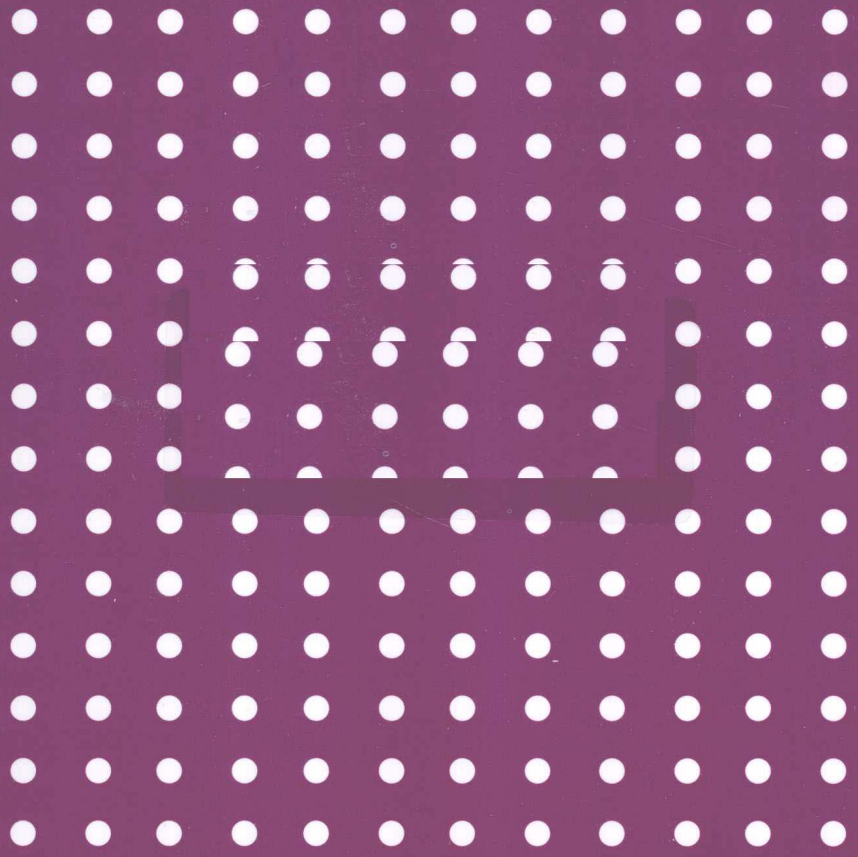
重点大学信息安全专业规划系列教材

信息安全综合实践

李建华 陈恭亮 陆松年 薛质 等 编著



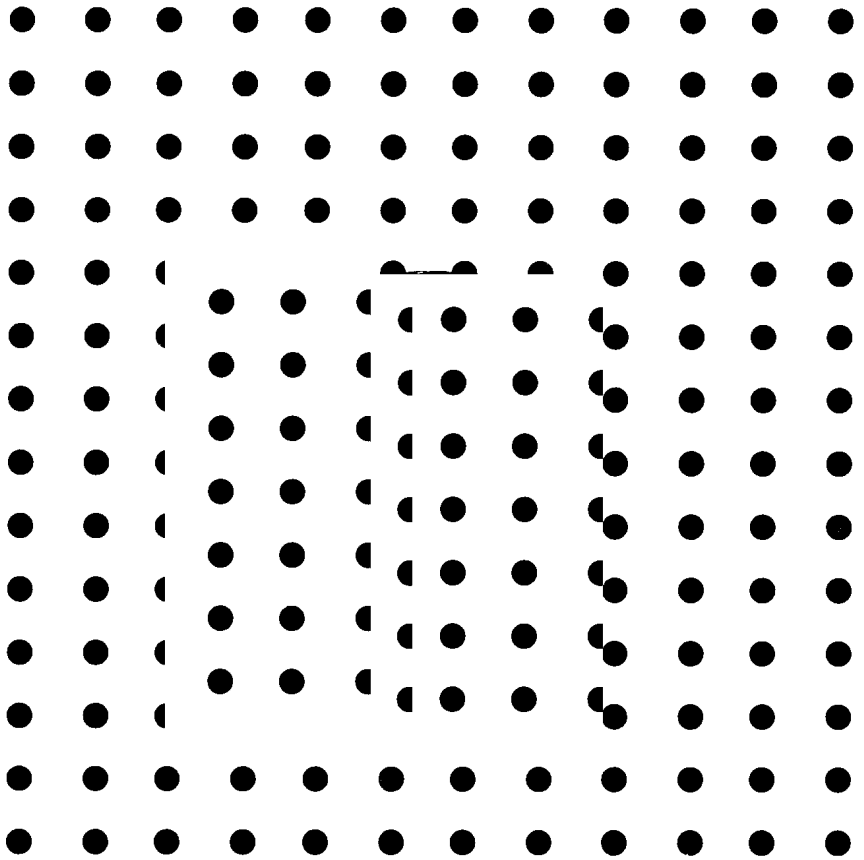
清华大学出版社

重点大学信息安全专业规划系列教材

信息安全综合实践

主编 李建华

编著 陈恭亮 陆松年 薛 质 孟 魁 蒋兴浩
张爱新 龚洁中 杜海波 吴 越 刘功申
范 磊 张保稳 马 进



清华大学出版社

北京

内 容 简 介

本书系统地介绍了信息安全所涉及的信息安全认证类、信息安全综合管理类、信息安全攻击与防护类以及无线网络安全等实验，这些实验分成基础性实验、拓展性实验和创新性实验，有些可独立实施，有些则要借助于信息安全综合实践平台来实现。

本书可作为信息安全专业、通信专业、计算机专业、信息专业的本科生和研究生的教科书，也可以供从事信息安全工作的科研和工程技术人员参考。

图书在版编目（CIP）数据

信息安全综合实践/李建华等编著. —北京：清华大学出版社，2010.2
（重点大学信息安全专业规划系列教材）
ISBN 978-7-302-21353-6

Ⅰ.信… Ⅱ.李… Ⅲ.信息系统-安全技术-高等学校-教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2009）第 194982 号

责任编辑：丁　岭　李玮琪
责任校对：李建庄
责任印制：王秀菊
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：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：23　**字　数**：571 千字
版　　次：2010 年 2 月第 1 版　　**印　　次**：2010 年 2 月第1 次印刷
印　　数：1～3000
定　　价：36.00 元

出版说明

计算机的广泛应用和网络技术的普及使得信息安全不仅涉及保密通信和数据安全，还涉及计算机安全、通信安全和网络安全，以及由此带来的保障信息系统正常运行等安全问题。国家信息基础设施在国家经济、政治、军事和社会生活中起着重要的核心作用，且信息也可作为重要的物质资源，因此，信息安全还关系到国家安全。

