密码学与网络安全（第2版）

CRYPTOGRAPHY AND NETWORK SECURITY

本书以清晰的脉络、简洁的语言，介绍了各种加密技术、网络安全协议与实现技术等内容，包括各种对称密钥算法与AES，非对称密钥算法、数字签名与RSA，数字证书与公钥基础设施，Internet安全协议，用户认证与Kerberos，Java、.NET和操作系统的加密实现，网络安全、防火墙与VPN，并给出了具体的加密与安全的案例实现分析，是一本关于密码学与网络安全的理论结合实践的优秀教材。

本书特点

* 本书语言表达流畅、简洁，使本书的阅读不再枯燥。
* 全书多达425幅插图，极大地方便了读者的学习和理解。
* 全书提供了丰富的多项选择题、练习题、设计与编程题，有利于加深读者对所学 知识的理解和掌握。

作者简介

Atul Kahate在印度和世界IT业中已经有12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。他与他人为Tata McGraw-Hill出版公司合著了多部著作，不少书被用作教材或全世界的大学/学院/IT公司用作参考书。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。

ISBN 978-7-302-19339-5

9 787302 193395 >

定价：49.00元

Mc Graw Hill Education

http://www.mheducation.com

世界著名计算机教材精选

密码学与网络安全

（第2版）

Atul Kahate 著

金 名 等译

清华大学出版社

北 京

Atul Kahate
Cryptography and Network Security, 2e
EISBN:0-07-064823-9

图书在版编目(CIP)数据

密码学与网络安全(第2版)/(印)卡哈特(Kahate, A.)著;金名等译. —北京:清华大学出版社,2009.3
(世界著名计算机教材精选)
书名原文:Cryptography and Network Security, 2e
ISBN 978-7-302-19339-5

Ⅰ.密… Ⅱ.①卡… ②金… Ⅲ.①密码—理论—教材 ②计算机网络—安全技术—教材
Ⅳ.TN918.1 TP393.08

中国版本图书馆 CIP 数据核字(2009)第 010592 号

责任编辑:龙啟铭
责任校对:徐俊伟
责任印制:杨 艳

出版发行:清华大学出版社 **地 址**:北京清华大学学研大厦 A 座
http://www.tup.com.cn **邮 编**:100084
社 总 机:010-62770175 **邮 购**:010-62786544
投稿与读者服务:010-62776969,c-service@tup.tsinghua.edu.cn
质 量 反 馈:010-62772015,zhiliang@tup.tsinghua.edu.cn
印 装 者:北京鑫海金澳胶印有限公司
经 销:全国新华书店
开 本:185×260 **印 张**:28.5 **字 数**:689 千字
版 次:2009 年月 3 第 1 版 **印 次**:2009 年 3 月第 1 次印刷
印 数:1～3000
定 价:49.00 元

译者序

随着计算机技术，尤其是网络技术的飞速发展，各行各业都离不开计算机，离不开网络。网络技术的出现和发展，在极大地方便了我们的工作和学习的同时，也带来了很多安全方面的难题。因安全漏洞和黑客入侵而造成巨大损失的案例日益增多。网络安全问题日益重要和迫切。要实现网络安全，就离不开加密技术。

本书以清晰的脉络、简洁的语言，介绍了各种加密技术、网络安全协议与实现技术等内容，并给出了具体的案例实现分析，是一本关于密码学与网络安全的理论结合实践的优秀教材。

本书自第 1 版出版以来，期间出现了多种新技术，已有的技术与协议又开发出了新版本，我们应当在本书中能看到这些新技术。本书对第 1 版所做的主要修改如下：

- 更详细地阐述了现代算法，如 AES、SHA-256 及其变体 TLS 等。
- 给出了更多的数学基础（只要有需要）。
- 扩展了已有的内容（只要有需要）。
- 介绍了一些在上一版中没有包含但在课程上将会讲授的内容。

本书在上一版的基础上，对一些翻译欠妥的地方进行了修改，在此表示感谢。本书由金名、张长富等主译，李晓春、王春桥、龚亚萍、韦笑、何雄、周云、袁科萍、王雷、贺军、贺民、陈安南、霍丽娜、史广飞、侯鹏、张红军、董武、陈河南、王峰、沈宏、郑晓蕊、李伟、白晓平、李月、汤效平、李东锋、邵世磊、张新苗、刘大为、薛飞、邹晓东、陈占军、夏绪虎、刘占坤、冯苗、裘蕾、任世华、金颖、吴霞、韩毅、马以辉、樊庆红等人也参与了部分翻译工作。欢迎广大读者指正。

作者介绍

Atul Kahate 在印度和世界 IT 业中已经有 12 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。他与他人为 Tata McGraw-Hill 出版公司合著了“Web Technologies - TCP/IP to Internet Application Architectures”、“Fundamentals of Computers”、“Information Technology and Numerical Methods”、“Foundations of Information Technology”、“Operating Systems and Sysmtems Programming”、“Operating Systems”、“Computer Communication Networks”、“Introduction to Database Management Systems”、“Object Oriented Analysis and Design”以及“Schaum's Series Outlines — Programming in C++”等专著。其中有两本由 McGraw-Hill 出版社出版了国际版，并翻译为中文。他的不少书被用作教材或被全世界的大学/学院/IT 公司用作参考书。

