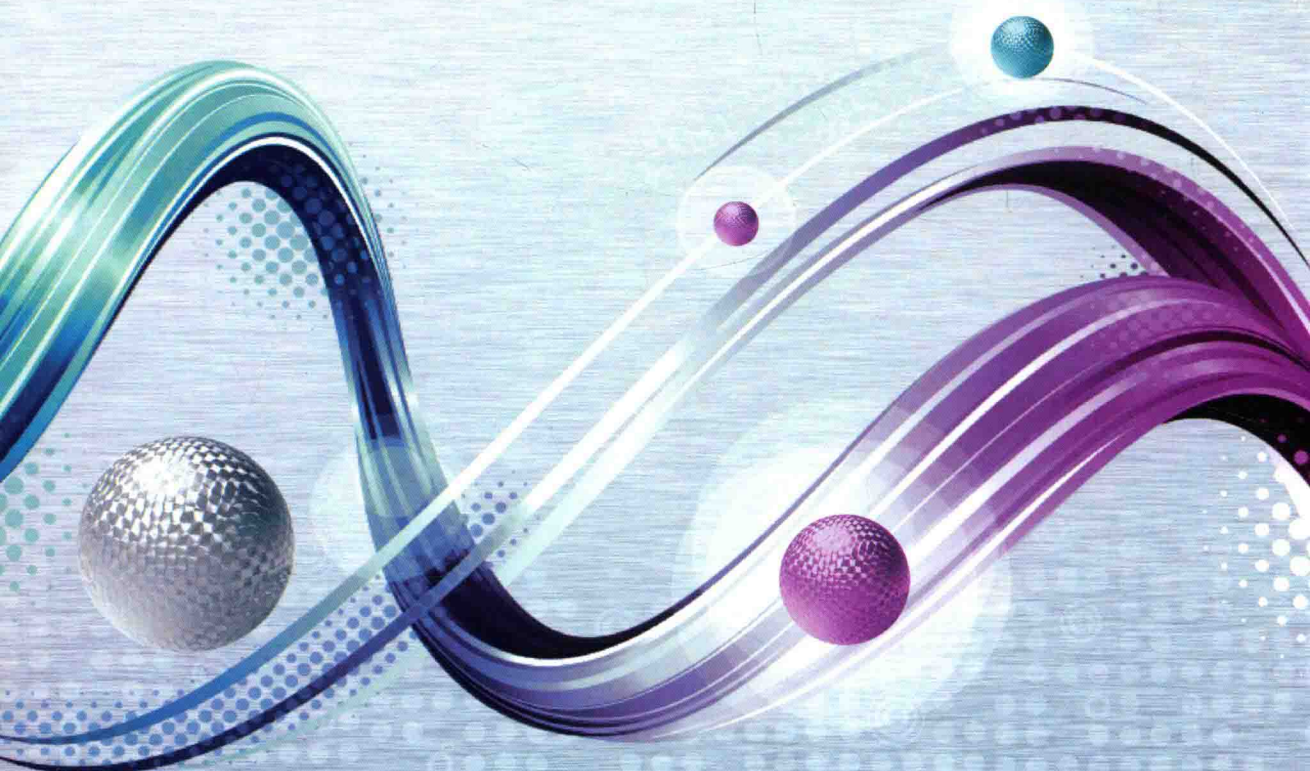
省级精品资源共享课配套教材

高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材

应用密码学

（卓越工程师计划）

张仕斌　万武南　张金全　编著



西安电子科技大学出版社
http://www.xduph.com

高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材

省级精品资源
共享课配套教材

应用密码学

（卓越工程师计划）

张仕斌　万武南　张金全　编著

西安电子科技大学出版社

内 容 简 介

本书是在作者多年前已出版的教材的基础上，结合近年来作者所在单位实施“卓越工程师教育培养计划”的成果和作者在教学与科研方面的实践经验，以工程技术为主线，面向应用实践而编写的一本应用密码学教材。本书在全面讲述密码算法基本理论内在规律和基本原理的同时，注重密码算法的应用，通过多个实用案例全面剖析了现代密码算法的原理，阐述了部分算法的安全性及密码学发展的新方向。本书还介绍了一些典型密码算法的应用案例，并给出密码学课程设计，使学生将所学密码学知识与应用实践结合起来。每章后都配有相应的习题以实现教与学的统一，也可让学生边学习边实践，最终“知其所以然”。

全书共13章，主要内容包括密码学基础知识、古典密码、对称密码、序列密码、非对称密码、Hash函数、数字签名、身份认证技术、密钥管理技术、信息隐藏技术、密码学发展的新方向、密码学的应用等；书后的知识拓展部分为应用密码学课程设计内容。书中标星号的为选修内容，读者可根据需要自行选择。本书既可作为普通高等院校信息安全、信息对抗技术、密码学、应用数学、通信工程、计算机、电子商务等相关专业本科生和研究生的教材，也可作为网络和信息系统安全相关设计、研发技术人员的参考书。

图书在版编目(CIP)数据

应用密码学/张仕斌，万武南，张金全编著.
—西安：西安电子科技大学出版社，2017.1
高等学校电子信息类“十三五”规划教材
ISBN 978-7-5606-4248-2