2003年中央《关于加强信息安全保障工作的意见》(27号)的文件将信息安全工作提升到保护公众利益和维护国家安全以及保障与促进信息化发展的高度，并明确提出要加强国内信息安全专业和院系建设，培养信息安全高级人才。国家中长期科技发展规划、国家"十一五"科技发展规划、国家信息化中长期发展规划等国家科技发展规划都强调建设信息安全保障体系。2005年教育部(7号)专门发文强调信息安全专业建设和信息安全学科专业技术教育。

信息安全是一门新兴的综合性交叉学科，它涉及通信、密码学、计算机、数学、物理、控制、人工智能、安全工程、法律、管理等诸多学科。信息安全技术随着信息技术的发展和信息化的推进而发展。本着安全性和有效性的原则，信息安全既要学习和应用新的信息技术，解决不断出现的信息安全问题，同时也不断提出新的科学问题，推动其他学科的发展。

近年来，我国高等学校信息安全专业学科建设取得了长足的进步，学科体系和课程体系日趋完善，信息安全专业人才培养实现了历史性的跨越。但也存在一些不足，例如，信息安全专业教材难以满足当前专业教学需要，特别是缺少与信息安全工程实践的结合的教材。为此，我们决定组织编写本系列教材，以满足信息安全专业的教学需要，并通过这些教材促进专业教学的发展，同时展示和示范近年来信息安全专业的教学成果。为了确保本系列教材质量，参加本系列教材的编写和编审工作的人员全部来自于国内重点高校信息安全专业的知名教师和专家。

系列教材建设目的

(1) 满足高等学校信息安全专业的教学需要，促进专业教学的教学发展。

(2) 共享高等学校信息安全专业的教育资源。

(3) 展示和示范高等学校信息安全专业的教学成果。

系列教材建设原则与特色

(1) 面向学科发展和内容的更新，适应当前社会对信息安全专业高级人才的培养需求，教材内容以基本理论为基础，反映基本理论和原理的综合应用，重视实践和应用环节。

(2) 反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，在选择教材内容和编写体系时注意体现素质教育、创新能力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

