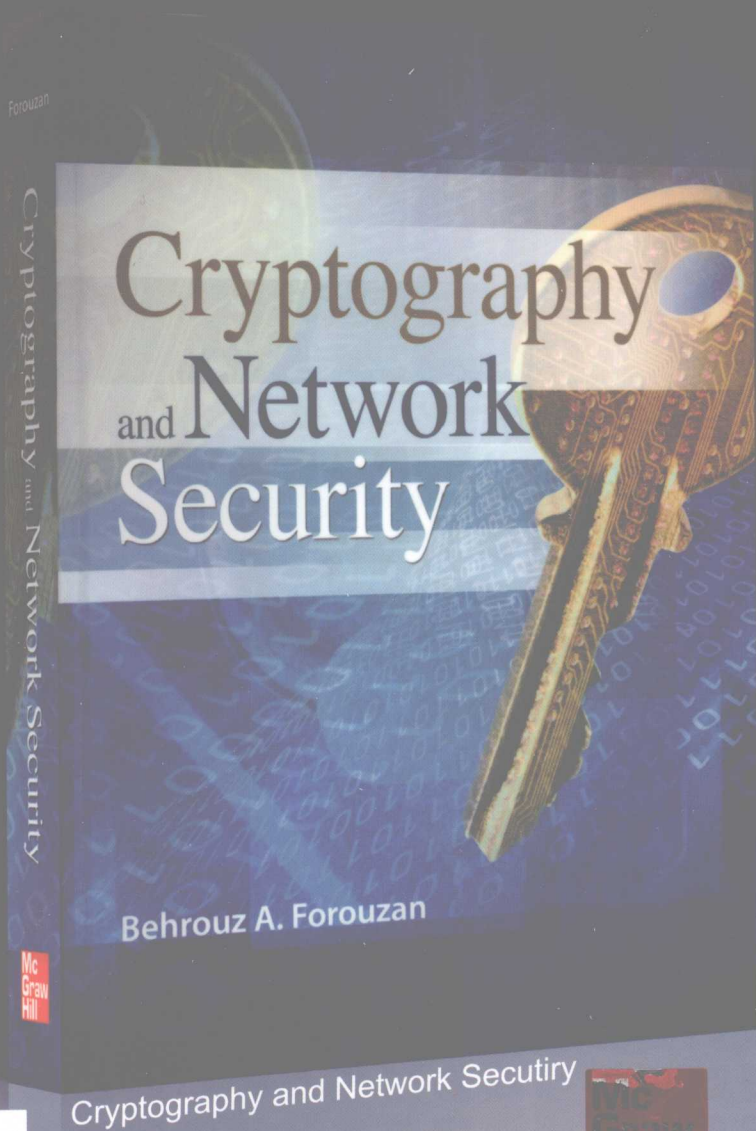


密码学 与网络安全

(美) Behrouz A. Forouzan 著 马振晗 贾军保 译



Mc
Graw
Hill Education

Mc
Graw
Hill

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

Copyright © 2008 by The McGraw-Hill Companies, Inc.

Original language published by The McGraw-Hill Companies, Inc. All Rights reserved. No part of this publication may be reproduced or distributed by any means, or stored in a database or retrieval system, without the prior permission of the publisher.

Simplified Chinese translation edition is published and distributed exclusively by Tsinghua University Press authorization by McGraw-Hill Education(Asia) Co., within the territory of the People's Republic of China (excluding Hong Kong, Macao SAR and Taiwan). Unauthorized export of this edition is a violation of the Act. Violation of this Law is subject to Civil and Criminal Penalties.

本书中文简体字翻译版由美国麦格劳-希尔教育出版(亚洲)公司授权清华大学出版社在中华人民共和国(不包括中国香港、澳门特别行政区和中国台湾地区)独家出版发行。未经许可之出口视为违反著作权法律之制裁。未经出版者预先书面许可,不得以任何方式复制或抄袭本书的任何部分。

北京市版权局著作权合同登记号 图字: 01-2007-3666

本书封面贴有 McGraw-Hill 公司防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话: 010-62782989 13701121933

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, 2008
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學需要。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,我们为这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