Ⅰ.① 应… Ⅱ.① 张… ② 万… ③ 张… Ⅲ.① 密码学
—高等学校—教材 Ⅳ.① TN918.1

中国版本图书馆CIP数据核字(2016)第256505号

策划编辑 李惠萍
责任编辑 宁晓蓉
出版发行 西安电子科技大学出版社(西安市太白南路2号)
电 话 (029)88242885 88201467 邮 编 710071
网 址 www.xduph.com 电子邮箱 xdupfxb001@163.com
经 销 新华书店
印刷单位 陕西华沐印刷科技有限责任公司
版 次 2017年1月第1版 2017年1月第1次印刷
开 本 787毫米×1092毫米 1/16 印张 24.875
字 数 587千字
印 数 1～3000册
定 价 46.00元
ISBN 978-7-5606-4248-2/TN

XDUP 4540001-1

序

进入21世纪以来，信息技术迅速改变着人们传统的生产和生活方式，社会的信息化已经成为当今世界发展不可逆转的趋势和潮流。信息作为一种重要的战略资源，与物资、能源、人力一起已被视为现代社会生产力的主要因素。目前，世界各国围绕着信息获取、利用和控制的国际竞争日趋激烈，网络与信息安全问题已成为一个世纪性、全球性的课题。党的十八大报告明确指出，要“高度关注海洋、太空、网络空间安全”。党的十八届三中全会决定设立国家安全委员会，成立中央网络安全和信息化领导小组，并把网络与信息安全列入了国家发展的最高战略方向之一。这为包含网络空间安全在内的非传统安全领域问题的有效治理提供了重要的体制机制保障，是我国国家安全体制机制的一个重大创新性举措，彰显了我国政府治国理政的战略新思维和“大安全观”。

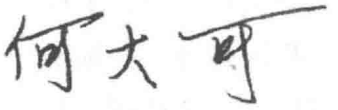
人才资源是确保我国网络与信息安全第一位的资源，信息安全人才培养是国家信息安全保障体系建设的基础和必备条件。随着我国信息化和信息安全产业的快速发展，社会对信息安全人才的需求不断增加。2015年6月11日，国务院学位委员会和教育部联合发出“学位[2015]11号”通知，决定在“工学”门类下增设“网络空间安全”一级学科，代码为“0839”，授予工学学位。这是国家推进专业化教育，在信息安全领域掌握自主权、抢占先机的重要举措。

建国以来，我国高等工科院校一直是培养各类高级应用型专门人才的主力军，培养网络与信息安全高级应用型专门人才，高等院校同样责无旁贷。目前，许多高等院校和科研院所已经开办了信息安全专业或开设了相关课程。作为国家首批61所“卓越工程师教育培养计划”试点院校之一，成都信息工程大学以《国家中长期教育改革和发展规划纲要(2010—2020年)》、《国家中长期人才发展规划纲要(2010—2020年)》、《卓越工程师教育培养计划通用标准》为指导，以专业建设和工程技术为主线，始终贯彻“面向工业界、面向未来、面向世界”的工程教育理念，按照“育人为本、崇尚应用”、“一切为了学生”的教学教育理念和“夯实基础、强化实践、注重创新、突出特色”的人才培养思路，遵循“行业指导、校企合

作、分类实施、形式多样”的原则，实施了一系列教育教学改革。令人欣喜的是，该校信息安全工程学院与西安电子科技大学出版社近期联合组织了一系列网络与信息安全专业教育教学改革的研讨活动，共同研讨培养应用型高级网络与信息安全工程技术人才的教育教学方法和课程体系，并在总结近年来该校信息安全专业实施“卓越工程师教育培养计划”教育教学改革成果和经验的基础上，组织编写了“应用型网络与信息安全工程技术人才培养系列教材”。本套教材总结了该校信息安全专业教育教学改革成果和经验，相关课程有配套的课程过程化考核系统，是培养应用型网络与信息安全工程技术人才的一套比较完整、实用的教材，相信可以对我国高等院校网络与信息安全专业的建设起到很好的促进作用。本套教材为中国电子教育学会高教分会推荐教材。

信息安全是相对的，信息安全领域的对抗永无止境。国家对信息安全人才的需求是长期的、旺盛的。衷心希望本套教材在培养我国合格的应用型网络与信息安全工程技术人才的过程中取得成功并不断完善，为我国信息安全事业做出自己的贡献。

高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材
名誉主编（中国密码学会常务理事）



二〇一五年十月

中国电子教育学会高教分会推荐
高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材
编审专家委员会名单

前　言

随着目前我国经济建设和信息化进程的全面加快，网络与信息系统的基础性、全面性作用日益增强，信息安全已成为国家安全的重要组成部分。党的十八大明确指出要“高度关注海洋、太空、网络空间安全”。因此，加快国家信息安全保障体系建设，确保我国的信息安全，已经成为我国的国家战略。人才资源是确保我国信息安全第一位的资源，信息安全人才培养是国家信息安全保障体系建设的基础和必备条件。密码学作为信息安全的核心技术和基石，在保障信息安全的应用中具有重要作用和意义，而对现代密码算法的掌握又是快速保障信息安全的重要途径。

一直以来，我国高等工科院校都是培养各类高级应用型专门人才的主力军，培养信息安全高级应用型专门人才，高等院校同样责无旁贷。2009 年 10 月，按照培养信息安全高级应用型专门人才的目标，我们编写了《应用密码学》一书(2009 年 12 月，西安电子科技大学出版社出版)，6 年多来，我们始终围绕着“以提高教学质量为核心”，深入开展“应用密码学”课程教育教学的一体化改革，在课程培养目标、培养标准、教学方法、教学体系、教学内容和课程过程考试评价机制等方面进行了大胆的尝试，取得了明显的成效。2010 年，“应用密码学”课程被评为四川省精品课程；2011 年，《应用密码学》教材被列入四川省“十二五”普通高等教育本科规划教材；2014 年，“应用密码学”课程被评为四川省精品资源共享课程。

