北京市高等教育精品教材立项项目

高等学校规划教材

信息安全原理与应用

王 昭 袁 春 编著
陈 钟 审校

网络工程与信息安全

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

北京市高等教育精品教材立项项目
高等学校规划教材

信息安全原理与应用

王 昭 袁 春 编著
陈 钟 审校

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本教材涉及密码编码与网络安全从技术到管理的方方面面，以数据机密性、数据完整性、不可否认性、鉴别和访问控制五大类安全服务和安全模型为线索，介绍了信息安全的基本原理。以密码编码与密码分析相结合的思路，比较完整地介绍了密码编码学的基本原理和算法实现，包括：古典密码、现代对称密码、公钥密码和散列函数，并讨论了密码算法实际应用中的一些问题，如密钥长度、密钥管理、硬件加密和软件加密，以及算法应用中曾经出现的教训等。在此基础上，介绍了相关综合应用，包括电子邮件的安全、网络安全协议和数据库安全。在网络安全与系统安全方面讨论了网络入侵与攻击、入侵检测、防火墙和计算机病毒防范。此外也介绍了信息安全的一些标准化情况，包括标准化机构和信息安全的评估标准。本书不仅介绍网络安全的基本原理，更注重理论与实际的结合，在相关章节后附有一些加深理论理解的难易程度不同的思考练习题和实践/实验题。

本书可作为信息类专业高年级本科生和研究生教材，也可以为信息安全、计算机、通信和电子工程等领域研究和开发人员提供有益的帮助和参考。

图书在版编目(CIP)数据

信息安全原理与应用/王昭，袁春编著. —北京：电子工业出版社，2010.1
高等学校规划教材
ISBN 978-7-121-09887-1

Ⅰ. 信… Ⅱ. ①王…②袁… Ⅲ. 信息系统一安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2009)第 209308 号

策划编辑：冯小贝
责任编辑：李秦华
印　　刷：北京季蜂印刷有限公司
装　　订：三河市鹏成印业有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1092　1/16　印张：21　字数：538 千字
印　　次：2010 年 1 月第 1 次印刷
印　　数：4000 册　　定价：32.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010) 88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：(010) 88258888。

前　言

信息安全是一门跨学科跨专业的综合性学科，它涵盖了非常丰富的内容，涉及数论、密码编码、信息论、通信、网络、编程等多方面的知识，无论是从事管理，还是技术研发的人员，甚至普通的计算机用户，都需要从不同层次和角度了解这方面的基本知识。并且随着信息技术的发展，信息安全新技术新思想不断涌现。此外，它还是一门理论与实际紧密结合的学科。

本书主要是以作者多年来在北京大学讲授信息安全、应用密码学等课程讲义为基础编写而成的。编写中，我们力求做到内容的系统、完整和深入浅出，理论与实际的结合，原理的经典性和技术的先进性。

信息安全问题的解决方案可以分为两类，一类是以密码编码为基础的解决方案，另一类是和密码无关的一些解决方案。本书尽可能全面地涵盖这两类原理和技术，主要内容安排如下：

第 1 章介绍了 ISO 7498—2 定义的 OSI 的五大类安全服务：数据机密性、数据完整性、不可否认性、鉴别和访问控制。本书以经典的通信安全模型和信息访问安全模型为线索，介绍了这五大类安全服务。

第 2～5 章以密码分析和密码编码相结合的思路，比较完整地介绍了密码编码学的基本原理和算法实现，包括：古典密码、现代对称密码、公钥密码和散列函数。密码算法都以国际上经典的标准或最新的标准为例。在原理介绍的基础上，第 6 章和第 7 章讨论了密码算法实际应用中的一些问题，包括：密钥长度、密钥管理、硬件加密和软件加密，以及算法应用中曾经出现的教训等。

第 8 章、第 10 章和第 11 章介绍了密码编码的相关综合应用，包括鉴别协议、安全电子邮件和网络安全协议，其中的内容都以最新的 RFC 文档和相关文献资料为参考。

第 9 章和第 12～15 章主要讨论了与密码算法无关的安全解决方案，包括访问控制、防火墙技术、黑客攻击与防范技术、计算机病毒防治和入侵检测技术。

第 16 章介绍了信息安全的一些标准化情况，包括信息安全的标准化机构和有关标准。

最后，第 17 章介绍了一个综合应用信息安全有关原理的实例——数据库系统安全。

在相关章节后附有一些加深理论理解的难易程度不同的思考和练习题、实践/实验题，以帮助读者更深入和扎实地掌握相关知识。

根据编者经验，主要内容的课堂讲授需要 50 学时左右，也可根据教学对象和教学目标进行删减，建议根据课程内容再安排一定学时的课外实践/实验。

在本书的编写过程中，查阅和参考了大量文献资料，限于篇幅未能在书后的参考文献中一一列出，在此一并致谢。

本书第 1～16 章由北京大学信息科学技术学院的王昭老师编写，第 17 章由清华大学深圳研究生院的袁春老师编写，全书最后由王昭老师统稿。在编写过程中，得到了解放军某部南湘浩研究员、中科院研究生院翟起滨教授和北京大学信息科学技术学院屈婉玲教授的多次热情指导和帮助。北京大学信息科学技术学院唐礼勇副教授、胡建斌副教授、关志博士、软件与微电子学院沈晴霓副教授、周继军副教授等老师也为本书的编写提供了相关资料和帮