Atul Kahate 从 12 岁开始就为报刊撰写板球方面的文章，还写了两本关于板球方面的书，为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，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、儿子 Harsh 一起住在 Pune，他的电子邮件地址为 akahate@gmail. 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，这是商业事务使用 Internet 的前提条件。仅在 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，本书的意义非常重大。构造基于 Web 的软件系统时，不能不考虑安全问题，因此，本书的出版是相当及时的。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。尽管这可以为我们生活的世界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、公司和组织随时都可能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 2 部著作《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，创作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，二是插图丰富。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

第2版前言

在信息技术领域工作了6年后(于2001年),我阅读了大量的信息安全以及如何实现安全方面的文章。但是,我对信息安全的概念是模糊的,我只是片面地知道些安全的技术。这让我很苦恼,从没有让我满意过。我好像并不了解信息安全的全貌。例如,我知道数字系统在密码学中起着重要的作用,但并不知道,要理解信息安全的概念,需要对数字系统了解到什么程度。同样,我也知道数字证书和公共密钥基础设施(PKI)是非常精彩的技术,但对它们的工作原理不甚了解。类似的例子还有很多。

后来,我有机会在i-flex solutions有限公司领导一个信息安全项目。我认为只要通过这个项目,就可以学习信息安全的知识。但是,我还强烈地感觉到,除非自己完全弄懂计算机安全和密码学的各个方面,否则无法正确开展这个项目的工作。由于这个原因,我开始研究这些技术的每个方面。但是,这有很多困难。最主要的困难是,没有一本书能解释所有我想知道的;而且更为重要的是,没有一本书能以我想要的方式解释。我这个项目中的同事在很多时候也表达了这种感觉。可获得的信息很分散,太复杂和难以理解,也不能以一种让人完全理解的方式进行阐述。

学习的过程很精彩。但是,我也应该尝试以一种非常简单的方式来阐述我所知道的,这样,其他想要进入该领域的人就无需走我所走过的弯路。这或许就是我编写本书的主要目的。简单地说,这使我感觉到,如果在开始学习安全与密码学时只需一本书那该多好。如果读者在学习了本书后也感到满意,那就是我最大的满足了。

本书的第1版于2003年出版。那时,关于安全与密码学主题的书非常少,即使有,也是太复杂和难以理解。因此,我决定尝试最大限度地简化这个主题。我编写本书没有按照某个教学大纲,而是以一种我认为更容易理解的方式。令我惊奇的是,在过去的四年半时间里,本书不仅在印度和其他很多国家和地区的教学中使用,而且有不少教学大纲和课程也按照本书来设计。这坚定了我的信念,本书内容的顺序和结构非常正确。这种信念受到了本书第1版的读者的欢迎,从本书的8次重印、国际版和中文翻译版的出版中可以印证这一点。

同时,安全技术发展非常迅速,用四年半来修订本书是一个很长的时间。

期间出现了多种新技术，已有的技术与协议也已开发出了新版本，我们应当在本书中能看到这些新技术。本书对第1版所做的主要修改如下：

- 更详细地阐述了现代算法，如AES、SHA-256及其变体TLS等。
- 给出了更多的数学基础（只要有需要）。
- 扩展了已有的内容（只要有需要）。
- 介绍了一些在上一版中没有包含但在课程上将会讲授的内容。

有了这些改变，我自信本书将更能满足读者的期望。

本版最大的变化是使得内容更好理解、更新、更简洁。

这些变化是为了满足不同教学的需要，并且体现了来自学生、读者、教授和IT专业人员的反馈。

本书主要针对两类读者：本科生、研究生、博士生，以及IT专业人员。为了满足这两类人的不同需要，本书进行了非常仔细的设计。一方面，它对每个内容进行了深入阐述，以满足学生的需要；另一方面，又涉及了IT专业人员希望在概念上进行了解的内容。

对本书内容的组织和顺序安排花费了不少精力。因此，我建议不要跳过任何章节。但是，对那些爱好者，不想了解全部内容，只想大致浏览的读者，可以跳过数学内容。

信息安全与密码学课程的学生和老师会发现本书非常有用。本书详细介绍了该技术，并有多达425幅插图可供教学使用。每章内容包含有：

- 本章小结，简要回顾一章的知识要点。
- 自测题，包括多项选择题、复习题。
- 设计与编程题。

本书试图保持表达流畅，语言简洁的特点。

下面介绍一下本书的组织结构。

第1章介绍了基本安全概念，介绍安全需求、安全原则，以及针对计算机系统与网络的各种攻击。介绍了所有这些内容背后的概念理论，以及实际问题，并一一举例说明，以便加深对安全性的了解。如果不了解为什么需要安全性，有什么威胁，就无从了解如何保护计算机系统与网络。新内容有：增加一节关于安全攻击的现代特性。讨论了可信系统、安全模式、安全管理实践，以及法律和道德问题。用新的一节来介绍攻击的类型。还介绍了诸如钓鱼欺骗和DNS欺骗等攻击。