(3) 实施精品战略，突出重点，保证质量。教材建设的重点依然是专业基础课和专业主干课；特别注意选择并安排原来基础比较好的优秀教材或讲义修订再版，如国家精品课程、部级及校级精品课程逐步形成精品教材；提倡并鼓励编写体现重点大学信息安全专业教学内容和课程体系改革成果的教材。

(4) 主张一纲多本，合理配套。专业基础课和专业主干课教材要配套，同一门课程可以有多本具有不同内容特点的教材。处理好教材统一性与多样化，基本教材与辅助教材、教学参考书，文字教材与软件教材的关系，实现教材系列资源配套。

(5) 依靠专家，择优落实。依靠各课程专家在调查研究本课程教材建设现状的基础上提出选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后要认真实行审稿程序，确保出书质量。

特别期待信息安全专业领域的科研技术人员、教师和专家能够向我们推荐更丰富的专业教材，希望在专业工程教学一线的专家同仁根据自身的教学特点，对本系列教材建设提出宝贵意见(dingl@ tup.tsinghua.edu.cn)。特别感谢上海交通大学信息安全工程学院等院系的对本系列教材建设工作的大力支持与帮助。

编　者

2009 年 8 月

FOREWORD

前言

信息安全学科是一门新兴的综合性交叉学科，涉及通信学、计算机科学、密码学、信息学、数学、安全工程、法律、管理等诸多学科，也关系到国家社会信息化的推进、国家基础信息系统的安全保障工作、电子政务和电子商务的应用以及国家安全。本书编者积极探索和建设以主干专业课为基础，以实习实践为主线，面向工程应用的实践教学模式。依托在国家863重大项目“信息安全工程实践综合实验平台研究与集成”等滚动支持下建设的国内首个信息安全综合实践平台，教学团队开设了“信息安全综合实践”、“信息安全科技创新”等课程，通过基础性实验、拓展性实验和创新性实验，深化学生专业理论知识的掌握和应用，培养学生的实践能力和创新精神，也形成了由信息安全认证类、信息安全综合管理类、信息安全攻击与防护类以及无线网络安全等部分组成的教材体系。为了更好地与国内外信息安全工作者进行学术和教学交流，推动国内信息安全工程实践人才的培养，教学团队将所形成的教材整理成书，抛砖引玉。对于书中的不足之处恳请读者批评指正。

参与本书编写的人员有李建华、陈恭亮、陆松年、薛质、孟魁、蒋兴浩、张爱新、龚洁中、杜海波、吴越、范磊、张宝稳、刘功申、马进等。

本书在编写过程中得到了上海交通大学信息安全工程学院许多教师以及本科生和研究生的支持和帮助，在此向他们表示衷心感谢。另外，特别感谢国家自然科学基金（项目编号：60672068）和国家863重大项目（项目编号：2002AA145090,2005AA145110）的支持。

CONTENTS

目录

第 1 章　密码技术及实验 ····· 1

1.1　密码技术 ····· 1
1.1.1　密码学基本概念 ····· 1
1.1.2　信息论和密码学 ····· 2
1.1.3　密码编制学 ····· 2
1.1.4　密码分析学 ····· 4
1.1.5　小结 ····· 5
1.2　素数生成实验 ····· 5
1.2.1　Eratosthenes 筛法实验 ····· 5
1.2.2　Rabin-Miller 素性检验实验 ····· 6
1.3　恺撒密码算法 ····· 6
1.4　线性反馈移位寄存器 ····· 7
1.4.1　线性反馈移位寄存器周期计算实验 ····· 8
1.4.2　反馈参数计算实验 ····· 8
1.5　DES 算法实验 ····· 9
1.5.1　DES 单步加密实验 ····· 9
1.5.2　DES 加解密实验 ····· 11
1.5.3　3DES 算法实验 ····· 12
1.6　MD5 算法实验 ····· 13
1.7　RSA 算法实验 ····· 15
1.8　SHA-1 算法实验 ····· 18
1.9　AES 算法实验 ····· 19
1.10　DSA 数字签名实验 ····· 21
1.11　ECC 算法实验 ····· 23
1.11.1　椭圆曲线简介 ····· 24
1.11.2　椭圆曲线上的离散对数问题 ····· 27
1.11.3　椭圆曲线密码算法 ····· 27
1.12　密码算法分析设计实验 ····· 27
1.13　密码技术应用实验 ····· 28

