网络与信息安全技术丛书

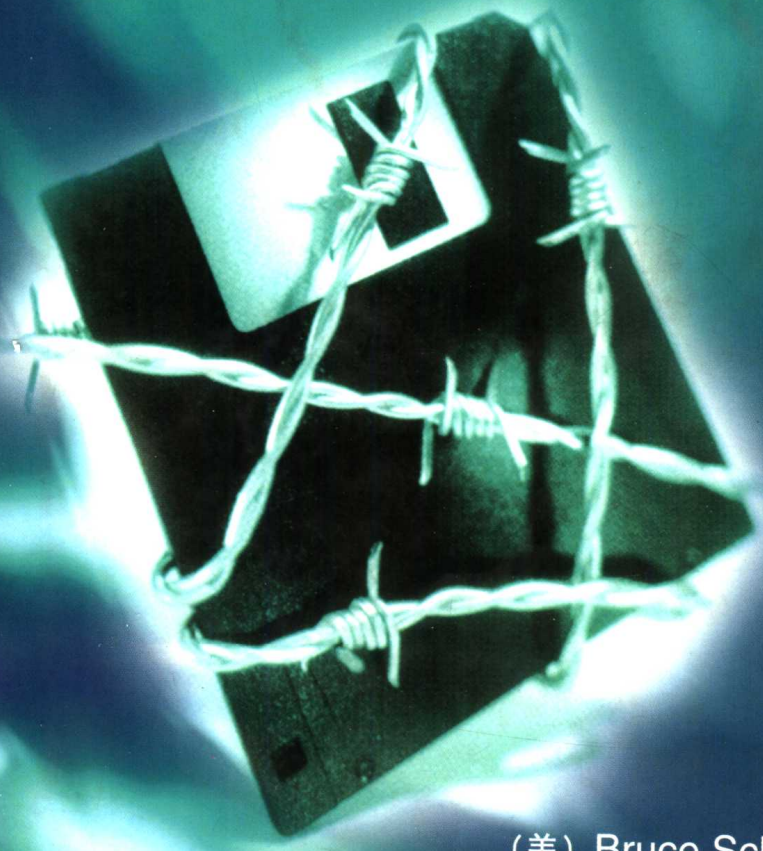
应用密码学

协议、算法与C源程序

Applied Cryptography

Protocols, algorithms, and source code in C

(Second Edition)



(美) Bruce Schneier 著

吴世忠 祝世雄 张文政 等译

机械工业出版社
China Machine Press

WILEY

网络与信息安全技术丛书

应用密码学

——协议、算法与C源程序

（美）Bruce Schneier 著

吴世忠 祝世雄 张文政 等译

何德全 审校

机械工业出版社
China Machine Press

本书真实系统地介绍了密码学及该领域全面的参考文献。

全书共分四个部分，首先定义了密码学的多个术语，介绍了密码学的发展及背景，描述了密码学从简单到复杂的各种协议，详细讨论了密码技术，并在此基础上列举了如DES、IDEA、RSA、DSA等10多个算法以及多个应用实例，并提供了算法的源代码清单。

全书内容广博权威，具有极大的实用价值。自出版以来，得到业内专家的高度赞誉，是致力于密码学研究的专业及非专业人员一本难得的好书。

Bruce Schneier: Applied Cryptography Second Edition: protocols, algorithms, and source code in C.

Authorized translation from the English language edition published by John Wiley & Sons, Inc.

本书版权登记号：图字：01－1999－2356

图书在版编目（CIP）数据

应用密码学：协议、算法与C源程序/（美）施奈尔(Schneier,B.)著；吴世忠等译. —北京：机械工业出版社，2000.1

（网络与信息安全技术丛书）

书名原文：Applied Cryptography Second Edition:protocols,algorithms,and source code in C.

