普通高等教育“十一五”国家级规划教材

信息安全专业系列教材

现代密码学教程

Xiandai Mimaxue Jiaocheng

谷利泽　郑世慧　杨义先　编著

北京邮电大学出版社
www.buptpress.com

普通高等教育“十一五”国家级规划教材

信息安全专业系列教材

现代密码学教程

谷利泽　郑世慧　杨义先　编著

北京邮电大学出版社
·北京·

内 容 简 介

本书是一本关于现代密码学的基础教材。全书共分 11 章和 1 个附录(参考文献),主要分成 4 部分。第 1 部分(第 1～3 章)主要介绍现代密码学的基础知识,包括密码学的基本概念、基本体制、基本思想以及所用到的理论知识等。第 2 部分(第 4～7 章)主要介绍现代密码学的基本技术,包括对称密码技术(分组密码、序列密码)、Hash 函数、公钥密码技术等。第 3 部分(第 8～10 章)主要介绍现代密码学的基本应用,包括数字签名技术、密钥管理、密码协议等。第 4 部分(第 11 章)对现代密码学的今后发展进行了展望。

本书重点突出、抓住核心;通俗易懂、容易入门;例证丰富、快速理解;习题多样、牢固掌握。

本书是信息安全专业的专业基础课教材,适合作为高等院校信息科学专业或其他相关专业本科生和研究生的教材,也可作为相关领域的教师、科研人员以及工程技术人员的参考书。

图书在版编目(CIP)数据

现代密码学教程/谷利泽,郑世慧,杨义先编著. —北京:北京邮电大学出版社,2009

ISBN 978-7-5635-2019-0

Ⅰ. 现… Ⅱ. ①谷…②郑…③杨… Ⅲ. 密码术—高等学校—教材 Ⅳ. TN918.1

中国版本图书馆 CIP 数据核字(2009)第 122449 号

书　　名:现代密码学教程
作　　者:谷利泽　郑世慧　杨义先
责任编辑:赵健琳
出版发行:北京邮电大学出版社
社　　址:北京市海淀区西土城路 10 号(邮编:100876)
发 行 部:电话:010-62282185　传真:010-62283578
E-mail:publish@bupt.edu.cn
经　　销:各地新华书店
印　　刷:北京忠信诚胶印厂
开　　本:787 mm×960 mm　1/16
印　　张:24
字　　数:524 千字
印　　数:1—3 000 册
版　　次:2009 年 8 月第 1 版　2009 年 8 月第 1 次印刷

ISBN 978-7-5635-2019-0　　定　价:38.00 元

信息安全专业系列教材（第2版）

编 委 会

第 2 版总序

发展 21 世纪中国信息安全要靠教育，而搞好信息安全教育就需要好的教材。2004 年，灵创团队北京邮电大学信息安全中心完成了第一套信息安全专业本科系列教材，该套教材被教育部列入了“普通高等教育‘十五’国家级规划教材”。至今，三年多的时间过去了，这套教材在信息安全专业的教学中发挥了重要的作用，起到了较好的教学效果，受到教师和学生的好评。

在这三年中，我们始终致力于包括专业建设、课程建设、师资建设、教材建设、实训基地建设、实验室建设和校企就业（创业）平台建设等在内的信息安全本科专业的全面建设。2005 年，作为组长单位我们完成了教育部“信息安全专业规范研究”和“信息安全学科专业发展战略研究”课题；召开了“全国高校本科‘信息安全专业规范与发展战略研究’成果发布与研讨会”。我们完成的国内第一次制定的信息安全专业规范，从知识领域、知识单元和知识点三个层次构建学科专业教学的知识体系；由通识教育内容、专业教育内容和综合教育内容三大部分，构建课程参考体系；采用顶层设计的方法构建了带有实践性环节的教学体系。我们在国内第一次较全面地提出信息安全学科专业教学改革与创新的研究以及发展思路和政策建议；这些成果已提交教育部相关教学指导委员会，对于引导高等学校信息安全学科专业教学改革与建设，指导信息安全学科专业评估，促进信息安全学科专业教学规范建设与管理，提高专业教育质量和水平起到了重要的作用。多所举办信息安全专业的高校都参照该课题成果调整了自己的教学计划、课程体系和实验方案。