这次重新编写的《应用密码学》一书是在保持第一版教材原有特色的基础上，按照《国家中长期教育改革和发展规划纲要(2010—2020 年)》、《国家中长期人才发展规划纲要(2010—2020 年)》、《卓越工程师教育培养计划通用标准》的要求，结合近年来作者所在单位实施“卓越工程师教育培养计划”的成果和多年来作者在教学与科研方面的实践经验，按照“育人为本、崇尚应用”、“一切为了学生”的教学教育理念和“夯实基础、强化实践、注重创新、突出特色”的人才培养思路，遵循“行业指导、校企合作、分类实施、形式多样”的原则，以工程技术为主线，为实施教育教学改革，使密码学面向应用实践，为高等院校信息安全、信息对抗技术、密码学、应用数学、通信工程、计算机、电子商务等相关专业本科生和研究生编写的一本应用密码学教材。在本教材的编写中，始终围绕着这样一个目标：为信息安全领域提供一本既可以作为教学用书，也可作为网络和信息系统安全相关设计、研究开发和工程技术人员自学与参考书的实用教材。

本书的编排从教学适用性出发，特别重视读者对密码学知识的系统理解、应用和有针对性地重点掌握，在体系结构、语言表达、内容选取和举例及应用等方面都做了特别的考虑，因此本书也非常适合自学。

本书内容除了与作者自身的研究内容相关以外，还参考了国内外大量的书籍及 Internet 上公布的相关资料，对此都尽量在参考文献中列出。但由于网上资料数量众多且杂乱，可能无法对所有文献一一注明出处。这些资料大多来源于众多大学、研究机构、商业公司及一些研究网络安全技术的个人，他们为推动网络安全技术的发展做出了贡献，在此表示衷心的感谢。作者写作过程中参考的这些资料，其原文版权属于原作者，特此声明。

本书由张仕斌教授组织编写并进行统稿，其中第 1 章、第 2 章、第 5 章、第 9 章、第 10 章、第 11 章和第 12 章由张仕斌老师编写，第 3 章、第 6 章、第 8 章和知识拓展(应用密码学课程设计)由张金全老师编写，第 4 章、第 7 章和第 13 章由万武南老师编写。