主任委员：

孙家广 清华大学教授

副主任委员：

周立柱 清华大学教授

委员（按姓氏笔画排序）：

王成山	天津大学教授
王 珊	中国人民大学教授
冯少荣	厦门大学教授
冯全源	西南交通大学教授
刘乐善	华中科技大学教授
刘腾红	中南财经政法大学教授
吉根林	南京师范大学教授
孙吉贵	吉林大学教授
阮秋琦	北京交通大学教授
何 晨	上海交通大学教授
吴百锋	复旦大学教授
李 彤	云南大学教授
沈钧毅	西安交通大学教授
邵志清	华东理工大学教授
陈 纯	浙江大学教授
陈 钟	北京大学教授
陈道蓄	南京大学教授
周伯生	北京航空航天大学教授
孟祥旭	山东大学教授
姚淑珍	北京航空航天大学教授
徐佩霞	中国科学技术大学教授
徐晓飞	哈尔滨工业大学教授
秦小麟	南京航空航天大学教授
钱培德	苏州大学教授
曹元大	北京理工大学教授
龚声蓉	苏州大学教授
谢希仁	中国人民解放军理工大学教授

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

查内

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。

准备时高师五第 教师民 长籍川京

本书的编写得到了许多专家的指导和帮助，特别是清华大学和北京邮电大学的专家们。在编写过程中，得到了许多专家和学者的帮助，特别是清华大学和北京邮电大学的专家们。在编写过程中，得到了许多专家和学者的帮助，特别是清华大学和北京邮电大学的专家们。在编写过程中，得到了许多专家和学者的帮助，特别是清华大学和北京邮电大学的专家们。

金德安网 位聘聘第

并本用刻研破

本书的编写得到了许多专家的指导和帮助，特别是清华大学和北京邮电大学的专家们。在编写过程中，得到了许多专家和学者的帮助，特别是清华大学和北京邮电大学的专家们。在编写过程中，得到了许多专家和学者的帮助，特别是清华大学和北京邮电大学的专家们。在编写过程中，得到了许多专家和学者的帮助，特别是清华大学和北京邮电大学的专家们。

目 录

第 1 章 导言	1
1.1 安全目标	1
1.1.1 机密性	2
1.1.2 完整性	2
1.1.3 可用性	2
1.2 攻击	2
1.2.1 威胁机密性的攻击	3
1.2.2 威胁完整性的攻击	3
1.2.3 威胁可用性的攻击	4
1.2.4 被动攻击与主动攻击	4
1.3 服务和机制	5
1.3.1 安全服务	5
1.3.2 安全机制	6
1.3.3 服务和机制之间的关系	8
1.4 技术	8
1.4.1 密码术	8
1.4.2 密写术	9
1.5 本书的其余部分	10
第 I 部分 对称密钥加密	10
第 II 部分 非对称密钥加密	11
第 III 部分 完整性、验证 和密钥管理	11
第 IV 部分 网络安全	11
1.6 推荐阅读	11
1.7 关键术语	11
1.8 概要	12
1.9 习题集	12

第 I 部分 对称密钥加密

第 2 章 密码数学 第 I 部分: 模算法、 同余和矩阵	17
2.1 整数算法	17

2.1.1 整数集	17
2.1.2 二进制运算	18
2.1.3 整数除法	18
2.1.4 整除性	20
2.1.5 线性丢番图方程	25
2.2 模运算	26
2.2.1 模算符	27
2.2.2 余集: \mathbb{Z}_n	27
2.2.3 同余	28
2.2.4 在集合 \mathbb{Z}_n 当中的运算	29
2.2.5 逆	32
2.2.6 加法表和乘法表	36
2.2.7 加法集和乘法集的不同	36
2.2.8 另外两个集合	37
2.3 矩阵	37
2.3.1 定义	37
2.3.2 运算和关系	38
2.3.3 行列式	39
2.3.4 逆	40
2.3.5 剩余阵	41
2.4 线性同余	41
2.4.1 单变量线性方程	41
2.4.2 线性方程组	42
2.5 推荐阅读	43
2.6 关键术语	44
2.7 概要	44
2.8 习题集	45

