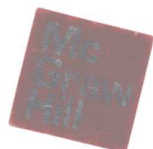


Cryptography and Network Security

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
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 written permission of the publisher.

Authorized English language edition jointly published by McGraw-Hill Education (Asia) Co. and Tsinghua University Press. This edition is authorized for sale only to the educational and training institutions, and 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 Copyright Act. Violation of this Law is subject to Civil and Criminal Penalties.

本书英文影印版由清华大学出版社和美国麦格劳-希尔教育出版(亚洲)公司合作出版。此版本仅限在中华人民共和国境内(不包括中国香港、澳门特别行政区及中国台湾地区)针对教育及培训机构之销售。未经许可之出口,视为违反著作权法,将受法律之制裁。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: 01-2009-1211

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(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

版式设计: 孔祥丰

责任印制: 何 芊

出版发行: 清华大学出版社

<http://www.tup.com.cn>

社 总 机: 010-62770175

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

封面设计: 久久度文化

责任校对: 成凤进

地 址: 北京清华大学学研大厦 A 座

邮 编: 100084

邮 购: 010-62786544

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

$ $	Divides
$\nmid$	Does not divide
$ $	Concatenation
$=$	Equality
$\neq$	Inequality
$\equiv$	Congruence
$\approx$	Approximate equality
$\leftarrow$	Assign
$\rightarrow$	Therefore
Π	Product
Σ	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- <i>O</i> notation
$\text{ord}(a)$	Order of a
$\pi(n)$	Number of primes less than n
$\mathbb{Z}$	Set of integers
$\mathbb{Z}_n$	Set of nonnegative integers less than n
$\mathbb{Z}_n^*$	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一起了。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/download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/download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/download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1章 导言(Introduction).....	1
1.1 安全目标(SEcurity GOALS).....	2
1.1.1 机密性(Confidentiality).....	2
1.1.2 完整性(Integrity).....	3
1.1.3 可用性(Availability).....	3
1.2 攻击(ATTACKS).....	3
1.2.1 威胁机密性的攻击(Attacks Threatening Confidentiality).....	3
1.2.2 威胁完整性的攻击(Attacks Threatening Integrity).....	4
1.2.3 威胁可用性的攻击(Attacks Threatening Availability).....	5
1.2.4 被动攻击与主动攻击(Passive Versus Active Attacks).....	5
1.3 服务和机制(SERVICES AND MECHANISM).....	6
1.3.1 安全服务(Security Services).....	6
1.3.2 安全机制(Security Mechanisms).....	7
1.3.3 服务和机制之间的关系(Relation between Services and Mechanisms).....	8
1.4 技术(TECHNIQUES).....	9
1.4.1 密码术(Cryptography).....	9
1.4.2 密写术(Steganography).....	10
1.5 本书的其余部分(THE REST OF THE BOOK).....	12
1.6 推荐阅读(RECOMMENDED READING).....	12
1.7 关键术语(KEY TERMS).....	13
1.8 概要(SUMMARY).....	13
1.9 习题集(PRACTICE SET).....	14

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

第2章 密码数学I: 模算法、同余和矩阵(Mathematics of Cryptography I:

