Mc Graw Hill Education 大学计算机教育国外著名教材系列 影印版

Cryptography and Network Security

密码学与网络安全

（中文导读英文版）

（美）Behrouz A. Forouzan 著

清华大学出版社

大学计算机教育国外著名教材系列(影印版)

密码学与网络安全

(中文导读英文版)

(美) Behrouz A. Forouzan 著

清华大学出版社

北 京

Behrouz A. Forouzan
Cryptography and Network Security
EISBN: 978-0-07-287022-0

北京市版权局著作权合同登记号　图字：01-2009-1211

图书在版编目(CIP)数据

密码学与网络安全(中文导读英文版)/(美)福罗赞(Forouzan，B.A.)著. —北京清华大学出版社，2009.4
(大学计算机教育国外著名教材系列(影印版))
书名原文：Cryptography and Network Security

ISBN 978-7-302-19727-0

Ⅰ. 密…　Ⅱ. 福…　Ⅲ. ①密码—理论—高等学校—教材—英文 ②计算机网络—安全技术—高等学校—教材—英文　Ⅳ. TN918.1 TP393.08
中国版本图书馆 CIP 数据核字(2009)第 036376 号

责任编辑：王　军　王　婷　　**封面设计**：久久度文化
版式设计：孔祥丰　　**责任校对**：成凤进
责任印制：何　芊

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：三河市李旗庄少明装订厂
经　　销：全国新华书店
开　　本：185×230　**印　张**：38.25　**字　数**：666 千字
版　　次：2009 年 4 月第 1 版　　**印　　次**：2009 年 4 月第1次印刷
印　　数：1～4000
定　　价：59.90 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：028629-01

符号及注释

$\mid$	Divides
$\nmid$	Does not divide
$\|\|$	Concatenation
$=$	Equality
$\neq$	Inequality
$\equiv$	Congruence
$\approx$	Approximate equality
$\leftarrow$	Assign
$\rightarrow$	Therefore
$\prod$	Product
$\sum$	Summation
$\oplus$	Modular addition
$\otimes$	Modular multiplication
$\|G\|$	order of a group
$D_K(C)$	Symmetric-key decryption
$E_K(P)$	Symmetric-key Encryption
$\phi(n)$	Euler's phi-function
F_n	Fermat number
gcd (a, b)	Greatest common divisor
$GF(2^n)$	The finite field of order 2^n
$GF(p)$	The finite field of order p
M_n	Mersenne number
mod	modulo operator (remainder after division)
n!	Factorial
$O(n)$	Big-O notation
ord(a)	Order of a
$\pi(n)$	Number of primes less than n
$\mathbf{Z}$	Set of integers
$\mathbf{Z}_n$	Set of nonnegative integers less than n
$\mathbf{Z}_n^*$	Set of nonnegative integers less than n and coprime to n

前言(Preface)

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(此部分内容可以从本书合作站点www.tupwk.com.cn/downpage上下载)。

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(此部分内容可以从本书合作站点www.tupwk.com.cn/downpage上下载)。

术语表和参考文献

本书为读者提供了内容广泛的术语列表以及作者引用的参考文献(此部分内容可以从本书合作站点www.tupwk.com.cn/downpage上下载)。

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至第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(Contents)

第I部分 对称密钥加密(Symmetric-Key Encipherment)

第III部分 完整性、验证和密钥管理

(Integrity, Authentication, and Key Management)