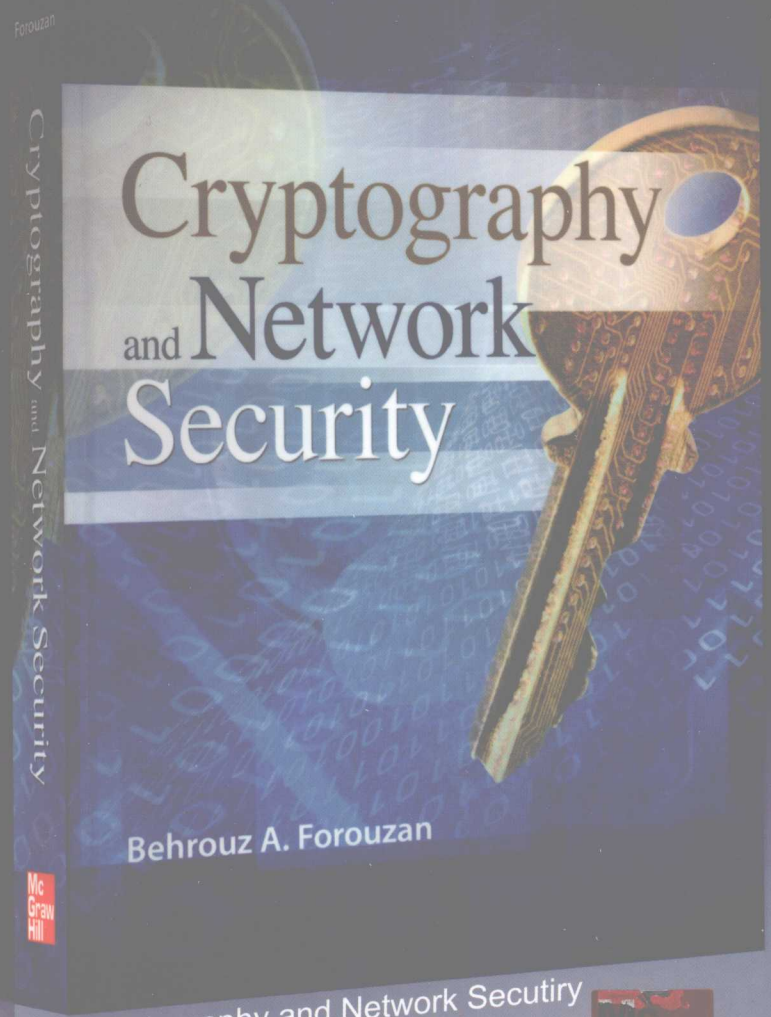
国外计算机科学经典教材

密码学与网络安全

(美) Behrouz A. Forouzan 著　　马振晗 贾军保 译



Mc Graw Hill Education
清华大学出版社

国外计算机科学经典教材

密码学与网络安全

(美) Behrouz A. Forouzan 著

马振晗 贾军保 译

清华大学出版社

北 京

Behrouz A. Forouzan
Cryptography and Network Security
ISBN: 978-0-07-332753-2

图书在版编目(CIP)数据

密码学与网络安全/(美)福罗赞(Forouzan, B.A.) 著；马振晗，贾军保 译. —北京：清华大学出版社，
书名原文：Cryptography and Network Security
(国外计算机科学经典教材)
ISBN 978-7-302-18584-0

I. 密… II. ①福…②马…③贾… 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(2008)第 143578 号

责任编辑：王 军 梁卫红
装帧设计：孔祥丰
责任校对：胡雁翎
责任印制：孟凡玉
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 刷 者：北京密云胶印厂
装 订 者：三河市新茂装订有限公司
经 销：全国新华书店
开 本：185×260 **印 张**：42.5 **字 数**：1034 千字
版 次：2009 年 1 月第 1 版 **印 次**：2009 年 1 月第1 次印刷
印 数：1～4000
定 价：79.80 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177 转 3103 产品编号：025547-01

出 版 说 明

近年来，我国的高等教育特别是计算机学科教育，进行了一系列大的调整和改革，亟需一批门类齐全、具有国际先进水平的计算机经典教材，以适应我国当前计算机科学的教学需要。通过使用国外优秀的计算机科学经典教材，可以了解并吸收国际先进的教学思想和教学方法，使我国的计算机科学教育能够跟上国际计算机教育发展的步伐，从而培养出更多具有国际水准的计算机专业人才，增强我国计算机产业的核心竞争力。为此，我们从国外多家知名的出版机构 Pearson、McGraw-Hill、John Wiley & Sons、Springer、CENGAGE Learning 等精选、引进了这套“国外计算机科学经典教材”。