助。北京大学信息科学技术学院的本科生李翔宇、研究生周光明、刘国鹏、陈宇、王永刚、刘勇、金永明、桂尼克参与了书稿的校对、资料收集等工作。本书是北京市精品教材建设立项项目，也得到了电子工业出版社的大力支持。在此表示衷心的感谢。

北京大学信息科学技术学院陈钟教授自始至终关心本书的编写工作。成书后，陈老师又认真审阅了全部书稿，在此致以特别谢意。

信息安全是一个不断发展的领域，由于编者水平有限，书中错误和不当之处在所难免，敬请广大读者和同行专家批评指正，在此先致感谢之意。

为了配合教学，本书还提供与教材配套的电子课件。

编者

2009 年 10 月

目　录

第 1 章　绪论 …… 1
1.1　信息和信息安全的概念 …… 1
1.1.1　信息的定义 …… 1
1.1.2　信息的属性和价值 …… 1
1.1.3　信息安全的含义 …… 2
1.2　信息安全的威胁 …… 2
1.3　安全服务 …… 3
1.3.1　数据机密性 …… 4
1.3.2　数据完整性 …… 4
1.3.3　不可否认性 …… 4
1.3.4　鉴别 …… 5
1.3.5　访问控制 …… 5
1.3.6　OSI 安全服务的分层配置 …… 5
1.4　信息安全模型 …… 6
1.4.1　通信安全模型 …… 6
1.4.2　信息访问安全模型 …… 6
1.4.3　动态安全模型 …… 7
1.5　信息安全的技术体系 …… 7
1.6　信息安全的政策法规 …… 8
1.6.1　国际信息安全政策法规 …… 8
1.6.2　国内信息安全政策法规 …… 9
1.7　信息安全的相关机构和相关标准 …… 10
1.7.1　国际标准化机构 …… 10
1.7.2　美国的标准化机构 …… 11
1.7.3　信息安全组织机构 …… 12
1.7.4　国内标准制定情况 …… 12
思考和练习题 …… 13

第 2 章　密码学基础 …… 14
2.1　密码学的基本概念和术语 …… 14
2.1.1　消息和加密 …… 14
2.1.2　恺撒密表 …… 15
2.1.3　密码体制 …… 15
2.1.4　密码算法的分类 …… 16
2.1.5　密码分析 …… 17

2.1.6 密码算法的安全性 …… 17
2.2 密码学的历史 …… 18
2.3 古典密码 …… 20
2.3.1 古典密码的数学基础 …… 20
2.3.2 代替密码 …… 22
2.3.3 置换密码 …… 33
2.3.4 古典密码算法小结 …… 33
思考和练习题 …… 34
实践/实验题 …… 34

第 3 章 现代对称密码 …… 35
3.1 乘积密码 …… 35
3.2 对称分组密码的设计原理与方法 …… 36
3.2.1 对称分组密码的三个安全设计原则 …… 36
3.2.2 对称分组密码的两个基本设计方法 …… 37
3.3 数据加密标准 DES …… 37
3.3.1 DES 的产生与应用 …… 37
3.3.2 Feistel 密码结构 …… 38
3.3.3 对 DES 的描述 …… 39
3.3.4 对 DES 的讨论 …… 44
3.4 三重 DES …… 46
3.4.1 双重 DES …… 46
3.4.2 三重 DES …… 47
3.5 高级数据加密标准 AES …… 48
3.5.1 AES 的背景 …… 48
3.5.2 AES 的数学基础 …… 49
3.5.3 对 AES 的描述 …… 52
3.6 分组密码的工作模式 …… 58
3.6.1 电码本(ECB)工作模式 …… 59
3.6.2 密码分组链接(CBC)工作模式 …… 59
3.6.3 密码反馈(CFB)工作模式 …… 61
3.6.4 输出反馈(OFB)模式 …… 62
3.6.5 计数器(CTR)模式 …… 63
3.6.6 不是分组长度整数倍的报文的处理 …… 64
3.6.7 三重 DES 的工作模式 …… 65
3.7 流密码 …… 66
3.7.1 流密码的定义 …… 66
3.7.2 同步流密码 …… 66
3.7.3 密钥流生成器 …… 67
3.7.4 RC4 …… 69