ISBN 7-111-07588-9

Ⅰ.应… Ⅱ.①施… ②吴… Ⅲ.电子计算机-密码-理论 Ⅳ.TP309

中国版本图书馆CIP数据核字（1999）第55432号

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：陈 谊

北京市密云县印刷厂印刷·新华书店北京发行所发行

2000年1月第1版 2000年5月第3次印刷

787mm×1092mm 1/16·35.25印张

印数：11 001－16 000册

定价：49.00元

译 者 序

自密码学从外交情报和军事领域走向公开后，密码学文献难觅的窘境已大为改观，但密码学资料的晦涩难懂却依然如故。广大研究人员和读者一直盼望能有一本全面介绍当代密码学现状且可读性强的著作。Bruce Schneier 所著《Applied Cryptography: protocols, algorithms, and source code in C》一书正是这样一部集大成之作。本书以生动的描述和朴实的文风将当代密码学的方方面面熔于一炉，1994 年第 1 版一经推出即在国际上引起广泛关注，成为近几年来引用最多，销量最大的密码学专著，极大地推动了国际密码学研究与应用的发展。作者顺应近年来世界各国对信息安全普遍关注的趋势，结合了第 1 版问世以来密码学的新成果，于 1996 年推出了第 2 版，仍是好评如潮。本书即根据第 2 版译出。

本书作者没有将密码学的应用仅仅局限在通信保密性上，而是紧扣密码学的发展轨迹，从计算机编程和网络化应用方面，阐述了密码学从协议、技术、算法到实现的方方面面，该书详细解释了大量的新概念，如盲签名、失败-终止签名、零知识证明、位承诺、数字化现金和保密的多方计算等，向读者全面展示了现代密码学的新进展。

本书的核心部分自然是论述密码协议、技术和算法的一系列章节。作者收集了大量的公开密钥和私人密钥密码体制的实例，内容几乎涵盖了所有已公开发表的具有实用性的密码算法。作者将它们分门别类，一一评论。其中，对密码技术中密钥管理技术和算法的分析与总结详尽全面；对数 10 种密码算法的软件实现提出的建议务实可行；对前苏联和南非的一些算法的介绍更是引人入胜。对编程人员和通信专业人士来说，尤若百科全书。难怪美国 Wired 杂志要说这是一本美国国家安全局永远也不愿看到它问世的密码学著作。此外作者还简述了各种散列函数和签名方案，并结合实例说明了如何有效地利用现有的工具箱，特别指出了实现保密协议的方法，比如盲签名和零知识证明。同时还涉猎了密码学领域中不少时髦的话题，比如阈下信道、秘密共享、隐密技术和量子密码学等。

该书的最后一部分也颇具特色，它以“真实世界”为题，向人们展示了密码学应用于社会的真实情况。首先作者用 10 多个实际的例子，讨论密码学应用于计算机网络的现实情况，内容包括了国外大多数的商用保密协议，如 IBM 公司的密钥管理方案、应用较多的 Kryptoxnight、ISO 的鉴别框架、因特网中的保密增强型电子邮件产品 PEM 以及 PGP 安全软件，甚至还讨论了密码学界的热门话题——美国军用保密电话 STU-Ⅲ、商用密码芯片 Clipper 和 CAPSTONE。接着作者从政治角度探讨了美国的密码政策，其中对围绕专利的争论、出口许可证的管理和新近提出的密钥第三方托管的评说，都让国内读者耳目一新。

当然，纵览全书，也不难看出该书的不足，如序列密码、密码的形式证明、密码学在金融系统（或银行）和军事系统中的应用等方面的内容略显不足。加之本书内容广博，作者在对引用资料的使用上也有一些失误。但是，正如作者在前言中所说，本书的目的是要将现代密码学的精髓带给计算机编程人员、通信与信息安全专业人员和对此有兴趣的爱好者，以此观之，上述的缺陷当在情理之中。

本书的正式翻译与出版，动议于中国工程院何德全院士所指导的信息安全与应用密码学博士研究生的教学计划，得益于信息产业部电子第三十研究所及四川大学等单位的大力支持。参加本书翻译和校对的同志有：吴世忠、祝世雄、张文政、朱甫臣、龚奇敏、钟卓新、蒋继洪、