第 2 章　PKI 系统及实验 ····· 29

2.1　PKI 体系结构 ····· 29

2.1.1 PKI 概述 29
2.1.2 PKI 实体描述 29
2.1.3 PKI 提供的核心服务 34
2.1.4 PKI 的信任模型 34
2.2 证书管理体系 40
2.2.1 证书种类 40
2.2.2 PKI 的数据格式 43
2.2.3 证书策略和证书实施声明 48
2.2.4 证书生命周期 51
2.3 PKI 实验系统简介 56
2.3.1 系统功能 56
2.3.2 系统特点 57
2.3.3 应用范围及对象 57
2.3.4 定义、缩写词及略语 57
2.3.5 系统环境要求 57
2.4 证书申请实验 58
2.5 PKI 证书统一管理实验 60
2.5.1 注册管理实验 60
2.5.2 证书管理实验 62
2.6 交叉认证及信任管理实验 63
2.6.1 信任管理实验 64
2.6.2 交叉认证实验 66
2.7 证书应用实验 68
2.7.1 对称加密实验 69
2.7.2 数字签名实验 70
2.8 SSL 应用实验 71
2.9 基于 S/MIME 的安全电子邮件系统的设计与实现 74
2.10 信息隐藏与数字水印实验 75
2.11 数字签章实验 75

第 3 章 IPSec VPN 系统 77

3.1 VPN 基础知识 77
3.2 IPSec 的原理以及 IPSec VPN 的实现 78
3.2.1 IPSec 的工作原理 78
3.2.2 IPSec 的实现方式 79
3.2.3 IPSec VPN 的实现方式 83
3.3 大规模交互式 VPN 教学实验系统 87
3.3.1 实验系统拓扑结构 88
3.3.2 VPN 安全性实验 88

3.3.3 VPN 的 IKE 认证实验 ····· 93
3.3.4 VPN 模式比较实验 ····· 96
3.4 IPSec VPN 的深入研究 ····· 102

第 4 章 MPLS VPN 技术及实验 ····· 104

4.1 MPLS 原理 ····· 104
4.2 MPLS 在 VPN 中的应用 ····· 106
4.3 MPLS 实验 ····· 109
4.4 MPLS VPN 实验 ····· 114

第 5 章 安全协议 ····· 117

5.1 安全协议基本知识 ····· 117
5.2 安全协议分析 ····· 119
5.2.1 安全协议分析过程 ····· 119
5.2.2 安全协议的运行环境 ····· 119
5.3 串空间技术 ····· 120
5.3.1 基本概念 ····· 121
5.3.2 渗入串空间 ····· 122
5.3.3 串空间分析的原理 ····· 123
5.4 课程实验 ····· 123
5.4.1 Needham-Schroeder 协议分析实验 ····· 123
5.4.2 NSL 协议分析实验 ····· 124

第 6 章 多级安全访问控制 ····· 126

6.1 基础知识 ····· 126
6.1.1 常用术语 ····· 126
6.1.2 访问控制级别 ····· 127
6.1.3 访问控制类别 ····· 128
6.2 访问控制策略 ····· 129
6.2.1 访问控制策略的概念 ····· 129
6.2.2 访问控制策略的研究和制定 ····· 129
6.2.3 当前流行的访问控制策略 ····· 130
6.2.4 访问控制策略的实现 ····· 133
6.2.5 访问控制机制 ····· 134
6.2.6 访问控制信息的管理 ····· 134
6.3 访问控制的作用与发展 ····· 135
6.3.1 访问控制在安全体系中的作用 ····· 135
6.3.2 访问控制的发展趋势 ····· 135
6.4 安全访问控制技术实验 ····· 137
6.4.1 PMI 属性证书技术实验 ····· 137

6.4.2 XACML 技术实验 ····· 143
6.4.3 模型实验 ····· 147
6.4.4 基于角色访问控制系统实验 ····· 150

第 7 章 安全审计系统 ····· 156

7.1 安全审计基础知识 ····· 156
7.1.1 安全审计的相关概念 ····· 156
7.1.2 安全审计的目标和功能 ····· 158
7.1.3 网络安全审计技术方案和产品类型 ····· 159
7.1.4 网络安全审计的步骤 ····· 162
7.1.5 网络安全审计的发展趋势 ····· 163
7.2 安全日志基础知识 ····· 163
7.2.1 日志的基本概念 ····· 163
7.2.2 如何发送和接收日志 ····· 164
7.2.3 日志检测和分析的重要性 ····· 164
7.2.4 如何分析日志 ····· 165
7.2.5 日志审计的结果 ····· 166
7.2.6 日志审计的常见误区和维持日志审计的方法 ····· 167
7.3 安全审计系统基础知识 ····· 169
7.3.1 安全审计系统的历史和发展 ····· 169
7.3.2 全审计系统的关键技术 ····· 170
7.3.3 安全审计系统的网络拓扑结构 ····· 172
7.4 安全审计实验系统 ····· 172
7.4.1 文件审计实验 ····· 173
7.4.2 网络审计实验 ····· 174
7.4.3 打印审计实验 ····· 176
7.4.4 拨号审计实验 ····· 177
7.4.5 审计跟踪实验 ····· 179
7.4.6 主机监控实验 ····· 181
7.4.7 日志查询实验 ····· 182

