

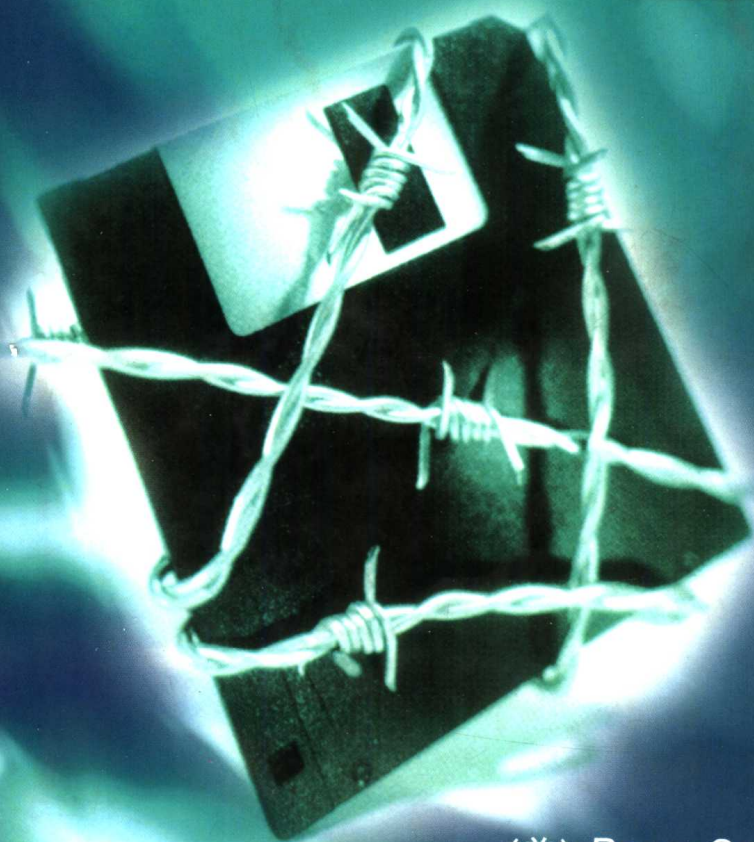
应用密码学

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



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.

Copyright © 1996 by John Wiley & Sons, Inc.

All rights reserved.

本书中文简体字版由约翰-威利父子公司授权机械工业出版社独家出版。未经出版者书面许可,不得以任何方式复制或抄袭本书的任何部分。

版权所有,侵权必究。

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

凡购本书, 如有倒页、脱页、缺页, 由本社发行部调换

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,比如阙下信道、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 的愿望大相径庭, 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, 而且也对在出口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。错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

译者序

W. 迪菲序

前言

第1章 基础知识	1
1.1 专业术语	1
1.1.1 发送者和接收者	1
1.1.2 消息和加密	1
1.1.3 鉴别、完整性和抗抵赖	2
1.1.4 算法和密钥	2
1.1.5 对称算法	3
1.1.6 公开密钥算法	3
1.1.7 密码分析	4
1.1.8 算法的安全性	6
1.1.9 过去的术语	7
1.2 隐写术	7
1.3 代替密码和换位密码	7
1.3.1 代替密码	7
1.3.2 换位密码	8
1.3.3 转轮机	9
1.3.4 进一步的读物	10
1.4 简单异或	10
1.5 一次一密乱码本	11
1.6 计算机算法	13
1.7 大数	13

第一部分 密码协议

第2章 协议结构模块	15
2.1 协议概述	15
2.1.1 协议的目的	16
2.1.2 协议中的角色	16
2.1.3 仲裁协议	16
2.1.4 裁决协议	18
2.1.5 自动执行协议	19
2.1.6 对协议的攻击	19
2.2 使用对称密码学通信	20
2.3 单向函数	21
2.4 单向散列函数	21
2.5 使用公开密钥密码学通信	22
2.5.1 混合密码系统	23