第 3 章 传统对称密钥密码

3.1 导言	51
3.1.1 Kerckhoff 原理	53
3.1.2 密码分析	53
3.1.3 传统密码的分类	55
3.2 代换密码	55

3.2.1	单码代换密码	56	5.2	现代流密码	135
3.2.2	多码代换密码	63	5.2.1	同步流密码	135
3.3	换位密码	74	5.2.2	异步流密码	140
3.3.1	无密钥换位密码	74	5.3	推荐阅读	140
3.3.2	有密钥的换位密码	75	5.4	关键术语	141
3.3.3	把两种方法组合起来	76	5.5	概要	141
3.4	流密码和分组密码	80	5.6	习题集	142
3.4.1	流密码	80	第6章	数据加密标准(DES)	145
3.4.2	分组密码	81	6.1	导言	145
3.4.3	组合	82	6.1.1	数据加密标准(DES)简史	145
3.5	推荐阅读	82	6.1.2	概观	146
3.6	关键术语	83	6.2	DES 的结构	146
3.7	概要	83	6.2.1	初始置换和最终置换	147
3.8	习题集	84	6.2.2	轮	148
第4章	密码数学		6.2.3	密码和反向密码	153
	第II部分: 代数结构	89	6.2.4	示例	158
4.1	代数结构	89	6.3	DES 分析	160
4.1.1	群	90	6.3.1	性质	160
4.1.2	环	96	6.3.2	设计标准	161
4.1.3	域	96	6.3.3	DES 的缺陷	162
4.1.4	小结	98	6.4	多重 DES	166
4.2	$GF(2^n)$ 域	98	6.4.1	双重 DES	167
4.2.1	多项式	99	6.4.2	三重 DES	168
4.2.2	运用一个生成器	106	6.5	DES 的安全性	169
4.2.3	小结	108	6.5.1	蛮力攻击	169
4.3	推荐阅读	108	6.5.2	差分密码分析	169
4.4	关键术语	109	6.5.3	线性密码分析	170
4.5	概要	109	6.6	推荐阅读	170
4.6	习题集	110	6.7	关键术语	170
第5章	现代对称密钥密码	113	6.8	概要	171
5.1	现代分组密码	113	6.9	习题集	171
5.1.1	代换与换位	114	第7章	高级加密标准(AES)	175
5.1.2	作为置换群的分组密码	115	7.1	导言	175
5.1.3	现代分组密码的成分	117	7.1.1	高级加密标准(AES)简史	175
5.1.4	换字盒	121	7.1.2	标准	176
5.1.5	乘积密码	125	7.1.3	轮	176
5.1.6	两类乘积密码	127	7.1.4	数据单位	177
5.1.7	关于分组密码的攻击	130	7.1.5	每一个轮的结构	179

7.2	转换	180
7.2.1	代换	180
7.2.2	置换	185
7.2.3	混合	186
7.2.4	密钥加	189
7.3	密钥扩展	190
7.3.1	在 AES-128 中的 密钥扩展	190
7.3.2	AES-192 和 AES-256 中 的密钥扩展	194
7.3.3	密钥扩展分析	194
7.4	密码	195
7.4.1	源设计	195
7.4.2	选择性设计	197
7.5	示例	198
7.6	AES 的分析	200
7.6.1	安全性	201
7.6.2	可执行性	201
7.6.3	复杂性和费用	201
7.7	推荐阅读	201
7.8	关键术语	202
7.9	概要	202
7.10	习题集	203
第 8 章 应用现代对称密钥		
	密码的加密	207
8.1	现代分组密码的应用	207
8.1.1	电子密码本模式	208
8.1.2	密码分组链接(CBC)模式	210
8.1.3	密码反馈(CFB)模式	212
8.1.4	输出反馈(OFB)模式	215
8.1.5	计数器(CTR)模式	217
8.2	流密码的应用	219
8.2.1	RC4	219
8.2.2	A5/1	222
8.3	其他问题	224
8.3.1	密钥管理	224
8.3.2	密钥生成	225
8.4	推荐阅读	225

8.5	关键术语	225
8.6	概要	226
8.7	习题集	227

第 II 部分 非对称密钥加密

第 9 章 密码数学 第 III 部分: 素数		
	及其相关的同余方程	231
9.1	素数	231
9.1.1	定义	231
9.1.2	素数的基数	232
9.1.3	素性检验	233
9.1.4	Euler Phi-(欧拉 $\phi(n)$)函数	234
9.1.5	Fermat(费尔马)小定理	236
9.1.6	Euler 定理	237
9.1.7	生成素数	238
9.2	素性测试	239
9.2.1	确定性算法	240
9.2.2	概率算法	241
9.2.3	推荐的素性检验	245
9.3	因数分解	246
9.3.1	算术基本定理	246
9.3.2	因数分解方法	247
9.3.3	Fermat 方法	248
9.3.4	Pollard $p-1$ 方法	249
9.3.5	Pollard rho 方法	250
9.3.6	更有效的方法	252
9.4	中国剩余定理	253
9.5	二次同余	254
9.5.1	二次同余模一个素数	255
9.5.2	二次同余模一个复合数	256
9.6	指数与对数	257
9.6.1	指数	257
9.6.2	对数	259
9.7	推荐阅读	264
9.8	关键术语	264
9.9	概要	265
9.10	习题集	266