我们积极搭建信息安全专业校际交流平台，组织成立了“全国信息安全本科教材编写委员会”和“全国信息安全本科专业师资交流与培训互助组”。主持召开了“全国信息安全专业教学经验交流和师资培训研讨会”和“全国信息安全专业实验室建设和实验课程教学经验交流研讨会”。在四川绵阳建设了占地 40 亩的全国信息安全专业本科生实习实训基地，接受了来自全国近 30 所高校的本科生进入该基地参加丰富多彩的实训。

我们努力建设精品课程，主办了“全国高校信息安全专业精品课程建设经验交流会议”，来自全国各地高校的专家齐聚北京邮电大学，介绍了精品课程建设的经验。我们组织建设了全国第一批信息安全实验室，并且编写出版了实验教材《信息安全实验指导》，我们的《现代密码学》课程已经被评为北京市精品课程，并在 2007 年度被评为“国家精品课程”。

经过灵创团队全体人员的共同努力，北京邮电大学信息安全本科专业被教育部评为

第二类优势特色专业。

三年多的时间过去了，无论信息安全的教育和产业都取得了丰硕的成果，随着信息安全向更高层次的发展，其趋势已经从基础的网络层建设开始向内容层建设过渡。为适应信息安全教育的发展需要，积极探索培养创新型高素质人才，我们按照制定的学科发展战略和专业规范的精神，结合近几年的教学实践，我们对这套信息安全专业本科系列教材进行了全面修订，并及时成立了灵创团队北京邮电大学数字内容研究中心。这次修订不仅对原来的系列教材在第1版的基础上进行修改和完善，还补充了信息安全最新的研究成果，使教材的内容更加翔实和新颖。同时，在原有的教材上又增加了一些新的课程教材，在新修订的系列教材中，目前有《信息安全概论》(第2版)、《现代密码学教程》、《网络安全》(第2版)、《信息安全管理》、《计算机病毒原理与防治》(第2版)、《数字版权管理》、《网络安全实验教程》、《信息安全专业科技英语》、《防火墙、入侵检测与VPN》、《对称密码学及其应用》、《信息安全导论》和《数字图像取证技术》等13本教材，今后随着信息安全专业教学的需要，还将不断地有新的教材补充到这个系列中来，使之更加完善和系统。目前，计划列入的相关教材还有：《入侵检测》(第2版)、《信息内容安全》、《信息安全工程》、《软件安全》和《信息安全标准与法律法规》等。

我们组织了强大的师资队伍，广泛吸收了有着丰富教学科研经验并多次讲授该系列教材的教师充实到这次修订工作中。作者队伍中不但包括北京邮电大学的教师，还包括哈尔滨工程大学、北京交通大学等重点院校的教师。经过反复研讨，本着理论与实际相结合的原则，对原来的系列教材进行了较大的修改和扩充，我们希望这套新修订的系列教材能够满足国内各类高校信息安全本科专业以及相关方向专业的不同需求。

这次修订对内容进行了精心的组织和安排，希望能促进信息安全课程的建设，涌现出更多的信息安全精品课程。虽然我们在这次修订中投入了很大精力，但是由于水平有限，时间仓促，且信息安全专业的发展速度非常快，书中的不足之处和错误在所难免，我们衷心期望使用和关心该系列教材的师生，继续对新的系列教材提出宝贵的意见和建议。

本套系列教材也是国家重点基础研究发展计划(973)(课题编号：2007CB310704和2007CB311203)资助的成果，并被教育部增补为“普通高等教育‘十一五’国家级规划教材”的选题。

在本系列教材的修订过程中，得到了北京邮电大学出版社的大力支持，同时也得到了灵创团队的骨干机构(北京邮电大学信息安全中心和北京邮电大学数字内容研究中心)300余位成员的支持与配合，在此一并表示感谢。