2.5.2 Merkle 的难题	24
2.6 数字签名	24
2.6.1 使用对称密码系统和仲裁者对文件签名	25
2.6.2 数字签名树	26
2.6.3 使用公开密钥密码术对文件签名	26
2.6.4 文件签名和时间标记	26
2.6.5 使用公开密钥密码学和单向散列函数对文件签名	27
2.6.6 算法和术语	27
2.6.7 多重签名	28
2.6.8 抗抵赖和数字签名	28
2.6.9 数字签名的应用	29
2.7 带加密的数字签名	29
2.7.1 重新发送消息作为收据	29
2.7.2 阻止重新发送攻击	30
2.7.3 对公开密钥密码术的攻击	30
2.8 随机和伪随机序列的产生	31
2.8.1 伪随机序列	31
2.8.2 密码学意义上安全的伪随机序列	32
2.8.3 真正的随机序列	32
第3章 基本协议	33
3.1 密钥交换	33
3.1.1 对称密码学的密钥交换	33
3.1.2 公开密钥密码学的密钥交换	33
3.1.3 中间人攻击	34
3.1.4 连锁协议	34
3.1.5 使用数字签名的密钥交换	35
3.1.6 密钥和消息传输	35
3.1.7 密钥和消息广播	36
3.2 鉴别	36
3.2.1 使用单向函数鉴别	36
3.2.2 字典式攻击和 salt	36
3.2.3 SKEY	37
3.2.4 使用公开密钥密码术鉴别	37
3.2.5 使用连锁协议互相鉴别	38
3.2.6 SKID	39

3.2.7 消息鉴别	39	4.9.4 模糊点	62
3.3 鉴别和密钥交换	39	4.10 公平的硬币抛掷	62
3.3.1 Wide-Mouth Frog 协议	40	4.10.1 使用单向函数的抛币协议	63
3.3.2 Yahalom 协议	40	4.10.2 使用公开密钥密码术的抛币 协议	64
3.3.3 Needham-Schroeder 协议	41	4.10.3 抛币入井协议	64
3.3.4 Otway-Rees 协议	41	4.10.4 使用抛币产生密钥	65
3.3.5 Kerberos 协议	42	4.11 智力扑克	65
3.3.6 Neuman-Stubblebine 协议	42	4.11.1 三方智力扑克	65
3.3.7 DASS 协议	43	4.11.2 对扑克协议的攻击	66
3.3.8 Denning-Sacco 协议	44	4.11.3 匿名密钥分配	66
3.3.9 Woo-Lam 协议	44	4.12 单向累加器	67
3.3.10 其他协议	45	4.13 秘密的全或无泄露	68
3.3.11 学术上的教训	45	4.14 密钥托管	68
3.4 鉴别和密钥交换协议的形式分析	45	第 5 章 高级协议	71
3.5 多密钥公开密钥密码学	47	5.1 零知识证明	71
3.6 秘密分割	49	5.1.1 基本的零知识协议	71
3.7 秘密共享	49	5.1.2 图同构	73
3.7.1 有骗子的秘密共享	50	5.1.3 汉密尔顿圈	74
3.7.2 没有 Trent 的秘密共享	51	5.1.4 并行零知识证明	74
3.7.3 不暴露共享的秘密共享	51	5.1.5 非交互式零知识证明	75
3.7.4 可验证的秘密共享	51	5.1.6 一般性	76
3.7.5 带预防的秘密共享	51	5.2 身份的零知识证明	76
3.7.6 带除名的秘密共享	51	5.2.1 国际象棋特级大师问题	77
3.8 数据库的密码保护	52	5.2.2 黑手党骗局	77
第 4 章 中级协议	53	5.2.3 恐怖分子骗局	77
4.1 时间标记服务	53	5.2.4 建议的解决方法	77
4.1.1 仲裁解决方法	53	5.2.5 多重身份骗局	78
4.1.2 改进的仲裁解决方法	53	5.2.6 出租护照	78
4.1.3 链接协议	54	5.2.7 成员资格证明	78
4.1.4 分布式协议	54	5.3 盲签名	79
4.1.5 进一步的工作	55	5.3.1 完全盲签名	79
4.2 阙下信道	55	5.3.2 盲签名协议	79
4.2.1 阙下信道的应用	56	5.3.3 专利	81
4.2.2 杜绝阙下的签名	56	5.4 基于身份的公开密钥密码学	81
4.3 不可抵赖的数字签名	57	5.5 不经意传输	81
4.4 指定的确认人签名	58	5.6 不经意签名	83
4.5 代理签名	58	5.7 同时签约	83
4.6 团体签名	59	5.7.1 带有仲裁者的签约	83
4.7 失败-终止数字签名	60	5.7.2 无需仲裁者的同时签约: 面对 面	83
4.8 加密数据计算	60	5.7.3 无需仲裁者的同时签约: 非面 对面	84
4.9 位承诺	60	5.7.4 无需仲裁者的同时签约: 使用 密码术	85
4.9.1 使用对称密码学的位承诺	61		
4.9.2 使用单向函数的位承诺	61		
4.9.3 使用伪随机序列发生器的位承 诺	62		

