Mc Graw Hill Education
世界著名计算机教材精选

密码学与网络安全

Atul Kahate 著
邱仲潘 等 译

CRYPTOGRAPHY AND NETWORK SECURITY

清华大学出版社
Mc Graw Hill

世界著名计算机教材精选

Cryptography and Network Security

密码学与网络安全

Atul Kahate 著
邱仲潘 等 译

清华大学出版社
北京

Atul Kahate
Cryptography and Network Security
EISBN: 0-07-049483-5

图书在版编目(CIP)数据

密码学与网络安全 /（印）卡哈特（Kahate, A.）著；邱仲潘等译. —北京：清华大学出版社，2005.9
（世界著名计算机教材精选）
书名原文：Cryptography and Network Security
ISBN 7-302-11490-0

Ⅰ. 密… Ⅱ. ①卡… ②邱… Ⅲ. ①密码-理论-高等学校-教材 ②计算机网络-安全技术-高等学校-教材 Ⅳ. ①TN918.1 ②TP393.08

中国版本图书馆 CIP 数据核字（2005）第 086918 号

出 版 者：清华大学出版社 **地 址**：北京清华大学学研大厦
http://www.tup.com.cn **邮 编**：100084
社 总 机：010-62770175 **客户服务**：010-62776969
责任编辑：龙啟铭
印 装 者：清华大学印刷厂
发 行 者：新华书店总店北京发行所
开 本：185×260 **印张**：24.25 **字数**：598 千字
版 次：2005 年 9 月第 1 版 2005 年 9 月第1 次印刷
书 号：ISBN 7-302-11490-0/TP・7540
印 数：1～4000
定 价：43.00 元

作 者 介 绍

Atul Kahate 在印度和世界 IT 业中已经有 8 年的工作经验，他取得了统计学学士学位和计算机系统专业的 MBA 学位。这是他撰写的第二部 IT 专著，他过去曾为 Tata McGraw-Hill 出版公司与他人合写了“Web Technologies –TCP/IP to Internet Application Architectures”一书。目前，他正在为 Tata McGraw-Hill 出版公司写另外三本书。此外，他还对 Tata McGraw-Hill 出版公司的另外三本书“Operating Systems”、“C and Data Structures”与“Data Communications and Networks”做了大量工作。

Atul Kahate 还写了两本板球方面的书，为印度和外国的报刊杂志撰写了一千多篇 IT 和板球方面的文章。他在教育、音乐和板球方面的兴趣很浓厚。他在多家教育机构和 IT 公司领导了多个培训项目。他还是多个比赛中的正式板球统计员和计分员。Atul Kahate 收集了大量关于 IT 与板球方面的书籍，建立了自己的数据库，可以提供任何时刻的最新板球统计信息。

Atul Kahate 还在印度和国外获得过多个奖项，过去曾就职于 Syntel、L&T Infotech American Express 和德国银行，现就职于 i-flex solution 有限公司。Atul Kahate 和妻子 Anita、女儿 Jui 和儿子 Harsh 一起住在 Pune，他的电子邮件地址为 akahate@indiatimes.com。

序　一

人类总是多疑的。发消息时，我们总是怀疑有人会截获它，并在阅读或修改后再发送。这个怀疑不是毫无根据的，因为人类同时也是爱打听消息的，总是希望知道他人之间收到的秘密消息，不管有没有商业或政治好处。显然，人类始终希望发出的消息只让所要的人看懂。

但是，加密的历史可以追溯到公元前 2000 年的古埃及，人们用象形文字装饰帝王的墓地。这些象形文字诉说了这些帝王的生平，介绍了他们的丰功伟绩。虽然这些象形文字很古怪，但并不是有意隐藏文本。随着时间的推移，这些作品显得越来越复杂，越来越难以书写和理解，最后，失去了市场。事实上，曾几何时，人们把加密看成神秘的黑色艺术，名声不好。印度的加密术很普及和先进，政府用加密术与间谍联系。在著名的希腊戏剧《伊利亚特》中，Bellerophon 就用加密术向国王传递情报。