作为世界级的图书出版机构，Pearson、McGraw-Hill、John Wiley & Sons、Springer、CENGAGE Learning 通过与世界级的计算机教育大师携手，每年都为全球的计算机高等教育奉献大量的优秀教材。清华大学出版社和这些世界知名的出版机构长期保持着紧密友好的合作关系，这次引进的“国外计算机科学经典教材”便全是出自上述这些出版机构。同时，为了组织该套教材的出版，我们在国内聘请了一批知名的专家和教授，成立了专门的教材编审委员会。

教材编审委员会的运作从教材的选题阶段即开始启动，各位委员根据国内外高等院校计算机科学及相关专业的现有课程体系，并结合各个专业的培养方向，从上述这些出版机构出版的计算机系列教材中精心挑选针对性强的题材，以保证该套教材的优秀性和领先性，避免出现“低质重复引进”或“高质消化不良”的现象。

为了保证出版质量，我们为该套教材配备了一批经验丰富的编辑、排版、校对人员，制定了更加严格的出版流程。本套教材的译者，全部由对应专业的高校教师或拥有相关经验的 IT 专家担任。每本教材的责编在翻译伊始，就定期不间断地与该书的译者进行交流与反馈。为了尽可能地保留与发扬教材原著的精华，在经过翻译、排版和传统的三审三校之后，我们还请编审委员或相关的专家教授对文稿进行审读，以最大程度地弥补和修正在前面一系列加工过程中对教材造成的误差和瑕疵。

由于时间紧迫和受全体制作人员自身能力所限，该套教材在出版过程中很可能还存在一些遗憾，欢迎广大师生来电来信批评指正。同时，也欢迎读者朋友积极向我们推荐各类优秀的国外计算机教材，共同为我国高等院校计算机教育事业贡献力量。

清华大学出版社

国外计算机科学经典教材

编审委员会

前　言

互联网作为一个世界范围的通信网络，已经在许多方面改变了我们的日常生活。一个最新的商业上的例子就是每个人都可以在线购物。万维网（WWW）还可以让我们分享信息。电子邮件的技术把世界各个角落的人联系在了一起。这种必然的发展也形成了对互联网的依赖。

互联网作为一个开放的论坛，已经产生了一些安全方面的问题。互联网需要有机密性、完整性和可信性。人们需要确保网络通信是机密的。当我们在线购物时，我们需要确保出售方是真实的。当我们把交易请求发送给银行时，我们还要保证信息的完整性不被破坏。

网络安全其实就是可以让我们放心使用互联网的一系列协议——没有安全攻击。最普通的可以为互联网提供安全的工具就是密码学，这是一门古老的技术，现在已经应用于网络安全了。本书首先向读者介绍密码学的基本原理，然后应用这些基本原理来说明网络安全协议。

本书的特点

本书的特点就是让读者更容易地理解密码学与网络安全。

结构

本书增加了一些讲授密码学与网络安全的方法。这些方法都是假定读者没有数论和抽象代数的知识。如果没有这些领域的知识背景，我们就没法讨论密码学与网络安全，所以我们在第 2 章、第 4 章和第 9 章讨论了这几方面的内容。如果读者对这几方面的内容熟悉的话，可以跳过这几章。从第 1~15 章讨论密码学。第 16~18 章讨论互联网的安全性。

视觉方法

本书运用图和文本之间的平衡关系，提供高技术的材料，而没有复杂的公式。与文本材料相关的 400 多幅图片，使本书的阐述更为直观。图片在说明难于理解的密码学概念和复杂的网络安全协议时起了非常重要的作用。

算法

算法在密码学的讲授中也是非常重要的。为了使讲述能够独立于任何的计算机语言，我们提供了算法伪代码，这样就可以更为容易地使用现代语言进行编程。

突出特点

为了能够快速查阅并立即找到某些重要概念，对这些概念我们做了突出显示。

示例

每一章都提供大量的示例，这些示例都应用本章讨论的概念。有些示例只表示出了概念和公式的直接应用；有些表示出了密码的输入/输出关系；还有的给出了一些额外的信息，可以使我们更好地理解一些复杂难懂的概念。