5.8 数字证明邮件	86
5.9 秘密的同时交换	87
第6章 深奥的协议	88
6.1 保密选举	88
6.1.1 简单投票协议1	88
6.1.2 简单投票协议2	88
6.1.3 使用盲签名投票	89
6.1.4 带有两个中央机构的投票	89
6.1.5 带有单个中央机构的投票	90
6.1.6 改进的带有单个中央机构的投票	90
6.1.7 无需中央制表机构的投票	91
6.1.8 其他投票方案	94
6.2 保密的多方计算	94
6.2.1 协议1	94
6.2.2 协议2	95
6.2.3 协议3	95
6.2.4 协议4	96
6.2.5 无条件多方安全协议	96
6.2.6 保密电路计算	96
6.3 匿名消息广播	97
6.4 数字现金	98
6.4.1 协议1	99
6.4.2 协议2	99
6.4.3 协议3	100
6.4.4 协议4	100
6.4.5 数字现金和高明的犯罪	102
6.4.6 实用化的数字现金	103
6.4.7 其他数字现金协议	103
6.4.8 匿名信用卡	104

第二部分 密码技术

第7章 密钥长度	105
7.1 对称密钥长度	105
7.1.1 穷举攻击所需时间和金钱估计	106
7.1.2 软件破译机	107
7.1.3 神经网络	108
7.1.4 病毒	108
7.1.5 中国式抽彩法	108
7.1.6 生物工程技术	109
7.1.7 热力学的局限性	110
7.2 公开密钥长度	110
7.2.1 DNA 计算法	114
7.2.2 量子计算法	115

7.3 对称密钥和公开密钥长度的比较	115
7.4 对单向散列函数的生日攻击	116
7.5 密钥应该多长	116
7.6 小结	117
第8章 密钥管理	118
8.1 产生密钥	118
8.1.1 减少的密钥空间	118
8.1.2 弱密钥选择	119
8.1.3 随机密钥	120
8.1.4 通行短语	121
8.1.5 X9.17 密钥产生	122
8.1.6 DoD 密钥产生	122
8.2 非线性密钥空间	122
8.3 传输密钥	123
8.4 验证密钥	124
8.4.1 密钥传输中的错误检测	125
8.4.2 解密过程中的错误检测	125
8.5 使用密钥	125
8.6 更新密钥	126
8.7 存储密钥	126
8.8 备份密钥	127
8.9 泄露密钥	128
8.10 密钥有效期	128
8.11 销毁密钥	129
8.12 公开密钥的密钥管理	129
8.12.1 公开密钥证书	130
8.12.2 分布式密钥管理	131
第9章 算法类型和模式	132
9.1 电子密码本模式	132
9.2 分组重放	133
9.3 密码分组链接模式	135
9.3.1 初始向量	135
9.3.2 填充	136
9.3.3 错误扩散	137
9.3.4 安全问题	137
9.4 序列密码算法	138
9.5 自同步序列密码	139
9.6 密码反馈模式	140
9.6.1 初始化向量	140
9.6.2 错误扩散	141
9.7 同步序列密码	141
9.8 输出反馈模式	142
9.8.1 初始化向量	142
9.8.2 错误扩散	143
9.8.3 安全问题	143