本书的编写还得到了成都信息工程大学、西安电子科技大学出版社和相关高等院校同仁的大力支持与热情帮助，在此一并致以诚挚的谢意。

为了便于多媒体教学，本书配有电子教案(PPT)，订购本书的教师可到西安电子科技大学出版社网站(http://www.xduph.com)下载。

由于现代密码技术及应用发展迅速，而作者水平有限，加上时间仓促，书中难免有不足之处，恳请读者提出宝贵意见，以便进一步修改完善。

编　者

2016 年 3 月于成都

目　录

第 1 章　绪论 …… 1

1.1　信息安全概述 …… 1

1.1.1　信息安全的基本概念 …… 1

1.1.2　信息安全问题的根源 …… 2

1.1.3　信息安全机制与信息安全服务 …… 4

1.1.4　信息安全模型 …… 5

1.1.5　安全性攻击的主要形式 …… 7

1.2　密码学在信息安全中的作用及发展历程 …… 8

1.2.1　密码学在信息安全中的作用 …… 8

1.2.2　密码学的发展历程 …… 9

1.3　密码学的基本知识 …… 10

1.3.1　密码学的基本概念 …… 10

1.3.2　保密通信模型 …… 11

1.3.3　密码体制的构成及其分类 …… 13

1.3.4　密码学的应用范围 …… 15

1.4　密码体制的安全性 …… 16

1.4.1　密码分析 …… 16

1.4.2　密码体制的安全性及安全条件 …… 17

习题 1 …… 19

第 2 章　古典密码体制 …… 20

2.1　古典密码概述 …… 20

2.2　传统隐写术 …… 20

2.3　替换密码技术 …… 21

2.3.1　单字符单表替换密码技术 …… 21

2.3.2　单字符多表替换密码技术 …… 23

2.4　换位密码技术 …… 27

2.4.1　列换位 …… 27

2.4.2　周期换位 …… 28

2.5　古典密码体制的安全性分析 …… 28

2.5.1　移位密码安全性分析 …… 28

2.5.2　仿射密码安全性分析 …… 29

习题 2 …… 29

第 3 章　密码学的数学基础 …… 31

3.1　初等数论 …… 31

3.1.1　素数 …… 31

3.1.2　最大公因数 …… 32

3.1.3　最小公倍数 …… 33

3.1.4　欧几里德算法 …… 34

3.1.5　模运算 …… 37

3.1.6　费马小定理和欧拉定理 …… 39

3.1.7　离散对数 …… 40

3.1.8　模重复平方计算法 …… 42

3.1.9　Miller-Rabin 素性检测算法 …… 43

3.2　群 …… 44

3.3　有限域 …… 45

3.3.1　有限域的定义 …… 45

3.3.2　域上的一元多项式 …… 46

3.3.3　域上一元多项式的运算规则 …… 46

3.3.4　一元多项式的整除 …… 47

3.3.5　域上一元多项式的带余除法 …… 48

3.3.6　多项式的公因式 …… 48

3.3.7　不可约多项式 …… 49

3.3.8　多项式同余 …… 50

3.3.9　一种构造有限域的方法 …… 50

3.4　椭圆曲线 …… 51

3.4.1　域 F_p 上的椭圆曲线 …… 52

3.4.2　域 F_{2^m} 上的椭圆曲线 …… 55

3.5　单向函数与单向限门函数 …… 58

3.6　密码学的复杂性理论概述 …… 59

习题 3 …… 60

第 4 章　分组密码体制 …… 61

4.1　分组密码的基本概念 …… 61

4.1.1　分组密码概述 …… 61

4.1.2　分组密码的基本设计原则 …… 63

4.2　分组密码的原理 …… 64

4.2.1　代替-置换网络(S-P 结构) …… 64

4.2.2 Feistel 密码结构 …… 65
4.3 数据加密标准(DES) …… 68
4.3.1 DES 算法概述 …… 68
4.3.2 DES 算法描述 …… 68
4.3.3 DES 的各种变形算法 …… 80
4.4 高级加密标准(AES) …… 83
4.4.1 AES 算法描述 …… 83
4.4.2 基本运算 …… 85
4.4.3 基本变换 …… 88
4.4.4 密钥扩展 …… 94
4.4.5 解密过程 …… 96
4.4.6 具体实例 …… 99
4.5 SM4 加密算法 …… 101
4.5.1 SM4 描述 …… 101
4.5.2 算法流程 …… 103
4.5.3 密钥扩展算法 …… 104
4.5.4 具体实例 …… 106
4.6 其他典型的分组密码体制简介 …… 106
4.6.1 国际数据加密算法(IDEA) …… 106
4.6.2 RC6 对称密码体制 …… 110
4.6.3 Twofish 对称密码体制 …… 112
4.7 分组密码的工作模式 …… 113
4.7.1 ECB(电子码本)模式 …… 113
4.7.2 CBC(密码分组链接)模式 …… 114
4.7.3 CFB(密码反馈)模式 …… 116
4.7.4 OFB(输出反馈)模式 …… 117
4.7.5 CTR(计数器)模式 …… 119
4.7.6 分组密码尾分组处理 …… 121
4.8 分组密码算法的安全性分析 …… 122
4.8.1 分组密码算法的分析方法 …… 122
4.8.2 差分分析 …… 124
习题 4 …… 126
第 5 章 序列密码体制 …… 128
5.1 密码学中的随机数 …… 128
5.1.1 随机数及其性质 …… 129
5.1.2 随机数的生成方法 …… 129
5.1.3 伪随机数产生器* …… 130
5.1.4 伪随机数的评价标准 …… 132
5.2 序列密码的基本原理 …… 132
5.2.1 序列密码体制的概念 …… 132
5.2.2 序列密码体制的分类 …… 133
5.2.3 分组密码与序列密码的比较 …… 135
5.3 线性反馈移位寄存器及密钥序列的伪随机性 …… 135
5.3.1 线性反馈移位寄存器 …… 135
5.3.2 密钥序列的伪随机性* …… 137
5.4 非线性反馈移位寄存器 …… 140
5.5 序列密码算法的破译* …… 142
5.6 常用的序列密码算法 …… 144
5.6.1 A5 序列密码算法* …… 144
5.6.2 SEAL 序列密码算法* …… 145
5.6.3 RC4 序列密码算法 …… 147
习题 5 …… 148
第 6 章 非对称密码体制 …… 149
6.1 非对称密码体制概述 …… 149
6.1.1 非对称密码体制的原理 …… 150
6.1.2 非对称密码体制的设计准则 …… 151
6.1.3 非对称密码体制的分类 …… 152
6.2 RSA 密码算法 …… 153
6.2.1 RSA 发展简史 …… 153
6.2.2 RSA 算法描述 …… 153
6.2.3 RSA 算法举例 …… 155
6.2.4 RSA 算法的安全性及常用攻击 …… 155
6.2.5 RSA 算法的实现 …… 158
6.3 ElGamal 密码算法 …… 159
6.3.1 ElGamal 算法描述 …… 159
6.3.2 ElGamal 算法举例 …… 160
6.3.3 ElGamal 算法的安全性及常用攻击方法 …… 160
6.4 椭圆曲线密码体制 …… 162
6.4.1 椭圆曲线密码体制简介 …… 162
6.4.2 椭圆曲线上的 ElGamal 密码体制 … 162
6.4.3 椭圆曲线 Menezes-Vanstone 加密算法* …… 163
6.4.4 SM2 椭圆曲线公钥加密算法 …… 165
6.4.5 椭圆曲线密码体制的安全性 …… 166
6.5 RSA、ElGamal 及椭圆曲线密码算法比较 …… 166
6.6 其他非对称密码体制简介 …… 167
习题 6 …… 168