教授、博导、长江学者特聘教授

杨义先

2007年7月

前　言

随着计算机网络的广泛应用和深入发展，信息安全越来越受到社会各界的高度重视，已成为影响国家安全、经济发展、社会稳定的重要因素。由于信息安全技术的核心源于现代密码学，使得现代密码学成为信息科学技术领域的研究热点，越来越多的人渴望获得现代密码学的知识，从事现代密码学研究和应用的人不断增多。为了适应实际需求，各大院校纷纷以多种形式开设了“现代密码学”这门课，为我国信息安全人才培养和传播现代密码学知识方面发挥了重要作用。为了适应时代的需求，作者根据已有的公开书籍和资料，结合教学实践，编写了这本基础理论型的密码学著作。

北京邮电大学信息安全中心是专门从事信息安全教学、科研和成果转化的重点实验室，是我国民间最早从事现代密码学研究的群体之一，在“密码学”专业领域内健全了博士后、博士、硕士和本科的培养教育体系，在全国高校中属较早开设“现代密码学”课程的学校。2007 年，“现代密码学”课程成为北京市精品课程，之后又成为国家精品课程。

根据北京邮电大学信息安全中心对这门课十多年的教学经验，并在总结众多国内外密码学相关教材、专著及文献的基础之上，针对教师教学工作的需要和学生学习的特点编撰了本书。与同类教材相比，本书具有如下特点。

(1) 重点突出：现代密码学涉及的内容很多，本书紧紧围绕现代密码学的核心内容，从基本原理、设计思路、分析方法等多方面介绍这些内容。

(2) 通俗易懂：对于初学者，现代密码学的内容有点“深奥”和难以理解。为此，本书通过背景介绍、实际需求、生动类比等多种方法使读者容易入门并理解其知识内容。

(3) 例证丰富：现代密码学的知识理论性强、推理复杂，需要较强的抽象思维。为此，本书重点章节都提供了具体例子，这使得读者能够快速地掌握现代密码学的基本概念和技术。

(4) 习题多样：为了巩固读者每章所学内容，每章的最后部分都包含多种形式(如判断题、选择题、填空题、简答题等)的习题，这些习题涵盖了本章的知识要点。

本书由谷利泽主持编写，各章节内容主要基于谷利泽的“现代密码学”课程的教学讲义。参加本书初稿编写的主要人员有郎风华博士、李佳伦博士、李晖老师、杨榆老师、陈晨

硕士、陈波硕士等，在此表示诚挚的感谢。谷利泽对全书进行了统稿，郑世慧老师、孙艳宾博士、王锋博士认真地通读全书，并提出了许多修改建议，完成全书的最后审阅和校对工作，在此表示诚挚的感谢。在本书编写过程中，多次得到杨义先老师的关心和指导，书中的主要思路也是源于杨老师的启发，在此表示诚挚的感谢。

限于作者水平和经验不足，书中的错误和缺憾在所难免，诚恳地希望读者在使用本书时能够及时指出发现的错误和问题，作者将把有益的批评和建议作为今后本书修改的动力。另外，本书内容引用许多国内外书籍和文献并在书后的参考文献中列出，由于引用量较大，难免有疏漏，请发现者及时通知作者，作者将及时更正或发表声明。作者的 E-mail：glzisc@bupt.edu.cn。

作　者

目　　录

第 1 章　密码学概论

1.1　信息安全与密码学 …… 1
1.1.1　信息安全的重要性 …… 1
1.1.2　攻击的主要形式和分类 …… 2
1.1.3　信息安全的目标 …… 4
1.1.4　密码学在信息安全中的作用 …… 5
1.2　密码学发展史 …… 6
1.2.1　传统密码 …… 7
1.2.2　现代密码学 …… 10
1.3　密码学基础 …… 12
1.3.1　密码体制模型及相关概念 …… 13
1.3.2　密码体制的原则 …… 14
1.3.3　密码体制的分类 …… 14
1.3.4　密码体制的安全性 …… 16
1.3.5　密码体制的攻击 …… 17
1.4　习题 …… 19