9.8.4 OFB 模式中的序列密码	144	11.3.1 模运算	167
9.9 计数器模式	144	11.3.2 素数	169
9.10 其他分组密码模式	144	11.3.3 最大公因子	170
9.10.1 分组链接模式	144	11.3.4 求模逆元	171
9.10.2 扩散密码分组链接模式	145	11.3.5 求系数	173
9.10.3 带校验和的密码分组链接	145	11.3.6 费尔马小定理	173
9.10.4 带非线性函数的输出反馈	145	11.3.7 欧拉 φ 函数	173
9.10.5 其他模式	146	11.3.8 中国剩余定理	173
9.11 选择密码模式	146	11.3.9 二次剩余	175
9.12 交错	147	11.3.10 勒让德符号	175
9.13 分组密码与序列密码	147	11.3.11 雅可比符号	176
第 10 章 使用算法	149	11.3.12 Blum 整数	177
10.1 选择算法	149	11.3.13 生成元	177
10.2 公开密钥密码学与对称密码学	150	11.3.14 伽罗瓦域中的计算	178
10.3 通信信道加密	151	11.4 因子分解	179
10.3.1 链-链加密	151	11.5 素数的产生	181
10.3.2 端-端加密	152	11.5.1 Solovag-Strassen	181
10.3.3 两者的结合	153	11.5.2 Lehmann	182
10.4 用于存储的加密数据	154	11.5.3 Rabin-Miller	182
10.4.1 非关联密钥	155	11.5.4 实际考虑	182
10.4.2 驱动器级与文件级加密	155	11.5.5 强素数	183
10.4.3 提供加密驱动器的随机 存取	155	11.6 有限域上的离散对数	183
10.5 硬件加密与软件加密	156	第 12 章 数据加密标准	185
10.5.1 硬件	156	12.1 背景	185
10.5.2 软件	157	12.1.1 标准的开发	185
10.6 压缩, 编码及加密	157	12.1.2 标准的采用	186
10.7 检测加密	158	12.1.3 DES 设备的鉴定和认证	187
10.8 密文中隐藏密文	158	12.1.4 1987 年的标准	187
10.9 销毁信息	159	12.1.5 1993 年的标准	188
第三部分 密码算法		12.2 DES 的描述	188
第 11 章 数学背景	161	12.2.1 算法概要	189
11.1 信息论	161	12.2.2 初始置换	190
11.1.1 熵和不确定性	161	12.2.3 密钥置换	190
11.1.2 语言信息率	161	12.2.4 扩展置换	191
11.1.3 密码系统的安全性	162	12.2.5 S-盒代替	192
11.1.4 唯一解距离	163	12.2.6 P-盒置换	194
11.1.5 信息论的运用	163	12.2.7 未置换	194
11.1.6 混乱和扩散	164	12.2.8 DES 解密	194
11.2 复杂性理论	164	12.2.9 DES 的工作模式	194
11.2.1 算法的复杂性	164	12.2.10 DES 的硬件和软件实现	195
11.2.2 问题的复杂性	165	12.3 DES 的安全性	196
11.2.3 NP 完全问题	167	12.3.1 弱密钥	197
11.3 数论	167	12.3.2 补密钥	198
		12.3.3 代数结构	199
		12.3.4 密钥的长度	199

12.3.5 迭代的次数	200	13.9.2 IDEA 的描述	226
12.3.6 S-盒的设计	200	13.9.3 IDEA 的速度	228
12.3.7 其他结论	201	13.9.4 IDEA 的密码分析	228
12.4 差分及线性分析	201	13.9.5 IDEA 的操作方式和变型	229
12.4.1 差分密码分析	201	13.9.6 敬告使用者	230
12.4.2 相关密钥密码分析	204	13.9.7 专利和许可证	230
12.4.3 线性密码分析	204	13.10 MMB 算法	230
12.4.4 未来的方向	206	13.11 CA-1.1 算法	232
12.5 实际设计的准则	206	13.12 Skipjack 算法	232
12.6 DES 的各种变型	207	第 14 章 其他分组密码算法	
12.6.1 多重 DES	207	(续)	234
12.6.2 使用独立子密钥的 DES	207	14.1 GOST 算法	234
12.6.3 DESX	208	14.1.1 GOST 的描述	234
12.6.4 CRYPT (3)	208	14.1.2 GOST 的密码分析	236
12.6.5 GDES	208	14.2 CAST 算法	236
12.6.6 更换 S-盒的 DES	209	14.3 Blowfish 算法	237
12.6.7 RDES	210	14.3.1 Blowfish 的描述	237
12.6.8 s ² DES	210	14.3.2 Blowfish 的安全性	239
12.6.9 使用相关密钥 S-盒的 DES	211	14.4 SAFER 算法	239
12.7 DES 现今的安全性如何	212	14.4.1 SAFER K-64 的描述	239
第 13 章 其他分组密码算法	213	14.4.2 SAFER K-128	241
13.1 Lucifer 算法	213	14.4.3 SAFER K-64 的安全性	241
13.2 Madryga 算法	213	14.5 3-WAY 算法	241
13.2.1 Madryga 的描述	214	14.6 Crab 算法	242
13.2.2 Madryga 的密码分析	215	14.7 SXAL8/MBAL 算法	243
13.3 NewDES 算法	215	14.8 RC5 算法	243
13.4 FEAL 算法	216	14.9 其他分组密码算法	244
13.4.1 FEAL 的描述	216	14.10 分组密码设计理论	245
13.4.2 FEAL 的密码分析	219	14.10.1 Feistel 网络	245
13.4.3 专利	220	14.10.2 简单关系	246
13.5 REDOC 算法	220	14.10.3 群结构	246
13.5.1 REDOC III	220	14.10.4 弱密钥	246
13.5.2 专利和许可证	221	14.10.5 强的抗差分攻击和线性	
13.6 LOKI 算法	221	攻击	246
13.6.1 LOKI91	221	14.10.6 S-盒的设计	247
13.6.2 LOKI91 的描述	221	14.10.7 设计分组密码	248
13.6.3 LOKI91 的密码分析	223	14.11 使用单向散列函数	248
13.6.4 专利和许可证	223	14.11.1 Kam	248
13.7 Khufu 和 Khafre 算法	223	14.11.2 Luby-Rackoff	249
13.7.1 Khufu	224	14.11.3 消息摘要密码	249
13.7.2 Khafre	224	14.11.4 基于单向散列函数的密码安	
13.7.3 专利	224	全性	250
13.8 RC2 算法	224	14.12 分组密码算法的选择	250
13.9 IDEA 算法	225	第 15 章 组合分组密码	252
13.9.1 IDEA	226	15.1 双重加密	252