方关宝、黄月江、李川、谭兴烈、王佩春、曾兵、韦文玉、黄澄、罗超、王英、伍环玉、蒋洪志、陈维斌等。本书最后由吴世忠、祝世雄统稿。何德全院士在百忙之中审校了全部译稿。

必须指出的是，该书内容浩繁，由多人翻译，限于水平和经验，加之密码学的很多概念在译法上本身就有难度，故而谬误在所难免，敬请读者见谅。

译　者

1999 年 12 月

于中国国家信息安全测评认证中心

W. 迪　菲　序

密码学文献有一个奇妙的发展历程，当然，密而不宣总是扮演着主要角色。第一次世界大战之前，密码学重要的进展很少出现在公开文献中，但该领域却和其他专业学科一样向前发展着。直到1918年，20世纪最有影响的密码分析文章之一——William F. Friedman的专题论文The Index of Coincidence and Its Applications in Cryptography（《重合指数及其在密码学中的应用》）[577]作为私立Riverbank实验室的一份研究报告问世了。其实，这篇论文所涉及的工作是在战时完成的。同年，加州奥克兰的Edward H.Hebern申请了第一个转轮机专利[710]，这种装置在差不多50年里被指定为美军的主要密码设备。

然而，第一次世界大战之后，情况开始变化，完全处于秘密工作状态的美国陆军和海军的机要部门开始在密码学方面取得根本性的进展。在三、四十年代，有多篇基础性的文章出现在公开的文献中，还出现了几篇专题论文，只不过这些论文的内容离当时真正的技术水平相去甚远。战争结束时，情况急转直下，公开的文献几乎殆尽。只有一个突出的例外，那就是Claude Shannon的文章The Communication Theory of Secrecy Systems（《保密系统的通信理论》）[1432]出现在1949年的Bell System Technical Journal（《贝尔系统技术杂志》）上，它类似于Friedman 1918年的文章，也是战时工作的产物。这篇文章在第二次世界大战结束后即被解密，可能是由于失误。

从1949年到1967年，密码学文献近乎空白。在1967年，一部与众不同的著作——David Kahn的The Codebreakers（《破译者》）[794]——出现了，它并没有任何新的技术思想，但却对密码学的历史作了相当完整的记述，包括提及政府仍然认为是秘密的某些事情。这部著作的意义不仅在于它涉及到了相当广泛的领域，而且在于它使成千上万原本不知道密码学的人了解了密码学。新的密码学文章慢慢地开始源源不断地被编写出来了。

大约在同一时期，早期为空军研制敌我识别装置的Horst Feistel在位于纽约约克镇高地的IBM Watson实验室里花费了毕生精力致力于密码学的研究。在那里他开始着手进行美国数据加密标准（Data Encryption Standard，DES）的研究，到70年代初期，IBM发表了Feistel和他的同事在这个课题方面的几篇技术报告[1482,1484,552]。

这就是我于1972年底涉足密码学领域时的情形，当时密码学的文献还不丰富，但却也包括一些非常有价值的东西。

密码学提出了一个一般的学科领域都难以遇到的难题：即它需要密码学和密码分析学紧密结合互为促进。这是由于缺乏实际通信检验所致。提出一个表面上看似不可破的系统并不难，许多学究式的设计就非常复杂，以至于密码分析家不知从何入手，分析这些设计中的漏洞远比原先设计它们更难。结果是，那些本可以强劲推动学术研究的竞争过程在密码学中并没起多大作用。

当我和Martin Hellman在1975年提出公开密钥密码学[496]时，我们的一种间接贡献是引入了一个看来不易解决的难题。现在一个有抱负的密码体制设计者能够提出被认为是很聪明的一些东西——这些东西比只是把有意义的正文变成无意义的乱语更有用。结果研究密码学的人数，召开的会议，发表的论文和专著都惊人地增加了。