第 8 章 病毒原理及其实验系统 ····· 185

8.1 计算机病毒基础知识 ····· 185
8.1.1 计算机病毒的定义 ····· 185
8.1.2 计算机病毒的特性 ····· 186
8.1.3 计算机病毒的分类 ····· 186
8.1.4 计算机病毒的命名准则 ····· 187
8.1.5 计算机病毒的历史发展趋势 ····· 189
8.2 计算机病毒的结构及技术分析 ····· 192
8.2.1 计算机病毒的结构及工作机制 ····· 192

8.2.2 计算机病毒的基本技术 ····· 193
8.3 计算机病毒防治技术 ····· 195
8.3.1 计算机病毒的传播途径 ····· 195
8.3.2 计算机病毒的诊断 ····· 197
8.3.3 计算机病毒的清除 ····· 199
8.3.4 计算机病毒预防技术 ····· 201
8.3.5 现有防治技术的缺陷 ····· 202
8.4 计算机病毒预防策略 ····· 203
8.4.1 国内外著名杀毒软件比较 ····· 203
8.4.2 个人计算机防杀毒策略 ····· 206
8.4.3 企业级防杀毒策略 ····· 208
8.4.4 防病毒相关法律法规 ····· 213
8.5 流行病毒实例 ····· 213
8.5.1 蠕虫病毒 ····· 213
8.5.2 特洛伊木马病毒 ····· 215
8.5.3 移动终端病毒 ····· 215
8.5.4 Linux 脚本病毒 ····· 217
8.6 病毒实验系统 ····· 221
8.6.1 网络炸弹脚本病毒 ····· 221
8.6.2 万花谷脚本病毒 ····· 223
8.6.3 欢乐时光脚本病毒 ····· 225
8.6.4 美丽莎宏病毒 ····· 228
8.6.5 台湾 No.1 宏病毒 ····· 231
8.6.6 PE 病毒实验 ····· 233
8.6.7 特洛伊木马病毒实验 ····· 236
第 9 章 防火墙技术及实验 ····· 238
9.1 防火墙技术基础 ····· 238
9.2 防火墙技术的发展 ····· 239
9.3 防火墙的功能 ····· 240
9.3.1 防火墙的主要功能 ····· 240
9.3.2 防火墙的局限性 ····· 241
9.4 防火墙的应用 ····· 241
9.4.1 防火墙的种类 ····· 241
9.4.2 防火墙的配置 ····· 243
9.4.3 防火墙的管理 ····· 245
9.5 防火墙技术实验 ····· 247
9.5.1 普通包过滤实验 ····· 247
9.5.2 NAT 转换实验 ····· 249
9.5.3 状态检测实验 ····· 251
9.5.4 应用代理实验 ····· 254

9.5.5 事件审计实验 ····· 260
9.5.6 综合实验 ····· 261

第 10 章 攻防技术实验 ····· 263

10.1 信息搜集 ····· 263
10.1.1 主机信息搜集 ····· 263
10.1.2 Web 网站信息搜集 ····· 265
10.2 嗅探技术 ····· 270
10.2.1 嗅探器工作原理 ····· 271
10.2.2 嗅探器造成的危害 ····· 272
10.2.3 常用的嗅探器 ····· 273
10.2.4 交换环境下的嗅探方法 ····· 273
10.3 ICMP 重定向攻击 ····· 275
10.3.1 ARP 协议的欺骗攻击 ····· 275
10.3.2 网络层协议的欺骗与会话劫持 ····· 277
10.3.3 应用层协议的欺骗与会话劫持 ····· 280
10.4 后门技术 ····· 284
10.4.1 木马概述 ····· 284
10.4.2 木马程序的自启动 ····· 287
10.4.3 木马程序的进程隐藏 ····· 289
10.4.4 木马程序的数据传输隐藏 ····· 290
10.4.5 木马程序的控制功能 ····· 292
10.5 缓冲区溢出攻击 ····· 293
10.5.1 缓冲区溢出攻击简介 ····· 293
10.5.2 缓冲区溢出技术原理 ····· 294
10.5.3 缓冲区溢出漏洞的预防 ····· 297
10.6 拒绝服务攻击 ····· 298
10.6.1 典型的 DoS 攻击 ····· 298
10.6.2 分布式拒绝服务攻击 ····· 299
10.6.3 分布式反射拒绝服务攻击 ····· 301
10.6.4 低速拒绝服务攻击 ····· 302