希腊的 Polybius 建立了很好的加密方法（现称为 Polybius 方格），Julius Caesar 使用了另一种方法（称为凯撒密文）。Leon Battista Alberti 被称为“西方加密术之父”，因为他建立了多码替换方法，而美洲的加密术之父是 James Lovell，他破译了许多英国密码，帮助美国革命取得成功。事实上，他破译的一个消息确定了战争最后胜利的地点。后来，Thomas Jefferson 于 1795 年前后发明了“轮密码”。

尽管第一次世界大战期间采用了加密方法，但在第二次世界大战中使用得更加淋漓尽致：Arthur Scherbius 开发的德国 Enigma 加密机和用 Herbert O.Yardley 发明的技术建立的日本紫色机器就是个范例。事实上，战争大大推进了加密学的进程。

20 世纪 70 年代，Horst Feistel 博士建立了 DES（数据加密标准）的前身，在 IBM 公司 Watson 研究实验室推出了所谓 Feistel 密码的密码系列。1976 年，美国国家安全局（NSA）利用 Feistel 密码建立了 FIPS PUB-46，就是现在的 DES。如今，美国财经研究所使用的安全标准是三重 DES 标准。也是在 1976 年，Feistel 的两个同时代人 Whitefield Diffie 与 Matin Hellman 在“New Directions in Cryptography”一书中首次提出了公钥加密法（PKC）的思想。

DES 采用对称密钥加密法，即用相同密钥进行加密和解密，因此，发送方和接收方要事先商定和知道这个密钥。这在 Internet 世界中存在严重问题，因为许多用户都要以安全方式向服务器发送和从服务器接收消息，每对密钥如何确定、交换和保密呢？

RSA 解决了这个问题，设计一个密钥对：一个用于加密，一个用于解密。事实上，用一个密钥加密的消息只能用对应的另一个密钥解密。这个方法的原理是，两个大素数的积很难反过来求出其因子（如一个 100 多位的素数）。在 RSA 中，可以用两个大素数作为密钥对：一个作为公钥，一个作为私钥。事实上，整个安全基础结构就是建立在公钥基础上的，称为公钥基础设施（PKI）。

RSA 是由 Rivest、Shamir 与 Adleman 设计的。他们提出挑战，声明谁能解密他们加密的消息，就可以得到 100 美元奖金。这是 1997 年 Martin Gardner 在“Scientific American”

杂志的“Mathematical Games”栏目中发表的，这是个非常受欢迎的栏目。利用当时非常强大的计算机，要破译这个消息估计要 4×10^{16} 年。1978 年后期，RSA 正式推出了 PKC 系统。

随着 Internet 的发展，对安全数据传输的需求成倍增加。事实上，这是业务事务使用 Internet 的前提条件。仅仅 2002 年，与安全相关的欺诈业务就达到 60 亿美元之巨。因此，安全是 Internet 世界中的主要问题，特别是财政和金融事务。

在这个背景下，本书的意义非常大。构造基于 Web 的软件系统时，不能不考虑安全问题，因此，本书是相当及时的。市面上也有一些相同主题的书，但本书以它的简单性脱颖而出。只要对计算环境有一定了解，几乎任何人都能读懂这本书。本书语言非常流畅简洁，并用大量框图帮助理解。有趣的是，尽管本书具有很简单的特点，但又不失深度和严谨性。因此，我认为本书相当有价值，不仅可以作为教材，也可以作为软件经理和软件设计人员的参考指南。

很荣幸有机会与 Atul 合著了“Web Technologies”一书，他是我见过的最聪明、最富系统性和洞察力的人。他不仅技术水平高，而且为人谦逊，这是我最敬重的。有趣的是，他还有许多其他兴趣，包括音乐和板球，他是个正式板球统计员。此外，我觉得他特别有人情味，是进行最终分析的最佳人选之一。