我在接受Donald E.Fink奖（该奖是奖给在IEEE杂志上发表过最好文章的人，我和Hell-

man 在 1980 年共同获得该奖）发表演讲时，告诉听众，我在写作 Privacy and Authentication（保密性与鉴别）一文时，有一种体验——这种体验，我相信即使在那些参加 IEEE 授奖会的著名学者们当中也是罕见的：我写的那篇文章，并非我的研究结果而是我想要研究的课题。因为在我首次沉迷于密码学的时候，这类文章根本就找不到。如果那时我可以走进斯坦福书店，挑选现代密码学的书籍，我也许能在多年前就了解这个领域了。但是在 1972 年秋季，我能找到的资料仅仅是几篇经典论文和一些难以理解的技术报告而已。

现在的研究人员再也不会遇到这样的问题了，他们的问题是要在大量的文章和书籍中选择从何处入手。研究人员如此，那些仅仅想利用密码学的程序员和工程师又会怎样呢？这些人会转向哪里呢？直到今天，在能够设计出一般的文章中所描述的那类密码实用程序之前，花费大量时间去寻找并研究那些文献仍是很有必要的。

本书正好填补了这个空白。作者 Bruce Schneier 从通信保密性的目的和达到目的所用的基本程序实例入手，对 20 年来公开研究的全部成果作了全景式的概括。书名开门见山：从首次叫某人进行保密会话的世俗目的，到数字货币和以密码方式进行保密选举的可能性，到处你都可以发现应用密码学的用处。

Schneier 不满足于这本书仅仅涉及真实世界（因为此书叙述了直至代码的全部过程），他还叙述了发展密码学和应用密码学的那些领域，讨论了从国际密码研究协会直到国家安全局这样的一些机构。

在 70 年代后期和 80 年代初期，当公众在密码学方面的兴趣显示出来时，国家安全局（NSA），即美国官方密码机构曾多次试图平息它。第一次是一名长期在 NSA 工作的雇员的一封信，据说这封信是这个雇员自己写的，此雇员自认是如此，表面上看来亦是如此。这封信是发给 IEEE 的，它警告密码资料的出版违反了国际武器交易条例（ITAR）。然而这种观点并没有被条例本身所支持，条例明显不包括已发表的资料。但这封信却为密码学的公开实践和 1977 年的信息论专题研讨会做了许多意想不到的宣传。

一个更为严重的事态发生在 1980 年，当时 NSA 为美国教育委员会提供资金，说服国会对密码学领域的出版物进行合法地控制，结果与 NSA 的愿望大相经庭，形成了密码学论文自愿送审的程序。研究人员在论文发表之前需就发表是否有损国家利益征询 NSA 的意见。

随着 80 年代的到来，NSA 将重点更多的集中在密码学的实际应用，而不是研究上。现有的法律授权 NSA 通过国务院控制密码设备的出口。随着商务活动的日益国际化和世界市场上美国份额的减退，国内外市场上需要单一产品的压力增加了。这种单一产品受到出口控制，于是 NSA 不仅对出口什么，而且也对在美国出售什么都施加了相当大的影响。

密码学的公开使用面临一种新的挑战，政府建议在可防止涂改的芯片上用一种秘密算法代替广为人知且随处可得的 DES，这些芯片将含有政府监控所需的编纂机制。这种“密钥托管”计划的弊病是它潜在地损害了个人隐私权，并且以前的软件加密不得不以高价增用硬件来实现。迄今，密钥托管产品正值熊市，这种方案却已经引起了广泛的批评，特别是那些独立的密码学家怨声载道。然而，人们看到的更多的是编程技术的未来而不是政治，并且还加倍地努力向世界提供更强的密码，这种密码能够实现对公众的监视。

从出口控制法律涉及第一修正案的意见来看，1980 年发生了大倒退，当时 Federal Register 公布了对 ITAR 的修正，其中提到：“……增加的条款清楚地说明，技术数据出口的规定并不干预第一修正案中个人的权利”，但事实上第一修正案和出口控制法律的紧张关系还未消除，最近由 RSA 数据安全公司召开的一次会议清楚地表明了这一点，从出口控制办公室来的 NSA 的代表表达了意见：发表密码程序的人从法律上说是处在“灰色领域”。如果真是这样的话，