第 11 章 入侵检测技术 ····· 304

11.1 入侵检测系统概述 ····· 304
11.1.1 基本概念 ····· 305
11.1.2 IDS 的发展历程 ····· 306
11.1.3 IDS 的功能 ····· 308
11.2 入侵检测基本原理 ····· 309
11.2.1 通用入侵检测模型 ····· 309
11.2.2 数据来源 ····· 310

11.2.3 检测技术 ····· 314
11.2.4 响应措施 ····· 316
11.3 入侵检测方法 ····· 317
11.3.1 异常检测技术 ····· 317
11.3.2 误用检测技术 ····· 318
11.3.3 其他检测方法 ····· 319
11.4 入侵检测实验 ····· 319
11.4.1 特征匹配检测实验 ····· 319
11.4.2 完整性检测实验 ····· 326
11.4.3 网络流量分析实验 ····· 329
11.4.4 误警分析实验 ····· 333
11.5 IDS 实现时若干问题的思考 ····· 337
11.5.1 当前 IDS 发展面临的问题 ····· 337
11.5.2 IDS 的评测 ····· 337
11.5.3 IDS 的相关法律问题 ····· 338
11.5.4 入侵检测技术发展趋势 ····· 339
11.6 小结 ····· 339

第 12 章 无线网络 ····· 340

12.1 无线网络安全 ····· 340
12.1.1 WEP ····· 340
12.1.2 802.1x ····· 341
12.1.3 WPA ····· 342
12.1.4 802.11i(WPA2) ····· 344
12.2 WEP 加密实验 ····· 344
12.3 WPA 加密实验 ····· 346
12.4 WEP 破解 ····· 346
12.5 WPA-EAP 配置 ····· 347
12.6 WDS 安全配置 ····· 349

参考文献 ····· 352

CHAPTER 1

密码技术及实验

第1章

1.1 密码技术

密码学是一门古老的科学。它的起源可以追溯到 4000 多年前的古埃及、巴比伦、古罗马和古希腊，大概自人类社会出现战争时起便出现了密码。在 1949 年之前，密码技术更多地只能称为艺术而不是科学，密码的设计和分析是凭直觉和经验来进行的，而不是靠严格的理论证明。而随着电子计算机的诞生以及香农 (Shannon) 发表了《保密系统的通信理论》一文，密码学的研究才真正进入现代科学研究的范畴。

密码学又是一门年轻的科学。随着科学技术的进步，密码学的研究也日新月异。首先，密码学越来越依赖于数学知识，现代密码学离开数学几乎是不可想象的；其次，密码学还与别的学科相互渗透，如量子力学、光学、混沌学、生物学等，并且互相促进。

1.1.1 密码学基本概念

自古以来，密码主要应用于军事、政治、外交等机要部门，因而密码学的研究工作本身也是秘密进行的。然而随着计算机科学、通信技术、微电子技术的发展，计算机网络的应用进入了人们的日常生活和工作中，从而产生了保护隐私、敏感甚至秘密信息的需求，而且这样的需求在不断扩大，于是密码学的应用和研究逐渐公开化，并呈现出了空前的繁荣。

研究密码编制的科学称为密码编制学（Cryptography），研究密码破译的科学称为密码分析学（Cryptanalysis），它们共同组成了密码学（Cryptology）。

密码技术的基本思想就是伪装信息，即对信息做一定的数学变换，使不知道密钥的用户不能解读其真实的含义。变换之前的原始数据称为明文（Plaintext），变换之后的数据称为密文（Ciphertext），变换的过程就叫做加密（Encryption），而通过逆变换得到原始数据的过程就称为解密（Decryption），解密需要的条件或者信息称为密钥（Key），通常情况下密钥就是一系列字符串。

一个密码系统主要由以下五部分构成：

(1) 明文空间 M—— 所有明文的集合；

(2) 密文空间 C—— 全体密文的集合；

(3) 密钥空间 K—— 全体密钥的集合，其中每一个密钥 k 均由加密密钥 K_e 和解密密钥 K_d 组成，即 $K=(K_e,K_d)$，在某些情况下 $K_e=K_d$；