Modular Arithmetic, Congruence, and Matrices) 19

2.1 整数算法(INTEGER ARITHMETIC) 20

2.1.1 整数集(Set of Integers) 20

2.1.2 二进制运算(Binary Operations) 20

2.1.3 整数除法(Integer Division) 21

2.1.4 整除性(Divisibility) 22

2.1.5 线性丢番图方程(Linear Diophantine Equations) 28

2.2 模运算(MODULAR ARITHMETIC) 29

2.2.1 模算符(Modulo Operator) 29

2.2.2 余集: Z_n (Set of Residues: Z_n) 30

2.2.3 同余(Congruence) 30

2.2.4 在集合 Z_n 当中的运算(Operations in Z_n) 32

2.2.5 逆(Inverses) 35

2.2.6 加法表和乘法表(Addition and Multiplication Tables) 39

2.2.7 加法集和乘法集的不同(Different Sets for Addition and Multiplication) 39

2.2.8 另外两个集合(Two More Sets) 40

2.3 矩阵(MATRICES) 40

2.3.1 定义(Definitions) 40

2.3.2 运算和关系(Operations and Relations) 41

2.3.3 行列式(Determinant) 43

2.3.4 逆(Inverses) 44

2.3.5 剩余阵(Residue Matrices) 44

2.4 线性同余(LINEAR CONGRUENCE) 45

2.4.1 单变量线性方程(Single-Variable Linear Equations) 45

2.4.2 线性方程组(Set of Linear Equations) 46

2.5 推荐阅读(RECOMMENDED READING) 47

2.6 关键术语(KEY TERMS) 47

2.7 概要(SUMMARY) 48

2.8 习题集(PRACTICE SET) 49

第3章 传统对称密钥密码(Traditional Symmetric-Key Ciphers) 55

3.1 导言(INTRODUCTION) 56

3.1.1 Kerckhoff原理(Kerckhoff's Principle) 57

3.1.2	密码分析(Cryptanalysis)·····	57
3.1.3	传统密码的分类(Categories of Traditional Ciphers)·····	60
3.2	代换密码(SUBSTITUTION CIPHERS)·····	61
3.2.1	单码代换密码(Monoalphabetic Ciphers)·····	61
3.2.2	多码代换密码(Polyalphabetic Ciphers)·····	69
3.3	换位密码(TRANSPOSITION CIPHERS)·····	80
3.3.1	无密钥换位密码(Keyless Transposition Ciphers)·····	81
3.3.2	有密钥的换位密码(Keyed Transposition Ciphers)·····	82
3.3.3	把两种方法组合起来(Combining Two Approaches)·····	83
3.4	流密码和分组密码(STREAM AND BLOCK CIPHERS)·····	87
3.4.1	流密码(Stream Ciphers)·····	87
3.4.2	分组密码(Block Ciphers)·····	89
3.4.3	组合(Combination)·····	89
3.5	推荐阅读(RECOMMENDED READING)·····	90
3.6	关键术语(KEY TERMS)·····	90
3.7	概要(SUMMARY)·····	91
3.8	习题集(PRACTICE SET)·····	92
第4章	密码数学II: 代数结构(Mathematics of Cryptography II: Algebraic Structures)·····	97
4.1	代数结构(ALGEBRAIC STRUCTURES)·····	98
4.1.1	群(Groups)·····	98
4.1.2	环(Ring)·····	104
4.1.3	域(Field)·····	105
4.1.4	小结(Summary)·····	107
4.2	$GF(2^n)$ 域($GF(2^n)$ FIELDS)·····	107
4.2.1	多项式(Polynomials)·····	108
4.2.2	运用一个生成器(Using a Generator)·····	114
4.2.3	小结(Summary)·····	117
4.3	推荐阅读(RECOMMENDED READING)·····	117
4.4	关键术语(KEY TERMS)·····	118
4.5	概要(SUMMARY)·····	118
4.6	习题集(PRACTICE SET)·····	119