15.2 三重加密	253	16.9.2 Pike 发生器	279
15.2.1 用两个密钥进行三重加密	253	16.9.3 Mush 发生器	279
15.2.2 用三个密钥进行三重加密	254	16.10 Gifford 算法	279
15.2.3 用最小密钥进行三重加密	254	16.11 M 算法	280
15.2.4 三重加密模式	254	16.12 PKZIP 算法	280
15.2.5 三重加密的变型	256	第 17 章 其他序列密码和真随机序	
15.3 加倍分组长度	257	列发生器	282
15.4 其他多重加密方案	257	17.1 RC4 算法	282
15.4.1 双重 OFB/计数器	257	17.2 SEAL 算法	283
15.4.2 ECB+OFB	258	17.2.1 伪随机函数族	283
15.4.3 xDES	258	17.2.2 SEAL 的描述	283
15.4.4 五重加密	259	17.2.3 SEAL 的安全性	284
15.5 缩短 CDMF 密钥	259	17.2.4 专利和许可证	284
15.6 白化	259	17.3 WAKE 算法	284
15.7 级联多重加密算法	260	17.4 带进位的反馈移位寄存器	285
15.8 组合多重分组算法	260	17.5 使用 FCSR 的序列密码	292
第 16 章 伪随机序列发生器和序列		17.5.1 级联发生器	292
密码	261	17.5.2 FCSR 组合发生器	292
16.1 线性同余发生器	261	17.5.3 CFSR/FCSR 加法/奇偶级联	293
16.2 线性反馈移位寄存器	264	17.5.4 交替停走式发生器	293
16.3 序列密码的设计与分析	269	17.5.5 收缩式发生器	294
16.3.1 线性复杂性	270	17.6 非线性反馈移位寄存器	294
16.3.2 相关免疫性	270	17.7 其他序列密码	295
16.3.3 其他攻击	270	17.7.1 Pless 发生器	295
16.4 使用 LFSR 的序列密码	270	17.7.2 蜂窝式自动发生器	295
16.4.1 Geffe 发生器	271	17.7.3 1/p 发生器	295
16.4.2 推广的 Geffe 发生器	272	17.7.4 crypt (1)	296
16.4.3 Jennings 发生器	272	17.7.5 其他方案	296
16.4.4 Beth-Piper 停走式发生器	272	17.8 序列密码设计的系统理论方法	296
16.4.5 交替停走式发生器	273	17.9 序列密码设计的复杂性理论	
16.4.6 双侧停走式发生器	273	方法	297
16.4.7 门限发生器	274	17.9.1 Shamir 伪随机数发生器	297
16.4.8 自采样发生器	274	17.9.2 Blum-Micali 发生器	297
16.4.9 多倍速率内积式发生器	275	17.9.3 RSA	297
16.4.10 求和式发生器	275	17.9.4 Blum, Blum 和 Shub	297
16.4.11 DNRSR	275	17.10 序列密码设计的其他方法	298
16.4.12 Gollmann 级联	275	17.10.1 Rip van Winkle 密码	298
16.4.13 收缩式发生器	276	17.10.2 Diffie 随机序列密码	299
16.4.14 自收缩式发生器	276	17.10.3 Maurer 随机序列密码	299
16.5 A5 算法	276	17.11 级联多个序列密码	299
16.6 Hughes XPD/KPD 算法	277	17.12 选择序列密码	300
16.7 Nanoteq 算法	277	17.13 从单个伪随机序列发生器产生多	
16.8 Rambutan 算法	277	个序列	300
16.9 附加式发生器	278	17.14 真随机序列发生器	301
16.9.1 Fish 发生器	278	17.14.1 RAND 表	301