第 2 章　传统密码体制

2.1　置换密码 …… 21
2.1.1　列置换密码 …… 22
2.1.2　周期置换密码 …… 23
2.2　代换密码 …… 24
2.2.1　单表代换密码 …… 24
2.2.2　多表代换密码 …… 26
2.2.3　转轮密码机 …… 31

2.3 传统密码的分析 …… 33
2.3.1 统计分析法 …… 34
2.3.2 明文-密文对分析法 …… 40
2.4 习题 …… 42

第 3 章 密码学基础

3.1 数论 …… 45
3.1.1 素数 …… 45
3.1.2 模运算 …… 46
3.1.3 欧几里得算法 …… 47
3.1.4 欧拉定理 …… 49
3.1.5 一次同余方程与中国剩余定理 …… 51
3.1.6 二次剩余和 Blum 整数 …… 53
3.1.7 勒让德和雅可比符号 …… 54
3.2 近世代数 …… 56
3.2.1 群 …… 56
3.2.2 环与域 …… 58
3.2.3 多项式环 …… 58
3.2.4 域上的多项式环 …… 60
3.2.5 有限域 …… 63
3.3 香农理论 …… 65
3.3.1 熵及其性质 …… 65
3.3.2 完全保密 …… 69
3.3.3 冗余度、唯一解距离与保密性 …… 72
3.3.4 乘积密码体制 …… 75
3.4 复杂度理论 …… 76
3.4.1 算法的复杂度 …… 76
3.4.2 问题的复杂度 …… 78
3.5 习题 …… 79

第 4 章 分组密码

4.1 分组密码概述 …… 82
4.1.1 分组密码简介 …… 82
4.1.2 理想分组密码 …… 84
4.1.3 分组密码的原理 …… 85

4.1.4 分组密码的设计准则 …… 88
4.2 数据加密标准(DES) …… 89
4.2.1 DES 的历史 …… 89
4.2.2 DES 的基本结构 …… 90
4.2.3 DES 的初始置换和逆初始置换 …… 92
4.2.4 DES 的 F 函数 …… 93
4.2.5 DES 的子密钥生成 …… 97
4.2.6 DES 的安全性 …… 98
4.2.7 三重 DES …… 101
4.2.8 DES 的分析方法 …… 103
4.3 AES 算法 …… 108
4.3.1 AES 的基本结构 …… 109
4.3.2 字节代换 …… 112
4.3.3 行移位 …… 116
4.3.4 列混合 …… 117
4.3.5 轮密钥加 …… 118
4.3.6 密钥扩展 …… 120
4.3.7 AES 的解密 …… 122
4.3.8 AES 的安全性和可用性 …… 124
4.3.9 AES 和 DES 的对比 …… 125
4.4 典型分组密码 …… 126
4.4.1 IDEA 算法 …… 126
4.4.2 RC6 算法 …… 129
4.4.3 Skipjack 算法 …… 131
4.4.4 Camellia 算法 …… 133
4.5 分组密码的工作模式 …… 137
4.5.1 电子密码本模式(ECB) …… 138
4.5.2 密码分组链接模式(CBC) …… 139
4.5.3 密码反馈模式(CFB) …… 141
4.5.4 输出反馈模式(OFB) …… 142
4.5.5 计数器模式(CTR) …… 143
4.6 习题 …… 145

第 5 章 序列密码

5.1 序列密码简介 …… 148

5.1.1 起源 …… 148
5.1.2 序列密码定义 …… 149
5.1.3 序列密码分类 …… 150
5.1.4 序列密码原理 …… 152
5.2 线性反馈移位寄存器 …… 153
5.2.1 移位寄存器 …… 153
5.2.2 线性反馈移位寄存器 …… 154
5.2.3 LFSR 周期分析 …… 156
5.2.4 伪随机性测试 …… 158
5.2.5 *m* 序列密码的破译 …… 159
5.2.6 带进位的反馈移位寄存器 …… 160
5.3 非线性序列 …… 162
5.3.1 Geffe 发生器 …… 163
5.3.2 *J-K* 触发器 …… 163
5.3.3 Pless 生成器 …… 164
5.3.4 钟控序列生成器 …… 165
5.3.5 门限发生器 …… 165
5.4 典型序列密码算法 …… 166
5.4.1 RC4 算法 …… 166
5.4.2 A5 算法 …… 169
5.4.3 SEAL 算法 …… 171
5.4.4 SNOW2.0 算法 …… 173
5.4.5 WAKE 算法 …… 175
5.4.6 PKZIP 算法 …… 176
5.5 习题 …… 178