(4) 加密算法 E—— 一组以 K_e 为参数的由 M 到 C 的变换，即 $C=E(K_e,M)$，可简写为 $C=E_{K_e}(M)$；

(5) 解密算法 D—— 一组以 K_d 为参数的由 C 到 M 的变换，可表示为 $M = D(K_d, C)$ 或 $M = D_{K_d}(C)$。

密码系统模型如图 1.1 所示。

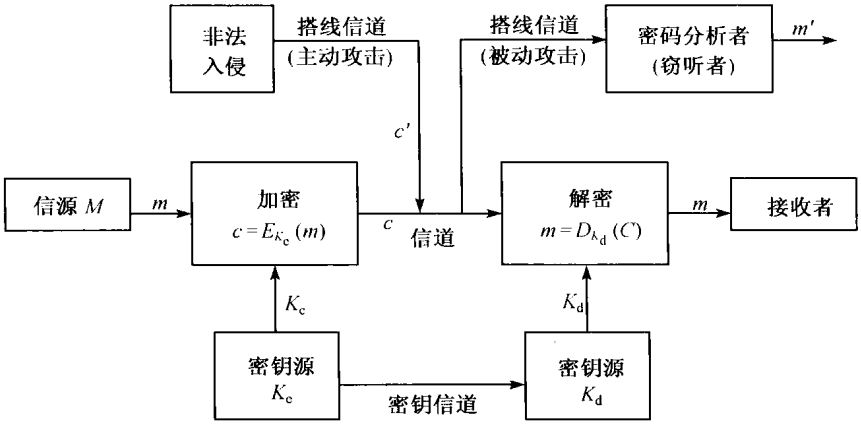


图 1.1　密码系统模型

从图 1.1 中可以了解密码系统工作的大体流程以及可能存在的被攻击的情形：信息的发送者通过一个加密算法将消息明文 m 加密为密文 c，然后通过不安全的信道传送给接收者，接收者接到密文 c 后用已知的密钥 K 来进行解密得到明文 m。而在信息的传输过程中，可能会有主动攻击者冒充发送者传送 c' 给接收者，干扰或者破坏通信；也可能会有被动攻击者盗取密文 c，那么密码分析者的工作就是在不知道 K 的情况下通过 c 来恢复出 m。以上两种攻击行为在现实生活中非常常见，因此对作为信息安全关键技术的密码学的研究就显得尤为重要和迫切。

1.1.2　信息论和密码学

现代信息论是由香农于 1948 年首先确立的，他在论文《通信的数学理论》中详细阐述了如何用信息论的观点处理存在随机干扰的通信系统中的信息传输问题。

1949 年香农发表了题为《保密系统的通信理论》的著名论文，从信息论的角度对信息源、密钥、加密和密码分析进行了数学分析，用不确定性和唯一解距离来度量密码体制的安全性，阐述了密码体制、完善保密性、纯密码、理论保密和实际保密等重要概念，把密码置于坚实的数学基础之上，标志着密码学作为一门独立学科的成立。从此，信息论成为密码学的重要理论基础之一。关于这部分内容的详细讨论请参考相关资料。

1.1.3　密码编制学

密码编制学是对消息进行编码以隐藏明文消息的一门学问。

从现代密码学的观点来看，许多古典密码都是不安全的，或者说是很容易被破译的。替代和置换是古典密码中常用的变换形式。

1. 替代密码

首先需要构造一两个或者多个密文字母表，然后用密文字母表中的字母或字母组来替

代明文字母或字母组，各个字母或字母组的相对位置不变，但其本身改变了。下面来看一下罗马皇帝 Julius Caesar 在公元前 50 年左右所使用的“恺撒密码”，这其实就是一种典型的替代密码。他将字母按字母表中的顺序循环排列，将明文中的每个字母用其后面的第三个字母代替以得到对应的密文。

以英文为例，恺撒密码所使用的明文字母表和密文字母表分别为：

明文字母表：a b c d e f g h i j k l m n o p q r s t u v w x y z
密文字母表：d e f g h i j k l m n o p q r s t u v w x y z a b c

那么，对于明文 attack postoffice，经恺撒密码变换后得到的密文为：

dwwdfn srvwriilfh

恺撒密码可以说是替代密码的最简单的例子。在替代密码中，密文中的字母顺序与明文中的字母顺序一致，只不过各密文字母是由相应的明文字母按某种映射变换得到的。

按照映射规则的不同，替代密码可分为 3 种：单表替代密码、多表替代密码和多字母替代密码。在此不再详述，有兴趣的读者可查看相关资料。

2. 置换密码

将明文中的字母重新排列，字母表示不变，但其位置改变了，这样编成的密码就称为置换密码。换句话说，明文与密文所使用的字母相同，但是它们的排列顺序不同。最简单的置换密码就是把明文中的字母顺序颠倒一下。