第2章介绍了加密的概念，这是计算机安全的核心内容。加密是用各种算法来实现的。所有这些算法或者将明文替换成密文，或者用某种变换方法，或者是两者的组合。然后本章将介绍加密与解密的重要术语。新内容有：详细介绍了Playfair加密法和希尔加密法。展开介绍了Diffie-Hellman密钥交换。详细介绍了攻击的类型。

第3章介绍了基于计算机的对称密钥加密法的各种问题。我们介绍流和块加密以及各种链接模式，并介绍了主要的对称密钥加密算法，如DES、IDEA、RC5与Blowfish。新内容有：详细介绍了Blowfish算法。对AES进行了重点扩展。

第4章介绍了非对称密钥加密的概念、问题与趋势，介绍了非对称密钥加密的历史，然后介绍了主要的非对称密钥加密，如RSA、MD5、SHA与HMAC。本章介绍了消息摘要、数字签名等关键术语，还介绍了如何把对称密钥加密与非对称密钥加密结合起来。新内容有：介绍了SHA-1消息摘要算法的变体，特别介绍了SHA-512。

第 5 章介绍了当前流行的公钥基础设施(PKI),介绍了数字证书及其生成、发布、维护与使用方法,介绍了证书机构(CA)与注册机构(RA)的作用,并介绍了公钥加密标准(PKCS)。新内容有:介绍了用 Java 语言创建数字证书的详细内容。

第 6 章介绍了 Internet 中的重要安全协议,包括 SSL、SHTTP、TSP、SET 与 3D 安全性,并介绍了电子货币的工作原理、涉及的危险和如何充分利用电子货币。本章将详细介绍电子邮件安全性,介绍 PGP、PEM 与 S/MIME 等主要电子邮件安全协议,并介绍无线安全性。新内容有:扩展介绍了 SSL,并将它与 TLS 进行比较。扩展了 PGP,介绍了密钥环、PGP 证书和可信管理等。

第 7 章介绍了如何认证用户,可以使用多种方法认证用户。本章详细介绍了每种方法及其利弊,介绍基于口令认证、基于口令派生信息的认证、认证令牌、基于证书认证和生物认证,并介绍了著名的 Kerberos 协议。新内容有:介绍安全握手协议,并详细介绍了单向认证和双向认证。

第 8 章介绍了加密的实际问题。目前,实现加密的 3 种主要方法是:使用 Sun 公司提供的加密机制(在 Java 语言中)、Microsoft 加密机制和第三方工具箱的加密机制,我们将介绍每种方法。新内容有:介绍了 Microsoft .NET 框架下的加密实现,增进操作系统安全,并介绍了数据库安全。

第 9 章介绍了网络层安全,介绍防火墙及其类型与配置,然后介绍 IP 安全性,最后介绍了虚拟专用网(VPN)。新内容有:介绍了网络地址转换(NAT),详细介绍了入侵与入侵检测的概念。

第 10 章介绍了加密与网络安全领域的几个案例分析,介绍如何把前面几章学到的概念应用到实践之中,还介绍了几个实际发生的安全攻击及其处理方法。这些内容分别从攻击者和被攻击者的角度加以介绍。新内容有:新增了几个案例研究。

在线学习中心(Online Learning Center)为学生和教师提供了有益帮助。其中包含有所有练习和编程的答案、Web 链接、幻灯片、AES 和 DES 小程序的加密演示程序,以及实际的案例研究。该网址的内容会经常更新。

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的道理。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。

我的父母和整个家庭给予了我很多的理解和支持。我要感谢他们。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。她的付出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时,好奇地看着我。

本书离不开许多人的帮助与支持。我在 i-flex 公司工作的 6 年中,从公司高层(Rajesh Hukku、Deepak Ghaisas、Nandu Kulkarni、N. K. Raman、V. Shankar、Vivek Govilkae)到新加入公司的所有人,都给了我难忘的记忆。感谢他们的支持、鼓励和智慧。感谢我的学生朋友,他们总是激发我学习新的知识。感谢 Bruce Schneier、Dan Conway 与 David Ireland 提供的一些编程练习。

全世界成百上千的第 1 版读者给我发来了电子邮件。感谢他们把宝贵的时间花费在他们认为有意义的事情上。

Tata McGraw-Hill(TMH)小组总是那么优秀，Vibha Mahajan、Nilanjan Chakravarty和小组的其他成员的经验与热情使本书有机会问世，衷心感谢他们。

感谢以下审阅人员为本书质量的提高给出了宝贵建议：V. S. Janakiraman博士、V. Valli Kumari女士、Jaydip Sen教授、Bhushan H. Trivedi教授、L. K. Suresh Kumar教授和Dilip Kumar先生。

非常欢迎读者来信：akahate@gmail.com。

Atul Kahate

第1版前言

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一个重要问题。

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是硬件/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，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 行业工作了 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，更重要的是这些书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。这也许是撰写本书最重要的意图。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

本书主要针对两类读者：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，提供了多达425幅插图，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插图做成幻灯片(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

目 录