第 7 章　认证理论与技术——Hash 函数 …… 169
7.1　认证与认证系统 …… 169
7.2　Hash 函数概述 …… 170
7.2.1　Hash 函数的概念及结构 …… 170
7.2.2　Hash 函数的发展现状 …… 172
7.3　Hash 函数算法 …… 174
7.3.1　SHA-1 算法 …… 174
7.3.2　SHA-256、SHA-384 和 SHA-512* 算法 …… 179
7.3.3　SHA-3 算法 …… 186
7.3.4　MD5 算法 …… 196
7.4　Hash 算法的攻击现状分析 …… 201
7.4.1　生日悖论问题 …… 201
7.4.2　生日攻击 …… 202
7.5　消息认证 …… 204
7.5.1　消息认证的基本概念 …… 204
7.5.2　HMAC …… 207
7.5.3　消息认证码的应用 …… 210
习题 7 …… 211
第 8 章　认证理论与技术——数字签名 … 213
8.1　数字签名概述 …… 213
8.2　数字签名的原理及分类 …… 214
8.2.1　数字签名的原理 …… 214
8.2.2　数字签名的分类 …… 215
8.3　典型的数字签名方案 …… 216
8.3.1　RSA 数字签名方案 …… 216
8.3.2　ElGamal 数字签名方案 …… 218
8.4　数字签名标准* …… 219
8.4.1　基于离散对数的美国数字签名标准 …… 219
8.4.2　基于椭圆曲线的美国数字签名标准 …… 220
8.4.3　基于离散对数的俄罗斯数字签名标准 …… 222
8.4.4　基于椭圆曲线的俄罗斯数字签名标准 …… 223
8.4.5　我国的数字签名标准 …… 223
8.5　专用数字签名方案及应用* …… 225
8.5.1　盲签名方案 …… 225
8.5.2　不可否认的签名方案 …… 228
8.5.3　群签名方案 …… 230
8.5.4　代理签名方案 …… 232
8.5.5　其他专用数字签名方案 …… 233
习题 8 …… 234
第 9 章　认证理论与技术——身份认证技术 …… 235
9.1　认证模型及认证协议 …… 235
9.1.1　认证及认证模型 …… 235
9.1.2　认证协议 …… 236
9.2　身份认证技术 …… 238
9.2.1　口令认证技术 …… 238
9.2.2　IC 卡认证技术 …… 242
9.2.3　个人特征识别技术 …… 246
9.3　基于零知识证明的身份认证技术 …… 247
9.3.1　零知识证明的基本概念 …… 247
9.3.2　基于零知识的身份认证技术 …… 250
9.4　几种典型的身份认证方案* …… 252
9.4.1　Schnorr 身份认证方案 …… 253
9.4.2　Okamoto 身份认证方案 …… 254
9.4.3　Guillou-Quisguater 身份认证方案 …… 255
9.4.4　基于身份的身份认证方案 …… 256
9.5　Kerberos 身份认证技术* …… 257
9.5.1　Kerberos 身份认证技术简介 …… 257
9.5.2　Kerberos 的工作原理 …… 258
9.5.3　Kerberos 域间的认证 …… 261
9.6　X.509 认证技术* …… 261
9.6.1　数字证书 …… 262
9.6.2　X.509 证书的格式及管理 …… 263
9.6.3　X.509 认证过程 …… 265
习题 9 …… 266
第 10 章　密钥管理技术 …… 268
10.1　密钥管理概述 …… 268
10.2　密钥的组织结构及分类 …… 269
10.2.1　密钥的组织结构 …… 269
10.2.2　密钥的分类 …… 270
10.3　密钥管理的内容 …… 271
10.4　密钥托管技术 …… 273

10.4.1 密钥托管技术简介 …… 273
10.4.2 密钥托管系统的组成 …… 275
10.5 密钥协商与密钥分配 …… 277
10.5.1 密钥协商 …… 277
10.5.2 秘密共享 …… 282
10.5.3 密钥分配技术 …… 286
10.6 PKI 技术* …… 291
10.6.1 概述 …… 291
10.6.2 PKI 的目标及研究的主要内容 …… 293
10.6.3 PKI 的基本组成 …… 293
10.6.4 PKI 的主要功能 …… 296
10.6.5 PKI 的优势及应用 …… 299
习题 10 …… 301

第 11 章 信息隐藏技术 …… 302
11.1 信息隐藏概述 …… 302
11.2 信息隐藏的原理及应用 …… 303
11.2.1 信息隐藏的原理 …… 303
11.2.2 信息隐藏的分类 …… 304
11.2.3 信息隐藏的应用 …… 306
11.3 信息隐藏的基本算法 …… 308
11.3.1 基于空域的信息隐藏算法 …… 308
11.3.2 基于变换域的信息隐藏算法 …… 312
11.4 数字水印技术 …… 315
11.4.1 数字水印的基本原理 …… 315
11.4.2 数字水印的分类 …… 316
11.4.3 数字水印的应用 …… 318
11.4.4 数字水印的常用算法 …… 319
习题 11 …… 320

第 12 章 密码学发展的新方向 …… 321
12.1 量子密码学* …… 321
12.1.1 量子密码学简介 …… 321
12.1.2 量子密码学原理 …… 323
12.1.3 量子密钥分配协议 …… 325
12.1.4 量子密码学面临的挑战及未来发展趋势 …… 327
12.2 基于混沌理论的密码体制* …… 329
12.2.1 混沌理论的基本概念 …… 329
12.2.2 混沌序列的产生及其随机序列 …… 330
12.2.3 混沌密码体制 …… 331
12.2.4 混沌密码的应用实例 …… 332
12.3 其他新密码体制简介* …… 333
习题 12 …… 335