推荐阅读

在每一章的末尾，读者都会找到一个进一步阅读的书籍列表。

关键术语

在每一章的末尾还有一个关键术语列表。所有的关键术语都在书后的术语表中作了说明。

概要

在每一章的末尾，都有一个说明本章内容的“概要”。“概要”对这一章的重点作简要概括。

习题集

在每一章的末尾，还有一个习题集，通过练习可以增强对一些重要概念的理解，并应用这些重要概念。

附录

附录提供快速参考资料和对本书中所讨论概念的复习资料。附录里还有一些对数学问题的讨论，这样那些已经熟悉了这部分内容的读者就不必再在这些问题上分心了。

证明

在本书中提到了一些数学结论，为了强调应用这些结论的结果，而没有提供证明。这部分内容在附录 Q 中给出，有兴趣的读者可以参考。

术语表

在本书的末尾，为读者提供了内容广泛的术语列表。

内容

在介绍性的第 1 章之后，本书可以分成 4 个部分。

第 I 部分　对称密钥加密

第 I 部分介绍了传统对称密钥密码学和现代对称密钥密码学。这一部分中的几章，强调对称密钥密码学在提供安全方面的应用。第 I 部分包括第 2~8 章。

第 II 部分　非对称密钥加密

第 II 部分讨论非对称密钥密码学。这一部分中的几章，阐明了为什么非对称密钥密码学可以提供安全性。第 II 部分包括第 9 章和第 10 章。

第III部分　完整性、验证和密钥管理

第III部分阐明了加密 hash 函数是怎样提供其他安全性的，如信息的完整性和可信性。这一部分中的几章也说明了非对称密钥密码学和对称密钥密码学是怎样相互补充的。第III部分包括第 11~15 章。

第 IV 部分：网络安全

第IV部分阐明了在第 I 部分中用三章的篇幅讨论过的密码学，可以用来在互联网模型的三个层级上创建网络安全协议。第IV部分包括第 16~18 章。

如何使用本书

研究理论的读者和专业的读者都可以使用本书。有兴趣的读者还可以用本书来自学。作为教科书，这一课程可以开设一学期也可以开设 1/4 学期。下面是有关使用本书的几点意见。

- 强烈推荐把第 I ~III部分作为教学内容。
- 如果课程需要从密码学进入到有关网络安全的领域，我们推荐把第IV部分也作为教学内容。对第IV部分来说，必须要有一个有关网络方面的一个课程作为准备。

如果您在使用本书的过程中有任何意见或建议，可发邮件至 wkservice@vip.163.com，如果您的意见是正确的，我们将在后续版本中采用，并感谢您的参与！

在线学习中心

McGraw-Hill 在线学习中心有许多与本书有关的附加材料，读者可以访问 www.mhhe.com/forouzan 这个网站。老师和学生都可以使用这里的授课材料，如 PowerPoint 幻灯片。为学生提供奇数问题的答案，老师可以通过密码访问问题的完整解答。此外，McGraw-Hill 有一个名为 PageOut 的独一无二的产品，可以使得为该课程建立网站变得更为容易。使用这一工具不需要有 HTML 的预备知识，不需要花费很长时间，也不需要有特殊的设计方面的技术。PageOut 可以提供一系列的模板。用你的课程信息简单地填充这些模板，然后再点击 16 种设计中的一种就可以了。这一过程只需要花费一个小时，就可以建立一个专业设计的网站。虽然，PageOut 可以提供“即时”的生成，但是一个完整的网站才能提供强大的功能。运用交互式的教学大纲你可以发送与课程相符的内容，所以，当学生访问你的 PageOut 网站时，你的大纲就可以把他们引导到 Forouzan 在线学习中心的相关部分，或者引导到你自己的指定材料。

目　录

第III部分 完整性、验证和密钥管理

第 1 章

导　言

目标

本章的几个目标是：

- 明确三种安全目标
- 明确威胁安全目标的几种攻击
- 明确安全服务的内容及其和三种安全目标的联系
- 介绍两种实现安全机制的技术：密码术和密写术

我们生活在信息时代，在生活的各方面都需要保持信息畅通。换句话说，信息是一种资产，它和其他任何资产一样具有价值，需要被保护以避免攻击。

为了安全，信息要被隐藏起来以避免未经授权的访问(机密性)，被保护起来以避免未经授权的更改(完整性)，还要保证对授权实体随时可用(可用性)。

直到几十年前，信息才被组织在一起并保存在物理文档中。访问人被限制在该组织内已被授权并可信赖的少数几个人中，这样就实现了文档的机密性。

随着计算机的出现，信息储存被电子化。信息并不是存储于物理介质之中，而是存于计算机中。然而三种安全要求却并未因此而改变。存储于计算机中的信息要求具有机密性、完整性和有效性，然而实现这三种要求的方法各不相同并具有挑战性。

过去的 20 年中，计算机网络在信息应用上掀起了一场革命。信息是分散的，利用计算机网络，一个被授权的人可以从很远的地方发送或接收信息。上述三种要求(机密性、完整性和可用性)不但并未改变，而且具有了新的含义。不仅在信息被保存在计算机当中时要确保其机密性，而且应当有一种方法，能使信息在由一台计算机被发送到另一台计算机的过程中，也能保证其机密性。

在本章中，我们首先讨论信息安全的三个主要目标，然后再来了解一下什么样的攻击才能对这三个目标构成威胁，并且进一步讨论与这三种安全目标有关的安全服务。最后，我们详细论述提供安全服务的机制，同时介绍用来实现安全机制的技术。

1.1　安全目标

我们首先讨论三个安全目标：机密性、完整性和可用性(图 1-1)。