可以将明文按矩阵的方式逐行写出，然后再按列读出，并将它们排成一排作为密文，列的阶就是该算法的密钥。在实际应用中，人们常常用某一单词作为密钥，按照单词中各字母在字母表中的出现顺序排序，用这个数字序列作为列的阶。

【例 1-1】 若以 coat 作为密钥，则它们的出现顺序为 2、3、1、4，对明文 attack postoffice 加密的过程如图 1.2 所示。

按照阶数由小到大逐列读出各字母，所得密文为：

t p o c a c s f t k t i a o f e

密钥	c o a t
阶	2 3 1 4
	a t t a c k p o s t o f f i c e

图 1.2 对明文 attack postoffice 加密的过程

对于这种列变换类型的置换密码，密码分析很容易进行：将密文逐行排列在矩阵中，并依次改变行的位置，然后按列读出，就可得到有意义的明文。为了提高它的安全性，可以按同样的方法执行多次置换。例如对上述密文再执行一次置换，就可得到原明文的二次置换密文：

o s t f t a t a p c k o c f i e

还有一种置换密码采用周期性换位。对于周期为 r 的置换密码，首先将明文分成若干组，每组含有 r 个元素，然后对每一组都按前述算法执行一次置换，最后得到密文。

【例 1-2】 一个周期为 4 的换位密码，密钥及密文同例 1-1，加密过程如图 1.3 所示。

密钥	c o a t	c o a t	c o a t	c o a t
阶	2 3 1 4	2 3 1 4	2 3 1 4	2 3 1 4
明文	a t t a	c k p o	s t o f	f i c e
密文	t a t a	p c k o	o s t f	c f i e

图 1.3 周期性换位密码

相比之下，现代密码算法的编制需要考虑的因素要比古典密码多得多，在设计方案上也要复杂得多。以最常见的数据加密标准 DES 为例，它就综合运用了置换、替代、代数等多种密码技术，堪称近代密码的一个典范。关于 DES 的更多详细内容，请参看《现代密码技术》一书。

1.1.4 密码分析学

密码分析学就是研究密码破译的科学。如果能够根据密文系统确定出明文或密钥，或者能够根据明文密文对系统确定出密钥，则称这个密码系统是可破译的。常用的密码分析方法主要有 3 种。

(1) 穷举攻击：对截获的密文，密码分析者试遍所有的密钥，以期得到有意义的明文；或者使用同一密钥，对所有可能的明文加密直到得到的密文与截获的密文一致。穷举攻击也称强力攻击或完全试凑攻击。

(2) 统计分析攻击：密码分析者通过分析明文与密文的统计规律，得到它们之间的对应关系。

(3) 数学分析攻击：密码分析者根据加密算法的数学依据，利用数学方法 (如线性分析、差分分析及其他一些数学知识) 来破译密码。

根据密码分析者可利用的数据，可将常见的密码分析攻击分为 4 类，由弱到强分别是唯密文攻击、已知明文攻击、选择明文攻击和选择密文攻击。

(1) 唯密文攻击：密码分析者有一些用同一密钥加密的密文，他们试图恢复出尽可能多的明文，或者推算出加密密钥以解出更多的密文。

(2) 已知明文攻击：密码分析者不仅得到了一些明文，而且也知道相应的密文，他们的任务是据此推出加密密钥或算法，而该算法可以对用同一密钥加密的任何密文进行解密。

(3) 选择明文攻击：密码分析者不仅可得到一些消息的密文和相应的明文，而且也可选择被加密的明文。通过选择特定的明文进行加密，有可能产生更多的关于密钥的消息，这比已知明文攻击更有效。如果分析者不仅能选择被加密的明文，还能基于以前的结果修正这个选择，那么就是自适应选择明文攻击。

(4) 选择密文攻击：密码分析者可选择不同的密文，并可得到对应的明文。这种攻击主要用于公钥算法。

一个密码系统，如果无论密码分析者截获多少密文和用什么技术方法进行攻击都不能被攻破，则称为绝对不可破译的。绝对不可破译的密码在理论上是存在的，这就是著名的 “一次一密” 密码。但是，由于密钥管理上的困难，“一次一密” 密码是不实用的。从理论上来说，如果能够拥有足够多的资源，那么任何实际使用的密码都是可以破译的。