第 6 章 Hash 函数和消息认证

6.1 Hash 函数 …… 180
6.1.1 Hash 函数的概念 …… 180
6.1.2 Hash 函数结构 …… 181
6.1.3 Hash 函数应用 …… 182
6.2 Hash 算法 …… 183
6.2.1 MD5 算法 …… 183
6.2.2 SHA1 算法 …… 189
6.2.3 SHA256 算法 …… 195

6.2.4 SHA512 算法 …… 198
6.3 消息认证 …… 204
6.3.1 消息认证码 …… 204
6.3.2 基于 DES 的消息认证码 …… 205
6.3.3 基于 Hash 的认证码 …… 206
6.4 Hash 函数的攻击 …… 208
6.4.1 生日悖论 …… 209
6.4.2 两个集合相交问题 …… 210
6.4.3 Hash 函数的攻击方法 …… 210
6.4.4 Hash 攻击新进展 …… 211
6.5 习题 …… 212

第 7 章 公钥密码体制

7.1 公钥密码体制概述 …… 215
7.1.1 公钥密码体制的提出 …… 215
7.1.2 公钥密码体制的思想 …… 216
7.1.3 公钥密码体制的分类 …… 217
7.2 RSA 公钥密码 …… 218
7.2.1 RSA 密钥对生成 …… 218
7.2.2 RSA 加解密算法 …… 218
7.2.3 RSA 公钥密码安全性 …… 221
7.3 ElGamal 公钥密码 …… 225
7.3.1 ElGamal 密钥对生成 …… 225
7.3.2 ElGamal 加解密算法 …… 225
7.3.3 ElGamal 公钥密码安全性 …… 227
7.4 椭圆曲线公钥密码 …… 229
7.4.1 椭圆曲线 …… 230
7.4.2 ECC 密钥对生成 …… 233
7.4.3 ECC 加解密算法 …… 234
7.4.4 ECC 安全性 …… 235
7.4.5 ECC 的优势 …… 236
7.5 其他公钥密码 …… 238
7.5.1 MH 背包公钥密码 …… 238
7.5.2 Rabin 公钥密码 …… 240
7.5.3 Goldwasser-Micali 概率公钥密码 …… 241

7.5.4 NTRU 公钥密码 …… 242
7.5.5 基于身份的公钥密码 …… 244
7.6 习题 …… 246

第 8 章 数字签名技术

8.1 数字签名概述 …… 249
8.1.1 数字签名简介 …… 249
8.1.2 数字签名原理 …… 251
8.2 数字签名的实现方案 …… 253
8.2.1 基于 RSA 的签名方案 …… 253
8.2.2 基于离散对数的签名方案 …… 254
8.2.3 基于椭圆曲线的签名方案 …… 262
8.3 特殊数字签名 …… 263
8.3.1 代理签名 …… 264
8.3.2 盲签名 …… 267
8.3.3 多重数字签名 …… 269
8.3.4 群签名 …… 273
8.3.5 不可否认签名 …… 275
8.3.6 其他数字签名 …… 276
8.4 习题 …… 280

第 9 章 密码协议

9.1 密码协议概述 …… 283
9.2 零知识证明 …… 285
9.2.1 Quisquater-Guillou 零知识协议 …… 286
9.2.2 Hamilton 零知识协议 …… 286
9.2.3 身份的零知识证明 …… 287
9.3 比特承诺 …… 290
9.3.1 基于对称密码算法的比特承诺方案 …… 291
9.3.2 基于单向函数的比特承诺方案 …… 291
9.3.3 Pedersen 比特承诺协议 …… 292
9.4 不经意传送协议 …… 293
9.4.1 Blum 不经意传送协议 …… 294
9.4.2 公平掷币协议 …… 295
9.5 安全多方计算 …… 297