本书第1版业已曝光，内容也处在“灰色领域”中了。本书自身的出口申请已经得到军需品控制委员会当局在出版物条款下的认可，但是，装在磁盘上的程序的出口申请却遭到拒绝。

NSA的策略从试图控制密码研究到紧紧抓住密码产品的开发和应用的改变，可能是由于认识到即便世界上所有最好的密码学论文都不能保护哪怕是一位的信息。如果束之高阁，本书也许不比以前的书和文章更好，但若置于程序员编写密码的工作站旁时，这本书无疑是最好的。

W. 迪菲（Whitfield Diffie）
于加州 Mountain View

前　言

世界上有两种密码：一种是防止你的小妹妹偷看你的文件；另一种是防止当局阅读你的文件资料。本书写的是后一种情况。

如果把一封信锁在保险柜中，把保险柜藏在纽约的某个地方…，然后告诉你去看这封信，这并不是安全，而是隐藏。相反，如果把一封信锁在保险柜中，然后把保险柜及其设计规范和许多同样的保险柜给你，以便你和世界上最好的开保险柜的专家能够研究锁的装置，而你还是无法打开保险柜去读这封信，这才是安全的概念。

许多年来，密码学是军队独家专有的领域。NSA 以及前苏联、英国、法国、以色列及其他国家的安全机构已将大量的财力投入到加密自己的通信，同时又千方百计地去破译别人的通信的残酷游戏之中。面对这些政府，个人既无专业知识又无足够财力保护自己的秘密。

在过去 20 年里，公开的密码学研究爆炸性地增长。从第二次世界大战以来，当普通公民还在长期使用经典密码时，计算机密码学已成为世界军事独占的领域。今天，最新的计算机密码学已应用到军事当局的高墙之外，现在就连非专业人员都可以利用密码技术去阻止最强大的敌人，包括军方的安全机构。

普通百姓真的需要这种保密性吗？是的，他们可能正在策划一次政治运动，讨论税收或正干一件非法的事情；也可能正设计一件新产品，讨论一种市场策略，或计划接管竞争对手的生意；或者可能生活在一个不尊重个人隐私权的国家，也可能做一些他们自己认为并非违法实际却是非法的事情。不管理由是什么，他的数据和通信都是私人的、秘密的，与他人无关。

本书正好在混乱的年代发表。1994 年，克林顿当局核准了托管加密标准（包括 Clipper 芯片和 Fortezza 卡），并将数字电话法案签署成为法律。这两个行政令企图确保政府实施电子监控的能力。

一些危险的 Orwellian 假设在作祟：即政府有权侦听私人通信，个人对政府保守秘密是错误的。如果可能，法律总有能力强制实施法院授权的监控，但是，这是公民第一次被迫采取“积极措施”，以使他们自己能被监控。这两个行政令并不是政府在某个模糊范围内的简单倡议，而是一种先发制人的单方面尝试，旨在侵占以前属于公民的权力。

Clipper 和数字电话不保护隐私，它强迫个人无条件地相信政府将尊重他们的隐私。非法窃听小马丁·路德·金电话的执法机构，同样也能容易地窃听用 Clipper 保护的电话。最近，地方警察机关在不少管区内都有因非法窃听而被控有罪或被提出民事诉讼，这些地方包括马里兰、康涅狄格、佛蒙特、佐治亚、密苏里和内华达。为了随时方便警察局的工作而配置这种技术是很糟糕的想法。

这给我们的教训是采用法律手段并不能充分保护我们自己，还需要用数学来保护自己。加密太重要了，不能让给政府独享。

本书为你提供了一些可用来保护自己隐私的工具。提供密码产品可能宣布为非法，但提供有关的信息绝不会犯法。

怎样阅读这本书

我写作本书的目的是为了在真实地介绍密码学的同时给出全面的参考文献。我尽量在不损

失正确性的情况下保持文本的可读性，我不想使本书成为一本数学书。虽然我无意给出任何错误信息，但匆忙中理论难免有失严谨。对形式方法感兴趣的人，可以参考大量的学术文献。