第5章 现代对称密钥密码(Introduction to Modern Symmetric-Key Ciphers)	123
5.1 现代分组密码(MODERN BLOCK CIPHERS)	124
5.1.1 代换与换位(Substitution or Transposition)	125
5.1.2 作为置换群的分组密码(Block Ciphers as Permutation Groups)	125
5.1.3 现代分组密码的成分(Components of a Modern Block Cipher)	128
5.1.4 换字盒(S-Boxes)	132
5.1.5 乘积密码(Product Ciphers)	136
5.1.6 两类乘积密码(Two Classes of Product Ciphers)	139
5.1.7 关于分组密码的攻击(Attacks on Block Ciphers)	143
5.2 现代流密码(MODERN STREAM CIPHERS)	148
5.2.1 同步流密码(Synchronous Stream Ciphers)	149
5.2.2 异步流密码(Nonsynchronous Stream Ciphers)	154
5.3 推荐阅读(RECOMMENDED READING)	154
5.4 关键术语(KEY TERMS)	154
5.5 概要(SUMMARY)	155
5.6 习题集(PRACTICE SET)	156
第6章 数据加密标准(Data Encryption Standard (DES))	159
6.1 引言(INTRODUCTION)	159
6.1.1 数据加密标准(DES)简史(History)	159
6.1.2 概观(Overview)	160
6.2 DES的结构(DES STRUCTURE)	160
6.2.1 初始置换和最终置换(Initial and Final Permutations)	160
6.2.2 轮(Rounds)	163
6.2.3 密码和反向密码(Cipher and Reverse Cipher)	167
6.2.4 示例(Examples)	173
6.3 DES分析(DES ANALYSIS)	175
6.3.1 性质(Properties)	175
6.3.2 设计标准(Design Criteria)	176
6.3.3 DES的缺陷(DES Weaknesses)	177
6.4 多重 DES(MULTIPLE DES)	181
6.4.1 双重DES(Double DES)	182
6.4.2 三重DES(Triple DES)	184
6.5 DES的安全性(SEcurity OF DES)	185
6.5.1 蛮力攻击(Brute-Force Attack)	185

6.5.2	差分密码分析(Differential Cryptanalysis)	185
6.5.3	线性密码分析(Linear Cryptanalysis)	186
6.6	推荐阅读(RECOMMENDED READING)	186
6.7	关键术语(KEY TERMS)	186
6.8	概要(SUMMARY)	187
6.9	习题集(PRACTICE SET)	188
第7章	高级加密标准(Advanced Encryption Standard (AES))	191
7.1	导言(INTRODUCTION)	191
7.1.1	高级加密标准(AES)简史(History)	191
7.1.2	标准(Criteria)	192
7.1.3	轮(Rounds)	192
7.1.4	数据单位(Data Units)	193
7.1.5	每一个轮的结构(Structure of Each Round)	195
7.2	转换(TRANSFORMATIONS)	196
7.2.1	代换(Substitution)	196
7.2.2	置换(Permutation)	202
7.2.3	混合(Mixing)	203
7.2.4	密钥加(Key Adding)	206
7.3	密钥扩展(KEY EXPANSION)	207
7.3.1	在AES-128中的密钥扩展(Key Expansion in AES-128)	208
7.3.2	AES-192和AES-256中的密钥扩展 (Key Expansion in AES-192 and AES-256)	212
7.3.3	密钥扩展分析(Key-Expansion Analysis)	212
7.4	密码(CIPHERS)	213
7.4.1	源设计(Original Design)	213
7.4.2	选择性设计(Alternative Design)	214
7.5	示例(EXAMPLES)	216
7.6	AES的分析(ANALYSIS OF AES)	219
7.6.1	安全性(Security)	219
7.6.2	可执行性(Implementation)	219
7.6.3	复杂性和费用(Simplicity and Cost)	220
7.7	推荐阅读(RECOMMENDED READING)	220
7.8	关键术语(KEY TERMS)	220
7.9	概要(SUMMARY)	221