第 13 章 密码学的应用 …… 336
13.1 密码学在电子邮件中的应用* …… 336
13.1.1 电子邮件概述 …… 336
13.1.2 PGP 及其使用 …… 340
13.2 密码学在电子商务中的应用 …… 342
13.2.1 电子商务系统面临的安全威胁 …… 343
13.2.2 电子商务系统安全需求 …… 343
13.2.3 电子商务的安全体系结构 …… 344
13.2.4 电子商务的交易协议 …… 346
13.3 密码学在数字通信中的应用 …… 352
13.3.1 数字保密通信概述 …… 352
13.3.2 第四代移动通信系统(4G)的安全性 …… 352
13.3.3 WiMAX 无线网域的安全性 …… 360
13.3.4 VPN 与 IPSec …… 362
13.4 密码学在图像加密中的应用* …… 367
13.4.1 图像加密概述 …… 367
13.4.2 图像加密的实现 …… 368
13.4.3 实现效果及分析 …… 369
13.5 密码学在 RFID 中的应用* …… 370
13.5.1 RFID 概述 …… 370
13.5.2 RFID 的安全性 …… 371
习题 13 …… 376

知识拓展 应用密码学课程设计 …… 377

参考文献 …… 384

第1章 绪 论

知识点

- ★ 信息安全的基本概念及问题的根源
- ★ 信息安全机制与信息安全服务
- ★ 信息安全模型及安全性攻击的主要形式
- ★ 密码学在信息安全中的作用及发展历程
- ★ 密码学的基本知识
- ★ 密码体制的安全性

本章导读

本章首先介绍信息安全的基本概念及基本属性、信息安全问题的根源、信息安全机制与信息安全服务、信息安全模型和安全性攻击的主要形式；接着介绍密码学在信息安全中的作用、密码学的发展历程；然后介绍密码学的基本概念、保密通信模型、密码体制的构成及其分类和密码学的应用范围；最后介绍密码分析及方法和密码体制的安全性。通过对本章的学习，使读者对信息安全和密码学的基本知识及它们间的关系有一个初步了解，对读者按计划学好本书后续知识具有重要的指导作用。

1.1 信息安全概述

信息是信息化社会发展的重要战略资源，也是衡量一个国家综合国力的重要指标之一。信息的普遍性、共享性、增值性、可处理性和多效用性，使其对于人类具有特别重要的意义。在信息时代，任何一个国家的政治、军事和外交等都离不开信息，经济建设、科学的发展和技术的进步也离不开信息。对信息的开发、控制和利用已成为国家间利益争夺的重要内容。当前，随着网络信息技术的迅猛发展，信息的地位与作用仍然在急剧上升，信息安全问题因此而日益突出。未来的军事斗争将首先在信息领域展开，并全程贯穿着信息战，信息安全将成为赢得战争胜利的重要保障。“没有网络安全就没有国家安全，没有信息化就没有现代化”，特别是在当前我国信息化建设已进入高速发展的阶段，电子政务、电子商务、网络金融、网络媒体等蓬勃发展，这些与国民经济、社会稳定发展息息相关的领域急需信息安全保障。因此，加强信息安全技术研究，提高信息安全的应用水平，在信息系统应用领域营造信息安全氛围，既是时代发展的客观要求，也是未来信息技术发展的迫切需要。

1.1.1 信息安全的基本概念

1. 信息安全的定义

到目前为止，“安全”并没有统一的定义，但其基本含义可以理解为：客观上不存在威胁，

主观上不存在恐惧。“信息安全”同样也没有公认和统一的定义，但国内外对信息安全的论述大致可分为两大类：一类是指具体的信息系统的安全；而另一类则是指某一特定信息体系结构(比如一个国家的金融系统、军事指挥系统)的安全。但一些专家认为这两种定义均很片面，所涉及的内容过窄。我们认为，信息安全是指信息网络的硬件、软件及系统中的数据受到保护，不受偶然或者恶意原因的影响而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，信息服务不中断。

2. 信息安全的基本属性

(1) 真实性(Authenticity)：确认和识别一个主体或资源就是其所声称的，被认证的对象可以是用户、进程、系统和信息等。

(2) 保密性(Confidentiality)：指信息不泄露给非授权的个人、实体和进程，或不能供其使用的特性。

(3) 完整性(Integrity)：指信息未经授权不被修改、不被破坏、不被插入、不延迟、不乱序和不丢失的特性。对网络信息安全进行攻击其最终目的就是破坏信息的完整性。

(4) 可用性(Availability)：指合法用户访问并能按要求顺序使用信息的特性，即保证合法用户在需要时可以访问到所需信息及相关资源。对可用性的攻击就是阻断信息的可用性，如破坏网络和有关系统的正常运行就属于这类攻击。

(5) 可控性(Controlability)：指授权机构对信息的内容及传播具有控制能力的特性，可以控制授权范围内的信息流向以及信息传播方式。

(6) 可审查性(Auditability)：指在信息交流过程结束后，通信双方不能抵赖曾经做出的行为，也不能否认曾经接收到对方的信息。

(7) 可靠性(Reliability)：指信息以用户认可的质量连续服务于用户的特性(包括信息准确、迅速和连续地传输、转移等)，但也有一些专家认为可靠性是人们对信息系统而不是对信息本身的要求。

安全总是相对的，没有绝对的安全，追求信息安全是永无止境的。信息安全的实质就是指采用一切可能的方法和手段，保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全，确保信息具有上述“七性”。在实际应用中，信息安全问题的关键是安全保护的成本和效益，如果安全保护的成本低于受保护信息的价值，并且破解安全保护的代价超过信息的价值，就可以认为是相对安全的。