第 10 章	非对称密钥密码学	271
10.1	引言	271
10.1.1	密钥	272
10.1.2	一般概念	272
10.1.3	双方的需要	274
10.1.4	单向暗门函数	274
10.1.5	背包密码系统	275
10.2	RSA 密码系统	278
10.2.1	简介	278
10.2.2	过程	279
10.2.3	一些普通的例子	281
10.2.4	针对 RSA 的攻击	282
10.2.5	建议	287
10.2.6	最优非对称加密填充 (OAEP)	288
10.2.7	应用	290
10.3	RABIN 密码系统	291
10.3.1	过程	291
10.3.2	Rabin 系统的安全性	293
10.4	ELGAMAL 密码系统	293
10.4.1	ElGamal 密码系统	294
10.4.2	过程	294
10.4.3	证明	295
10.4.4	分析	296
10.4.5	ElGamal 的安全性	296
10.4.6	应用	298
10.5	椭圆曲线密码系统	298
10.5.1	基于实数的椭圆曲线	298
10.5.2	基于 $\text{GF}(p)$ 的 椭圆曲线	300
10.5.3	基于 $\text{GF}(2^n)$ 的 椭圆曲线	302
10.5.4	模拟 ElGamal 的椭圆 曲线加密系统	304
10.6	推荐阅读	306
10.7	关键术语	307
10.8	概要	307
10.9	习题集	309

第 III 部分 完整性、验证 和密钥管理

第 11 章	信息的完整性和信息验证	315
11.1	信息完整性	315
11.1.1	文档与指纹	315
11.1.2	信息与信息摘要	316
11.1.3	区别	316
11.1.4	检验完整性	316
11.1.5	加密 hash 函数标准	316
11.2	随机预言模型	319
11.2.1	鸽洞原理	320
11.2.2	生日问题	320
11.2.3	针对随机预言模型 的攻击	322
11.2.4	针对结构的攻击	327
11.3	信息验证	327
11.3.1	修改检测码	327
11.3.2	信息验证代码(MAC)	328
11.4	推荐阅读	331
11.5	关键术语	332
11.6	概要	332
11.7	习题集	333
第 12 章	加密 hash 函数	337
12.1	引言	337
12.1.1	迭代 hash 函数	337
12.1.2	两组压缩函数	338
12.2	SHA-512	341
12.2.1	简介	341
12.2.2	压缩函数	345
12.2.3	分析	349
12.3	WHIRLPOOL	349
12.3.1	Whirlpool 密码	350
12.3.2	小结	357
12.3.3	分析	357
12.4	推荐阅读	357
12.5	关键术语	358

12.6	概要	359	14.1.1	数据源验证与 实体验证	387
12.7	习题集	359	14.1.2	验证的类型	388
第 13 章	数字签名	363	14.1.3	实体验证和密钥管理	388
13.1	对比	363	14.2	口令	388
13.1.1	包含性	363	14.2.1	固定口令	388
13.1.2	验证方法	364	14.2.2	一次性密码	391
13.1.3	关系	364	14.3	挑战—应答	392
13.1.4	二重性	364	14.3.1	对称密钥密码的运用	393
13.2	过程	364	14.3.2	带密钥 hash 函数 的应用	394
13.2.1	密钥需求	364	14.3.3	非对称密钥密码的 应用	395
13.2.2	摘要签名	365	14.3.4	数字签名的应用	396
13.3	服务	366	14.4	零知识	397
13.3.1	信息身份验证	366	14.4.1	Fiat-Shamir 协议	397
13.3.2	信息完整性	366	14.4.2	Feige-Fiat-Shamir 协议	400
13.3.3	不可否认性	367	14.4.3	Guillou-Quisquater 协议	400
13.3.4	机密性	368	14.5	生物测试	401
13.4	针对数字签名的攻击	368	14.5.1	设备	401
13.4.1	攻击类型	368	14.5.2	注册	402
13.4.2	伪造类型	369	14.5.3	验证	402
13.5	数字签名方案	369	14.5.4	技术	402
13.5.1	RSA 数字签名方案	369	14.5.5	准确性	403
13.5.2	ElGamal 数字 签名方案	373	14.5.6	应用	404
13.5.3	Schnorr 数字 签名方案	375	14.6	推荐阅读	404
13.5.4	数字签名标准(DSS)	378	14.7	关键术语	404
13.5.5	椭圆曲线数字 签名方案	380	14.8	概要	405
13.6	变化与应用	382	14.9	习题集	405
13.6.1	变化	382	第 15 章	密钥管理	407
13.6.2	应用	383	15.1	对称密钥分配	407
13.7	推荐阅读	383	15.2	KERBEROS	413
13.8	关键术语	384	15.2.1	服务器	413
13.9	概要	384	15.2.2	操作	414
13.10	习题集	385	15.2.3	不同服务器的运用	414
第 14 章	实体验证	387	15.2.4	Kerberos 第五版	415
14.1	引言	387			