第 1 章介绍了密码学，定义了许多术语，简要讨论了计算机出现前密码学的情况。

第一部分（第 2～6 章）描述密码学的各种协议：人们能用密码学做什么。协议范围从简单（一人向另一人发送加密消息）到复杂（在电话上抛掷硬币）再到深奥（秘密的和匿名的数字货币交易）。这些协议中有些一目了然，有些却十分奇异。密码学能够解决大多数人绝没有认识到的许多问题。

第二部分（第 7～10 章）讨论密码技术。对密码学的大多数基本应用来说，这一部分的四章都很重要。第 7 章和第 8 章讨论密钥：密钥应选多长才能保密，怎样产生、存储密钥，怎样处理密钥等等。密钥管理是密码学最困难的一部分，经常是保密系统的一个致命弱点；第 9 章讨论了使用密码算法的不同方法；第 10 章给出了与算法有关的细节：怎样选择、实现和使用算法。

第三部分（第 11～23 章）列出了多个算法。第 11 章提供了数学背景，如果你对公开密钥算法感兴趣，那么这一章你一定要了解。如果你只想实现 DES（或类似的东西），则可以跳过这一章；第 12 章讨论 DES：DES 算法、它的历史、安全性和一些变形；第 13～15 章讨论其他的分组算法。如果你需要比 DES 更保密的算法，请阅读 IDEA 和三重 DES 算法这节。如果你想知道一系列比 DES 算法更安全的算法，就请读完整章；第 16 章和第 17 章讨论序列密码算法；第 18 章集中讨论单向散列函数。虽然讨论了多种单向散列函数，但 MD5 和 SHA 是最通用的；第 19 章讨论公开密钥加密算法。第 20 章讨论了公开密钥数字签名算法；第 21 章讨论了公开密钥鉴别算法；第 22 章讨论了公开密钥交换算法。几种重要的公开密钥算法分别是 RSA、DSA、Fiat-Shamir 和 Diffie-Hellman 算法；第 23 章有更深奥的公开密钥算法和协议。这一章的数学知识非常复杂，请系好你的安全带。

第四部分（第 24～25 章）转向密码学的真实世界。第 24 章讨论这些算法和协议的一些实际实现；第 25 章接触到围绕密码学的一些政治问题，这些章节并不全面。

此外，书中还包括在第三部分中讨论的 10 个算法的源代码清单，由于篇幅的限制，不可能给出所有的源代码，况且，密码的源代码不能出口（非常奇怪的是，国务院允许本书的第 1 版和源代码出口，但不允许含有同样源代码的计算机磁盘的出口）。配套的源代码盘包括的源代码比本书中列出的要多得多，这也许是除军事机构以外最大的密码源代码集。我只能给住在美国和加拿大的公民发送源代码盘，但我希望有一天这种情况会改变。

对这本书的一种批评，是它的广博性代替了可读性。这是对的，但我想给可能是偶然在学术文献或产品中需要一个算法的人提供一个参考。密码学领域正日趋热门，这是第一次把这么多资料收集在一本书中。即使这样，还是有许多东西限于篇幅舍弃了，我尽量保留了那些我认为是重要的、有实用价值的或者是有趣的专题。如果我对某一专题讨论不深，我会给出深入讨论这些专题的参考文献。

我在写作过程中已尽力查出和根除书中的错误，但我相信不可能消除所有的错误。第 2 版肯定比第 1 版的错误少得多。谬误表可以从我这里得到，并且它被定期发往 Usenet 的新闻组 sci.crypt。如果读者发现错误，请通知我，我将不胜感谢。

B. 施奈尔（Bruce Schneier）

目　录

第二部分 密码技术

第三部分 密码算法