1.1.2 信息安全问题的根源

当今的信息安全问题，已经不再像以前那样仅简单地谈计算机病毒，信息安全的防御也不再是仅安装了病毒软件和防火墙就能达到目的，这是因为信息系统所面临的安全威胁正随着信息技术的广泛应用在不断增加。产生信息安全问题的根源可以从两方面来进行分析：一是我们使用的个人终端所面临的安全威胁；二是网络系统所面临的威胁。

1. 个人终端所面临的主要安全威胁

随着信息技术及应用的飞速发展，个人终端(包括个人计算机、笔记本电脑、平板电脑、智能手机、PDA 等)也得到了广泛普及，个人终端也成为了黑客攻击的目标之一，就其安全威胁而言，主要涉及以下几个方面。

(1) 普通计算机病毒：是当前最常见、最主要的威胁，几乎每天都有计算机病毒产生。计算机病毒的主要危害体现在破坏计算机文件(如.com、.exe、.doc、.pdf文件等)和数据，导致文件无法使用，系统无法启动；消耗计算机 CPU、内存和磁盘资源，导致一些正常服务无法进行，出现死机，占用大量的磁盘空间；有的还会破坏计算机硬件，导致计算机彻底瘫痪。

(2) 木马：是一种基于远程控制的黑客工具，使远程计算机能够通过网络控制用户个人终端，并且可能造成用户信息损失、系统瘫痪甚至损坏。木马作为一种远程控制的黑客工具，主要危害包括窃取用户信息(比如计算机或网络账户和密码、网络银行账户和密码、QQ 账户和密码、E-mail 账户和密码等)，携带计算机病毒(造成计算机或网络不能正常运行，甚至完全瘫痪)，或被黑客控制，攻击用户计算机或网络。

(3) 恶意软件：是指一类特殊的程序，是介于普通计算机病毒与黑客软件之间的软件的统称。它通常在用户不知晓也未授权的情况下潜入系统，具有用户不知道(一般也不许可)的特性，激活后将影响系统或应用的正常功能，甚至危害或破坏系统。其主要危害体现在非授权安装(也被称为“流氓软件”)、自动收集系统或用户信息(也称为“间谍软件”)、自动拨号、自动弹出各种广告界面、恶意共享和浏览器劫持等。当前，恶意软件的出现、发展和变化给计算机及网络系统带来了巨大的危害。

(4) 后门：是指绕过安全性控制而获取对程序或系统访问权的方法。通常是在软件开发阶段，程序员在程序内创建后门以方便修改程序中的缺陷。但如果后门被其他人知道或软件发布之前未被删除，那么它就成了安全隐患。

(5) 恶意脚本：是指利用脚本语言编写的以危害或损坏系统功能、干扰用户正常使用为目的的任何脚本程序或代码段。目前，恶意脚本的危害不仅仅体现在修改用户个人终端的配置方面，而且还可以作为传播病毒和木马等的工具。用于编制恶意脚本的脚本语言包括 Java Attack Applets(Java 攻击小程序)、ActiveX 控件、JavaScript、VBScript、PHP、Shell 语言等。

(6) 移动终端恶意代码：是对移动终端各种病毒的广义称谓，是指以移动终端为感染对象，以移动网络和有线网络为平台，通过无线或有线的方式对移动终端进行攻击，从而造成移动终端异常的各种不良程序代码，如各种病毒、木马程序。

2. 网络所面临的主要安全威胁

相对于个人计算机而言，网络所面临的安全威胁除包括个人终端所面临的六种常见的威胁之外，主要是指由于网络的开放性、网络自身固有的安全缺陷和网络黑客的入侵与攻击(人为的因素)等三个方面带来的安全威胁。

1) 网络的开放性

网络的开放性主要表现为网络业务都是基于公开的协议，连接的建立是基于主机上彼此信任的原则，远程访问使得各种攻击无需到现场就能成功。因此，正是由于网络的开放性，使得在虚幻的计算机网络中网络犯罪往往十分隐蔽，虽然有时会留下一些蛛丝马迹，但更多的时候是无迹可寻。

2) 网络自身固有的安全缺陷

这是网络安全领域首要关注的问题，发现系统漏洞(安全缺陷)也是黑客进行入侵和攻击的主要步骤。据调查，国内 80%以上的网站存在明显的漏洞。漏洞的存在给网络上不法分子的非法入侵提供了可乘之机，也给网络安全带来了巨大的风险。据美国 CERT/CC 统计，

2014年总共收到系统漏洞报告7038个，平均每天超过19个(自1995年以来，漏洞报告总数已经达到数十万个)。这些漏洞的存在对广大互联网用户的系统造成了严重的威胁。

当前，操作系统的漏洞是我们面临的最大风险。比如，Windows操作系统是目前使用最为广泛的系统，但经常发现存在漏洞。过去Windows操作系统的漏洞主要被黑客用来攻击网站，对普通用户没有多大影响，但近年来一些新出现的网络病毒利用Windows操作系统的漏洞进行攻击，能够自动运行、繁衍，无休止地扫描网络和个人计算机，然后进行有目的的破坏，比如“红色代码”、“尼姆达”、“蠕虫王”以及“冲击波”等。随着Windows操作系统越来越复杂和庞大，出现的漏洞也越来越多，利用Windows操作系统漏洞进行攻击造成的危害越来越大，甚至有可能给整个互联网带来不可估量的损失。