很高兴认识他和他共事，祝他的事业更加辉煌。

A CHYUT S G ODBOLE
CEO –Apar Technologies, Mumbai
（Operating Systems, Data Communications and Networks
和 Web Technologies 的作者，均已由 Tata McGraw-Hill 出版）

序　二

信息安全已成为现代计算系统非常关键的一个方面。随着 Internet 在全球的普及，几乎每台计算机都与别的计算机相互连接。尽管这样可以为我们生活的世界上带来巨大的生产率和前所未有的机会，但也对计算机用户带来了新的风险。用户、公司和组织都可能随时受到黑客与攻击者威胁，他们用各种技术和工具破解计算机系统、窃取信息、改变数据和制造混乱。

正是在这种情况下，Atul Kahate 推出了他的第二部专著《密码学与网络安全》。Atul 的知识不仅是从学习与研究中来的，而且来自解决许多实际问题的第一手经验，包括处理公钥基础设施（PKI）和相关领域事务、在复杂软件系统中建立和测试加密法与安全性。印度 Pune 的 i-flex 支付系统中心为他近两年的学习和研究提供了非常合适的环境。

获取和开发知识是个巨大的成就，而通过共享知识让别人理解则更有意义。要以通俗易懂的方式解释自己知道的东西是个非常麻烦、费时和困难的任务。Atul 在这方面做得很好，以逻辑和实用的方式介绍知识，创做了这样一本综合性教材。Atul 之前曾经与人合著了“Web Technologies”一书（也在 Tata McGraw-Hill 出版），受到广大读者好评。

i-flex 公司很高兴看到 Atul 完成了第二本计算机技术方面的书籍，为他而自豪。我们坚信，他今后会推出更多好书。除了深入和广泛的介绍外，本书还有两大特点：一是语言流畅，一是插图丰富。Atul 一步一步地介绍加密与安全的复杂内容，无疑能大大便利读者理解所有关键概念。我们坚信，本书对各个层次的学生、老师和 IT 人员都会大有帮助。

一个重要启示是，我们不能满足于平凡的日常工作，而应该有更高目标和更大努力，从而在工作的不同方面出类拔萃（甚至超出工作范围）。

我代表 i-flex solutions 公司的全体同仁祝 Atul 的这本书取得成功。

RAJESH HUKKU
i-flex solutions 公司
董事长兼总经理

前　言

背景

“要让三个人保住秘密，其中两个人必须死亡！”

——本杰明·富兰克林

这类名言随处可见，因为保密是非常困难的。事实上，传播秘密和探听秘密是人们的两大天性！有人说，要宣扬某件事，最好把它称为秘密，悄悄地告诉更多人，传闻会自动传播开来！

在早期计算中（20 世纪 50~60 年代），人们对安全强调得不多，因为当时的系统是专属和封闭的。简单地说，计算机之间虽然也交换数据和信息，但形成的网络完全在组织控制之下。那个时候，计算机之间通信所用的协议也是不公开的。因此，别人很难访问交换的信息。这样，当时信息安全并不是个重要问题。

随着 20 世纪 70 年代和 80 年代小型机与微机的发展，信息安全问题越来越突出，但其在经理和技术人员的心目中仍然不是最重要的。人们通常把信息安全看成硬件/软件系统的目标之一。这种情形一直持续到 20 世纪 90 年代初。但是，Internet 的出现改变了整个计算模式，使计算机之间通信的方式大大改变，使计算机世界突然变得很开放。专属协议（如 IBM 公司的 SNA）不再普及，取而代之的是 TCP/IP 之类的开放标准，这些开发标准成为连接全球计算机的纽带。

Internet 的迅速增长带来了无穷的计算机会，但同时也带来了全新的问题和担心，特别是信息交换的安全性。例如：

- 在 Internet 网络上向另一台计算机发送信用卡信息不再安全。
- 访问发送方和接收方之间的连接就可以读到正在交换的电子邮件。
- 人们可能用别人的身份登录，使用别人的权限。