7.10 习题集(PRACTICE SET).....	222
第8章 应用现代对称密钥密码的加密(Encipherment Using Modern Symmetric-Key Ciphers).....	225
8.1 现代分组密码的应用(USE OF MODERN BLOCK CIPHERS).....	225
8.1.1 电子密码本模式(Electronic Codebook (ECB) Mode).....	226
8.1.2 密码分组链接(CBC)模式(Cipher Block Chaining (CBC) Mode).....	228
8.1.3 密码反馈(CFB)模式(Cipher Feedback (CFB) Mode).....	231
8.1.4 输出反馈(OFB)模式(Output Feedback (OFB) Mode).....	234
8.1.5 计数器(CTR)模式(Counter (CTR) Mode).....	236
8.2 流密码的应用(USE OF STREAM CIPHERS).....	238
8.2.1 RC4.....	238
8.2.2 A5/1.....	242
8.3 其他问题(OTHER ISSUES).....	244
8.3.1 密钥管理(Key Management).....	244
8.3.2 密钥生成(Key Generation).....	244
8.4 推荐阅读(RECOMMENDED READING).....	245
8.5 关键技术语(KEY TERMS).....	245
8.6 概要(SUMMARY).....	246
8.7 习题集(PRACTICE SET).....	246

第II部分 非对称密钥加密(Asymmetric-Key Encipherment)

第9章 密码数学III: 素数及其相关的同余方程(Mathematics of Cryptography III: Primes and Related Congruence Equations).....	251
9.1 素数(PRIMES).....	251
9.1.1 定义(Definition).....	251
9.1.2 素数的基数(Cardinality of Primes).....	252
9.1.3 素性检验(Checking for Primeness).....	253
9.1.4 Euler Phi-函数(Euler's Phi-Function).....	254
9.1.5 Fermat(费尔马)小定理(Fermat's Little Theorem).....	256
9.1.6 Euler定理(Euler's Theorem).....	257
9.1.7 生成素数(Generating Primes).....	258
9.2 素性测试(PRIMALITY TESTING).....	260
9.2.1 确定性算法(Deterministic Algorithms).....	260
9.2.2 概率算法(Probabilistic Algorithms).....	261

9.2.3	推荐的素性检验(Recommended Primality Test)	266
9.3	因数分解(FACTORIZATION)	267
9.3.1	算术基本定理(Fundamental Theorem of Arithmetic)	267
9.3.2	因数分解方法(Factorization Methods)	268
9.3.3	Fermat方法(Fermat Method)	269
9.3.4	Pollard $p-1$ 方法(Pollard $p-1$ Method)	270
9.3.5	Pollard rho方法(Pollard rho Method)	271
9.3.6	更有效的方法(More Efficient Methods)	272
9.4	中国剩余定理(CHINESE REMAINDER THEOREM)	274
9.5	二次同余(QUADRATIC CONGRUENCE)	276
9.5.1	二次同余模一个素数(Quadratic Congruence Modulo a Prime)	276
9.5.2	二次同余模一个复合数(Quadratic Congruence Modulo a Composite)	277
9.6	指数与对数(EXPONENTIATION AND LOGARITHM)	278
9.6.1	指数(Exponentiation)	279
9.6.2	对数(Logarithm)	281
9.7	推荐阅读(RECOMMENDED READING)	286
9.8	关键术语(KEY TERMS)	286
9.9	概要(SUMMARY)	287
9.10	习题集(PRACTICE SET)	288
第10章	非对称密钥密码学(Asymmetric-Key Cryptography)	293
10.1	导言(INTRODUCTION)	293
10.1.1	密钥(Keys)	294
10.1.2	一般概念(General Idea)	294
10.1.3	双方的需要(Need for Both)	296
10.1.4	单向暗门函数(Trapdoor One-Way Function)	296
10.1.5	背包密码系统(Knapsack Cryptosystem)	298
10.2	RSA密码系统(RSA CRYPTOSYSTEM)	301
10.2.1	简介(Introduction)	301
10.2.2	过程(Procedure)	301
10.2.3	一些普通的例子(Some Trivial Examples)	304
10.2.4	针对RSA的攻击(Attacks on RSA)	305
10.2.5	建议(Recommendations)	310
10.2.6	最优非对称加密填充 (Optimal Asymmetric Encryption Padding (OAEP))	311