17.14.2 使用随机噪声	302	18.14.6 IBC-Hash	328
17.14.3 使用计算机时钟	302	18.14.7 单向散列函数 MAC	329
17.14.4 测量键盘反应时间	303	18.14.8 序列密码 MAC	329
17.14.5 偏差和相关性	303	第 19 章 公开密钥算法	330
17.14.6 提取随机性	304	19.1 背景	330
第 18 章 单向散列函数	307	19.2 背包算法	331
18.1 背景	307	19.2.1 超递增背包	331
18.1.1 单向散列函数的长度	308	19.2.2 由私人密钥产生公开密钥	332
18.1.2 单向散列函数综述	308	19.2.3 加密	332
18.2 Snefru 算法	308	19.2.4 解密	332
18.3 N-Hash 算法	309	19.2.5 实际实现方案	333
18.4 MD4 算法	311	19.2.6 背包的安全性	333
18.5 MD5 算法	311	19.2.7 背包变型	333
18.5.1 MD5 的描述	312	19.2.8 专利	333
18.5.2 MD5 的安全性	315	19.3 RSA 算法	334
18.6 MD2 算法	315	19.3.1 RSA 的硬件实现	335
18.7 安全散列算法	316	19.3.2 RSA 的速度	336
18.7.1 SHA 的描述	316	19.3.3 软件加速	336
18.7.2 SHA 的安全性	318	19.3.4 RSA 的安全性	337
18.8 RIPE-MD 算法	319	19.3.5 对 RSA 的选择密文攻击	337
18.9 HAVAL 算法	319	19.3.6 对 RSA 的公共模数攻击	338
18.10 其他单向散列函数	319	19.3.7 对 RSA 的低加密指数攻击	338
18.11 使用对称分组算法的单向散列函 数	320	19.3.8 对 RSA 的低解密指数攻击	339
18.11.1 散列长度等于分组长度的方 案	320	19.3.9 经验	339
18.11.2 改进的 Davies-Meyer	322	19.3.10 对 RSA 的加密和签名的攻 击	339
18.11.3 Preneel-Bosselaers-Govaerts- Vandewalle	322	19.3.11 标准	339
18.11.4 Quisqater-Girault	322	19.3.12 专利	340
18.11.5 LOKI 双分组	323	19.4 Pohlig-Hellman 算法	340
18.11.6 并行 Davies-Meyer	323	19.5 Rabin 算法	340
18.11.7 串联和并联 Davies-Meyer	323	19.6 ElGamal 算法	341
18.11.8 MDC-2 和 MDC-4	324	19.6.1 ElGamal 签名	342
18.11.9 AR 散列函数	325	19.6.2 ElGamal 加密	342
18.11.10 GOST 散列函数	326	19.6.3 速度	343
18.11.11 其他方案	326	19.6.4 专利	343
18.12 使用公开密钥算法	326	19.7 McEliece 算法	343
18.13 选择单向散列函数	326	19.8 椭圆曲线密码系统	344
18.14 消息鉴别码	327	19.9 LUC 算法	345
18.14.1 CBC-MAC	327	19.10 有限自动机公开密钥密码系统	345
18.14.2 信息鉴别算法	327	第 20 章 公开密钥数字签名算法	347
18.14.3 双向 MAC	328	20.1 数字签名算法	347
18.14.4 Jueman 方法	328	20.1.1 对通告的反应	347
18.14.5 RIPE-MAC	328	20.1.2 DSA 的描述	349
		20.1.3 快速预计算	350
		20.1.4 DSA 的素数产生	351