9.5.1 百万富翁问题 …… 298
9.5.2 平均薪水问题 …… 300
9.6 电子商务中密码协议 …… 302
9.6.1 电子货币 …… 302
9.6.2 电子投票 …… 307
9.6.3 电子拍卖 …… 311
9.7 习题 …… 316

第 10 章 密钥管理

10.1 密钥管理概述 …… 319
10.1.1 密钥管理的层次结构 …… 320
10.1.2 密钥管理的原则 …… 322
10.2 密钥生命周期 …… 323
10.3 密钥分发技术 …… 326
10.3.1 公开密钥的分发 …… 326
10.3.2 秘密密钥分发模式 …… 328
10.4 密钥协商技术 …… 331
10.4.1 Diffie-Hellman 密钥交换协议 …… 331
10.4.2 中间人攻击 …… 332
10.4.3 端-端协议 …… 332
10.5 密钥托管技术 …… 333
10.5.1 密钥托管简介 …… 333
10.5.2 密钥托管主要技术 …… 334
10.6 秘密共享技术 …… 337
10.6.1 Shamir 门限方案 …… 338
10.6.2 Asmuth-Bloom 门限方案 …… 341
10.7 习题 …… 343

第 11 章 密码学新进展

11.1 量子密码学 …… 346
11.1.1 量子密码学的物理学基础 …… 346
11.1.2 量子密码信息理论 …… 347
11.1.3 量子密码的实现 …… 347
11.1.4 量子密码的应用 …… 348
11.1.5 量子密码面临的问题 …… 350

11.2 混沌密码学 …… 351
11.2.1 混沌学的历史发展与现状 …… 351
11.2.2 混沌学基本原理 …… 352
11.2.3 混沌密码学原理 …… 353
11.2.4 混沌密码目前存在的主要问题 …… 354
11.3 DNA 密码 …… 355
11.3.1 背景与问题的提出 …… 355
11.3.2 相关生物学背景 …… 356
11.3.3 DNA 计算与密码学 …… 357
11.3.4 DNA 密码 …… 358
11.3.5 DNA 密码安全性分析 …… 359
11.3.6 DNA 计算及 DNA 密码所遇到的问题 …… 360
11.4 习题 …… 361

参考文献 …… 363

第1章

密码学概论

密码学(Cryptology)是结合数学、计算机科学、电子与通信等诸多学科于一体的交叉学科，是研究信息系统安全保密的一门科学，它分为密码编码学和密码分析学两类。本章首先介绍密码学与信息安全的关系，然后简述密码学发展史，最后介绍密码学中的一些基本知识。

1.1 信息安全与密码学

因特网的飞速发展和普及应用加速了信息社会的节奏与步伐，信息作为一种无形的资源，已经成为促进经济增长和社会进步的重要力量。现在，信息系统已被广泛地应用于政治、军事、经济和科研等诸多领域，并逐渐成为一种很重要的工具和手段。但事物都具有两重性，当我们尽情享受信息社会带来的诸多便利和高效的同时，也需要防范它带来的负面影响。信息网络的社会性、开放性和共享性等特点使其蒙上了不安全因素的阴影。由于信息的存储、传递、处理等过程往往是在开放的通信网络中进行的，使信息容易受到窃听、截取、篡改、伪造、假冒、重放等多种攻击手段的威胁。如果信息安全问题不解决，信息社会就不能稳步有序地发展，电子商务、电子政务、网络银行等应用都将无法开展起来。因此，信息安全已经成为信息社会亟须解决的最重要问题之一。

信息安全是一门综合的学科，它涉及信息论、计算机科学和密码学等多方面知识，其主要任务是研究计算机系统和通信网络中信息的保护方法，以及实现系统内信息的机密性、完整性、可用性、不可否认性和认证性等，其中密码学正是实现这些功能的核心技术。

1.1.1 信息安全的重要性

随着以 Internet 为代表的全球性信息化浪潮日益高涨，计算机以及信息网络技术的