机构提供了安全监控服务。Niels 在创立自己的咨询公司 MacFergus 之前，也在 Counterpane 公司工作。我们已经看到密码学在现实世界中的存在情况，它艰难地对抗着工程实现上的现实，甚至更糟糕的是，对抗着商业上的现实。我们有资格写这本书，是因为我们不得不一次又一次地为我们的咨询客户写这些同样的内容。

如何阅读本书

与其说《实用密码学》是一本参考书，不如说它是一本叙事书。它涉及从特定算法选择的密码系统的设计，到使其成功工作所需的基础设施实现上的各个环节。我们讨论单一的加密问题（一个让两个人能够安全沟通的方法），这是几乎每个密码应用程序的核心问题。为了这个目标，我们专注于一个问题和一个设计哲学，这样我们相信可以更多地教授密码工程的现实情况。

我们认为密码学是你可以通过数学得到的最有趣的内容。我们试图把这种乐趣渗透到这本书里，希望你能够喜欢这个结果。感谢你参与到我们的旅途中。

致谢

这本书是基于我们在密码学领域工作多年的共同经验写成的。非常感谢所有与我们合作的人。他们使我们的工作很有趣，帮助我们把洞察写成书。还要感谢我们的客户，不仅因为他们提供资金，使我们能够继续密码研究，也因为他们为我们提供了写这本书所必需的真实经验。

特别感谢以下这些人的工作：Beth Friedman 进行了非常有价值的编辑工作，Denise Dick 的校对工作大大提高了稿件质量，John Kelsey 提供了关于加密内容的有价值的反馈。还要感谢 Carol Long 和 Wiley 团队的其他成员将我们的想法付诸现实。

最后，要感谢世界上所有的程序员，他们一直在编写有加密功能的代码，并将其免费提供给了全世界。

Niels Ferguson
Bruce Schneier
2003 年 1 月

关于作者

Cryptography Engineering: Design Principles and Practical Applications

Niels Feiguso 的整个职业生涯都是密码工程师。在 Eindhoven 大学学习数学后，他在 DigiCash 分析、设计和实现用来保护用户隐私的高级电子支付系统。后来，他担任 Counterpane 公司和 MacFergus 公司的密码顾问，分析了数百个系统并参与了几十个系统的设计。他参与了 Twofish 分组密码设计，对 AES 做了一些最好的初步分析，并参与了现在 WiFi 所使用的加密系统的研发。自 2004 年以来，他在微软工作，帮助设计和实现 BitLocker 磁盘加密系统。他目前在 Windows 密码小组工作，负责 Windows 和其他微软产品中的加密实现。

Bruce Schneier 是国际知名的安全技术专家，被《经济学人》杂志称为“安全教父”。他是 14 本书的作者，其中包括畅销书《超越恐惧：在一个不确定的世界中明智地思考安全》《秘密和谎言》和《应用密码学》，并发表了数百篇文章和学术论文。他的很有影响力的通讯“Crypto-Gram”和博客“Schneier on Security”有超过 25 万读者。他是电视和广播电台的常客，并且他关于安全和隐私问题的言论经常被报纸引用。他曾多次在国会作证，并且曾在多个政府技术委员会任职。他是 BT（原英国电信）的首席安全技术官。

Tadayoshi Kohno（Yoshi）是华盛顿大学计算机科学与工程系教授。他的研究兴趣是提高当前和未来技术的安全性和隐私性。他在 2003 年对 Diebold AccuVote-TS 电子投票机的源代码进行了初步安全分析，并从此将研究领域转向了从无线植入式起搏器和除颤器到云计算的新兴安全技术。他获得了国家科学基金会 CAREER 奖和 Alfred P. Sloan 研究奖学金。2007 年，鉴于他对应用密码学的贡献，入选《麻省理工学院科技评论》全球青年科技创新人才榜（TR35），是 35 岁以下的世界顶级创新者之一。他在加州大学圣迭戈分校获得计算机科学博士学位。

Niels、Bruce 和 Yoshi 是 Skein 散列函数设计团队的成员，该团队是 NIST 的 SHA-3 竞赛的参与者之一。

第一部分

Cryptography Engineering: Design Principles and Practical Applications

概　述