10.2.7	应用(Applications)	314
10.3	RABIN密码系统(RABIN CRYPTOSYSTEM)	314
10.3.1	过程(Procedure)	315
10.3.2	Rabin系统的安全性(Security of the Rabin System)	317
10.4	ELGAMAL密码系统(ELGAMAL CRYPTOSYSTEM)	317
10.4.1	ElGamal密码系统(ElGamal Cryptosystem)	317
10.4.2	过程(Procedure)	317
10.4.3	证明(Proof)	319
10.4.4	分析(Analysis)	319
10.4.5	ElGamal的安全性(Security of ElGamal)	320
10.4.6	应用(Application)	321
10.5	椭圆曲线密码系统(ELLIPTIC CURVE CRYPTOSYSTEMS)	321
10.5.1	基于实数的椭圆曲线(Elliptic Curves over Real Numbers)	321
10.5.2	基于 $GF(p)$ 的椭圆曲线(Elliptic Curves over $GF(p)$)	324
10.5.3	基于 $GF(2^n)$ 的椭圆曲线(Elliptic Curves over $GF(2^n)$)	326
10.5.4	模拟ElGamal的椭圆曲线加密系统 (Elliptic Curve Cryptography Simulating ElGamal)	328
10.6	推荐阅读(RECOMMENDED READING)	330
10.7	关键术语(KEY TERMS)	331
10.8	概要(SUMMARY)	331
10.9	习题集(PRACTICE SET)	333

第III部分 完整性、验证和密钥管理

(Integrity, Authentication, and Key Management)

第11章 信息的完整性和信息验证

(Message Integrity and Message Authentication) 339

11.1	信息完整性(MESSAGE INTEGRITY)	339
11.1.1	文档与指纹(Document and Fingerprint)	340
11.1.2	信息与信息摘要(Message and Message Digest)	340
11.1.3	区别(Difference)	340
11.1.4	检验完整性(Checking Integrity)	340
11.1.5	加密hash函数标准(Cryptographic Hash Function Criteria)	340
11.2	随机预言模型(RANDOM ORACLE MODEL)	343
11.2.1	鸽洞原理(Pigeonhole Principle)	345

11.2.2	生日问题(Birthday Problems).....	345
11.2.3	针对随机预言模型的攻击(Attacks on Random Oracle Model).....	347
11.2.4	针对结构的攻击(Attacks on the Structure).....	351
11.3	信息验证(MESSAGE AUTHENTICATION).....	352
11.3.1	修改检测码(Modification Detection Code).....	352
11.3.2	信息验证代码(Message Authentication Code (MAC)).....	353
11.4	推荐阅读(RECOMMENDED READING).....	357
11.5	关键术语(KEY TERMS).....	357
11.6	概要(SUMMARY).....	358
11.7	习题集(PRACTICE SET).....	359
第12章	加密hash函数(Cryptographic Hash Functions).....	363
12.1	导言(INTRODUCTION).....	363
12.1.1	迭代hash函数(Iterated Hash Function).....	363
12.1.2	两组压缩函数(Two Groups of Compression Functions).....	364
12.2	SHA-512.....	367
12.2.1	简介(Introduction).....	367
12.2.2	压缩函数(Compression Function).....	372
12.2.3	分析(Analysis).....	375
12.3	WHIRLPOOL.....	376
12.3.1	Whirlpool密码(Whirlpool Cipher).....	377
12.3.2	小结(Summary).....	384
12.3.3	分析(Analysis).....	384
12.4	推荐阅读(RECOMMENDED READING).....	384
12.5	关键术语(KEY TERMS).....	385
12.6	概要(SUMMARY).....	385
12.7	习题集(PRACTICE SET).....	386
第13章	数字签名(Digital Signature).....	389
13.1	对比(COMPARISON).....	390
13.1.1	包含性(Inclusion).....	390
13.1.2	验证方法(Verification Method).....	390
13.1.3	关系(Relationship).....	390
13.1.4	二重性(Duplicity).....	390
13.2	过程(PROCESS).....	390
13.2.1	密钥需求(Need for Keys).....	391