3) 人为因素的威胁

虽然人为因素和非人为因素都对计算机及网络系统构成威胁，但精心设计的人为攻击(因素)威胁最大。人为因素的威胁是指人为造成的威胁，包括偶发性和故意性威胁。具体来说主要包括网络攻击、蓄意入侵和计算机病毒等。一般来说，人为因素威胁可以分为人为失误、恶意攻击和管理不善。

(1) 人为失误：一是配置和使用中的失误，比如系统操作人员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不恰当，用户将自己的账号随意转借给他人或信息共享等都会对网络安全带来威胁；二是管理中的失误，比如用户安全意识薄弱，对网络安全不重视，安全措施不落实，导致安全事故发生。据调查表明，在发生安全事件的原因中，居前两位的分别是“未修补软件安全漏洞”和“登录密码过于简单或未修改”，这表明大多数用户缺乏基本的安全防范意识和防范常识。

(2) 恶意攻击：这是当前计算机及网络系统面临的最大威胁，主要分为两大类：一是主动攻击，它使用各种攻击方式有选择地破坏信息的完整性、有效性和可用性等；二是被动攻击，它是在不影响计算机及网络系统正常工作的情况下，进行信息的窃取、截获、破译等，以获取重要的机密信息。这两类攻击均能对计算机及网络系统造成极大的破坏，并导致机密信息泄露。

(3) 管理不善：一般来说，网络安全不能单靠数学算法和安全协议来满足，还需要妥善的法律法规、管理制度才能达到期望的目标。目前，系统管理不善也为一些不法分子提供了可乘之机。据统计，80%以上的机密泄露都是由于系统内部人员管理不善造成的。同时，对网络系统的严格管理也是避免受到攻击的重要措施。

1.1.3 信息安全机制与信息安全服务

当前，为了保证网络系统中信息安全的实现，人们通常在某些安全机制的基础上，向用户提供一定的安全服务，以保障各种资源合法地使用和稳定、可靠地运行及传输。

1. 安全机制

所谓安全机制就是保护系统安全运行，确保系统免受攻击、侦听及恢复系统的技术或方法。信息系统的安全是一个系统的概念，为了保障信息系统的安全可以采用多种安全机制。在ISO 7498-2(我国称为GB/T9387-2)标准中，将安全机制定义为通用安全机制和特殊安全机制两大类。

1) 通用安全机制

(1) 可信功能：根据安全策略而建立起来的标准被认定是可信的。

(2) 安全标签：主要是资源的标签，用以指明该资源的安全属性。

(3) 事件检测：检测与安全相关的事件。

(4) 安全审计跟踪：指对系统记录和系统行为的检查和回顾。

(5) 安全恢复机制：根据安全机制的要求，对受攻击后的系统采取恢复的行为。

2) 特殊安全机制

(1) 加密(Encryption)：运用密码算法将明文数据加密成不可直接识读的密文数据。

(2) 数字签名(Digital Signature)：证实数据来源的真实性，防止伪造和否认。

(3) 访问控制(Access Control)：对系统资源进行访问控制的各种机制。

(4) 数据完整性(Data Integrity)：保证数据不被篡改、伪造等。

(5) 鉴别(Authentication)：用来确认数据来源的真实性或实体的身份。

(6) 业务流量填充(Traffic Padding)：为了阻止流量分析而采取插入无用数据的操作。

(7) 路由控制(Routing Control)：可为某些特定的数据选取物理上安全的传输路线。

(8) 公正机制(Notarization Mechanisms)：利用可信第三方来保证数据交换的真实性、完整性、不可否认性等。

在以上安全机制中，除了业务流量填充、路由控制和事件检测之外，其余安全机制都与密码算法有关，因此说密码算法是信息安全的核心技术。通常，一种安全机制可以提供多种安全服务，而一种安全服务也可采用多种安全机制。

2. 安全服务

安全服务就是加强信息系统数据处理和信息传输安全性的一类服务，采用安全服务也能在一定程度上弥补和完善现有操作系统和信息系统的安全漏洞，其目的在于采用一种或多种安全机制阻止安全攻击。在 ISO 7498－2 标准中定义了六类可选的安全服务：鉴别(Authentication)、数据机密性(Data Confidentiality)、数据完整性(Data Integrity)、访问控制(Access Control)、可用性(Availability)、不可否认性(Non-repudiation)。

1.1.4 信息安全模型

为了更好地分析信息系统的安全问题，找出问题的关键，需要建立一个信息系统安全的基本模型。从网络通信的角度看，网络信息系统可分为通信服务提供者(系统)和通信服务使用者(系统)两个系统。两个系统的侧重点不一样，其基本的安全模型也不一样。

1. 通信服务提供者的信息安全模型

通信服务提供者的目标是安全可靠地跨越网络传输信息。当通信双方欲传递某个消息时，首先需要在网络中确定从发送方到接收方的一个路由，然后在该路由上共同采用通信协议协商建立一个逻辑上的信息通道。实现安全通信主要包括以下两个方面。

(1) 对消息进行安全相关的变换：如对消息进行加密和鉴别。加密的目的是对消息进行重新编码(组合)，以使非授权用户无法读懂消息的内容；鉴别的目的是确保发送者身份的真实性。

(2) 通信双方共享某些秘密信息：这些信息是不希望对手获知的，比如加密密钥。