如今，新的信息威胁与攻击不断出现。在技术人员找到针对这些攻击的保护方法的同时，而攻击者则在不断寻求新的攻击方法。这种情况必将继续下去。因此，一定要知道如何安全地交换信息。

动机

本人在 IT 行业工做了 8 年，对信息安全及其实现方法有许多了解。但是，我的概念曾经很模糊，关于安全的知识是一点一点积累起来的。这个过程很烦人，很难有满足感，总觉得没有一个全局概念。例如，我知道数字系统在加密学中起着重要作用，但不知道要对数字系统有多少了解才能了解密码学。同样，我知道数字证书和公钥基础设施（PKI）是

很好的技术，但只是对其一知半解。这样的情况还有很多。

后来，我有机会领导了一个 PKI 项目，通过这个项目学到了很多东西，但我总觉得自己要对计算机安全/加密的各个方面有个透彻了解才能更胜任这个项目。为此，我开始研究这些技术的每个方面。但是，这个研究遇到了许多障碍，主要是没有一本书能回答我的所有问题，更重要的是不能按我要求的方式回答问题，我的同事也常有同感。信息非常分散，很难理解，而且说得不够透彻。我要花很大力气才能了解这些内容。

学习的挑战性很妙，但也让我感到需要用浅显易懂的方式解释这些知识，使别人不必重复这个劳动。这也许是本书最重要的意图。假如我开始学习安全/加密时就有这样的书，那该多好！如果读者遇到类似情形时能有同感，读了本书后能有同样的满足感，那就是我最大的满足了。

目标读者

本书针对两类读者：IT 专业人员和本科生/研究生。为了满足不同人员的要求，本书经过了精心设计：一方面，书中简单介绍了 IT 专业人员要知道的方面（概念层），同时又深入介绍每个方面，以满足学生的需要。

组织

讲授信息安全/加密课程的老师肯定会喜欢这本书，书中详细介绍了这个技术，提供了四百多个框图，可以在课堂讨论中使用。每章提供了要点总结和一组概念与术语。为了帮助读者检查对概念的理解，本章最后还有自测题，有多项选择题、复习题和独特的设计/编程练习，使读者有充分的练习机会。

我将尽量使行文流畅，语言简洁。

我们为教师建立了联机学习中心（http://www.tatamcgrawhill.com/digital_solutions/kahate），其中有每章复习题和设计/编程练习的答案。这个网站还把书中的重要框图做成幻灯片（具有相应标注），可以直接在课堂和演示中使用。

第 1 章末尾介绍了本书的章节安排。

意见与建议

欢迎提供意见与建议，我的电子邮件地址为 akahate@indiatimes.com

ATUL KAHATE

致　谢

毫无疑问，Achyut Godbole 对我的生活有巨大影响。我从他身上学到了许多东西，包括技术和为人处世。他对我不断鼓励、真诚建议和经常激励，我的谢意是无法用言语表达的。

妻子 Anita 不仅帮我完成了各种家务，而且帮助进行了多处审阅，提出了许多建议，因为她本人就是个软件专业人员。她的牺牲使我能更好地利用业余时间。小女儿 Jui 非常可爱，经常在凌晨被我的键盘声吵醒后，好奇地看着我。感谢双亲和整个家庭的理解与支持，也感谢我的所有好友。

本书得到了许多人的帮助与支持，感谢 Nandu Kulkarni 先生与 B Ramanathan 先生让我利用业务时间和公司的设备创作这本书。我的同事也很好，不少人都实际提供了各种帮助，感谢他们，特别是 Tarun Matai、Pradnyesh Naik、Faizy Chaudhary、Radhika Joshi、K Giridhar 与 Ravi Battula。感谢 Sandhya Khan 帮我画了一些很复杂的框图，感谢 Bruce Schneier、Dan Conway 与 David Ireland 提供的一些编程练习。

Tata McGraw-Hill（TMH）小组总是那么优秀，Vibha Mahajan、Yusuf Khan、Mini Narayanan、Manohar Lal 和整个小组的经验与热情使本书有机会问世，衷心感谢他们。

Atul Kahate

目　录