15.2.5	领域	416
15.3	对称密钥协定	416
15.3.1	Diffie-Hellman 密钥协定	416
15.3.2	站对站密钥协定	420
15.4	公钥分配	421
15.4.1	公钥公布	422
15.4.2	可信中心	422
15.4.3	可信中心的控制	423
15.4.4	认证机关	423
15.4.5	X.509	424
15.4.6	公钥基础设施(PKI)	427
15.5	推荐阅读	429
15.6	关键术语	430
15.7	概要	430
15.8	习题集	431

第IV部分 网络安全

第16章 应用层的安全性:

	PGP 和 S/MIME	435
16.1	电子邮件	435
16.1.1	电子邮件的构造	435
16.1.2	电子邮件的安全性	437
16.2	PGP	438
16.2.1	情景	438
16.2.2	密钥环	440
16.2.3	PGP 证书	442
16.2.4	密钥撤回	449
16.2.5	从环中提取消息	449
16.2.6	PGP 包	451
16.2.7	PGP 信息	456
16.2.8	PGP 的应用	457
16.3	S/MIME	458
16.3.1	MIME	458
16.3.2	S/MIME	463
16.3.3	S/MIME 的应用	467
16.4	推荐阅读	467
16.5	关键术语	467

16.6	概要	467
16.7	习题集	468

第17章 传输层的安全性:

	SSL 和 TLS	471
17.1	SSL 结构	472
17.1.1	服务	472
17.1.2	密钥交换算法	472
17.1.3	加密/解密算法	474
17.1.4	散列算法	475
17.1.5	密码套件	476
17.1.6	压缩算法	477
17.1.7	加密参数的生成	477
17.1.8	会话和连接	478
17.2	4 个协议	480
17.2.1	握手协议	481
17.2.2	改变密码规格协议	487
17.2.3	告警协议	488
17.2.4	记录协议	488
17.3	SSL 信息构成	491
17.3.1	改变密码规格协议	491
17.3.2	告警协议	491
17.3.3	握手协议	492
17.3.4	应用数据	498
17.4	传输层安全	499
17.4.1	版本	499
17.4.2	密码套件	500
17.4.3	加密秘密的生成	500
17.4.4	告警协议	502
17.4.5	握手协议	503
17.4.6	记录协议	504
17.5	推荐阅读	505
17.6	关键术语	505
17.7	概要	506
17.8	习题集	506

第18章 网络层的安全: IPsec

18.1	两种模式	510
18.2	两个安全协议	512
18.2.1	验证文件头(AH)	512

18.2.2	封装安全载荷(ESP)	513	附录 C	TCP/IP 套件	557
18.2.3	IPv4 和 IPv6	514	附录 D	初等概率	561
18.2.4	AH 和 ESP	514	附录 E	生日问题	565
18.2.5	IPSec 提供的服务	514	附录 F	信息论	569
18.3	安全关联	516	附录 G	不可约多项式与 本原多项式列举	575
18.3.1	安全关联的概念	516	附录 H	小于 10 000 的素数	577
18.3.2	安全关联数据库(SAD)	516	附录 I	整数的素因数	581
18.4	安全策略	518	附录 J	小于 1000 素数的 一次本原根列表	585
18.5	互联网密钥交换(IKE)	521	附录 K	随机数生成器	587
18.5.1	改进的 Diffie-Hellman 密钥交换	522	附录 L	复杂度	593
18.5.2	IKE 阶段	524	附录 M	ZIP	599
18.5.3	阶段和模式	524	附录 N	DES 差分密码分析和 DES 线性密码分析	603
18.5.4	阶段 I: 主模式	525	附录 O	简化 DES(S-DES)	611
18.5.5	阶段 I: 野蛮模式	530	附录 P	简化 AES(S-AES)	619
18.5.6	阶段 II: 快速模式	532	附录 Q	一些证明	631
18.5.7	SA 算法	534	术语表		639
18.6	ISAKMP	535	参考文献		657
18.6.1	一般文件头	535			
18.6.2	有效载荷	536			
18.7	推荐阅读	544			
18.8	关键术语	544			
18.9	概要	544			
18.10	习题集	545			
附录 A	ASCII	549			
附录 B	标准与标准化组织	551			

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)。