3.7.5 A5 算法 ····· 70
3.8 随机数 ····· 70
3.8.1 真随机序列产生器 ····· 71
3.8.2 伪随机数产生器 ····· 72
3.8.3 基于密码编码方法的随机数 ····· 73
思考和练习题 ····· 73
实践/实验题 ····· 73

第 4 章 公钥密码 ····· 74
4.1 公钥密码体制的基本原理 ····· 74
4.1.1 公钥密码体制的概念 ····· 74
4.1.2 公钥密码体制的应用 ····· 75
4.1.3 公钥密码体制的思想和要求 ····· 76
4.1.4 公钥密码体制的安全性 ····· 76
4.2 公钥密码算法的数学基础 ····· 77
4.2.1 若干基本定理 ····· 78
4.2.2 离散对数难题 ····· 80
4.3 Diffie-Hellman 密钥交换算法 ····· 81
4.3.1 对 Diffie-Hellman 密钥交换算法的描述 ····· 81
4.3.2 对 Diffie-Hellman 密钥交换的攻击 ····· 82
4.4 背包算法 ····· 82
4.4.1 背包问题和背包算法的思想 ····· 82
4.4.2 超递增背包 ····· 83
4.4.3 转换背包 ····· 83
4.4.4 Merkle-Hellman 公钥算法 ····· 83
4.5 RSA 算法 ····· 84
4.5.1 RSA 算法描述 ····· 84
4.5.2 RSA 实现中的问题 ····· 86
4.5.3 RSA 的安全性 ····· 87
4.5.4 对 RSA 实现的攻击方法 ····· 88
4.6 EIGamal 算法 ····· 90
4.7 椭圆曲线密码算法(ECC) ····· 91
4.7.1 椭圆曲线的概念 ····· 91
4.7.2 有限域上的椭圆曲线 ····· 92
4.7.3 椭圆曲线密码算法 ····· 93
4.8 密码算法小结 ····· 95
思考和练习题 ····· 96
实践/实验题 ····· 96

第 5 章 消息鉴别和数字签名 ····· 97
5.1 消息鉴别 ····· 97

5.1.1 鉴别系统模型 …… 97
5.1.2 消息加密 …… 98
5.1.3 消息鉴别码 MAC …… 99
5.1.4 散列函数 …… 100
5.2 散列算法 …… 105
5.3 HMAC …… 106
5.4 数字签名 …… 107
5.4.1 数字签名的功能与特性 …… 107
5.4.2 数字签名方案 …… 109
思考和练习题 …… 113
实践/实验题 …… 113

第 6 章 密码实际应用问题 …… 114
6.1 密码功能的位置 …… 114
6.2 密钥管理 …… 115
6.2.1 密钥的类型 …… 116
6.2.2 密钥的产生和登记 …… 117
6.2.3 密钥的装入 …… 118
6.2.4 密钥的存储和保护 …… 118
6.2.5 密钥的分配 …… 119
6.2.6 密钥的使用控制 …… 124
6.2.7 密钥的撤销和销毁 …… 124
6.2.8 密钥的备份/恢复和更新 …… 124
6.3 密钥的长度 …… 125
6.3.1 对称算法的密钥长度 …… 125
6.3.2 公开密钥密码体制的密钥长度 …… 126
6.3.3 密码体制密钥长度的对比 …… 127
6.4 硬件加密和软件加密 …… 127
6.5 存储数据加密的特点 …… 128
6.6 压缩、纠错编码和加密 …… 128
6.7 文件删除 …… 128
6.8 关于密码的一些教训 …… 129
6.8.1 声称你的算法是“不可攻破的” …… 129
6.8.2 多次使用一次性密码本 …… 129
6.8.3 没有使用最好的可能算法 …… 129
6.8.4 没有正确实现算法 …… 129
6.8.5 在产品中放置了后门 …… 129
思考和练习题 …… 130
实践/实验题 …… 130

第 7 章　公开密钥管理 …… 131
7.1　公开密钥基础设施 …… 131
7.1.1　PKI 概述 …… 131
7.1.2　数字证书 …… 133
7.1.3　CA 的组成 …… 136
7.1.4　密钥和证书的生命周期 …… 137
7.1.5　PKI 信任模型 …… 138
7.1.6　PKI 发展中的问题 …… 142
7.2　基于身份的密码学 …… 142
7.2.1　基于身份的密码学原理 …… 142
7.2.2　IBC 的方案 …… 143
7.2.3　IBC 的实际问题 …… 144
7.3　ECC 组合公钥体制 …… 145
7.3.1　CPK 相关概念 …… 146
7.3.2　ECC 复合定理 …… 146
7.3.3　标识密钥 …… 146
7.3.4　密钥的复合 …… 147
7.3.5　CPK 数字签名 …… 148
7.3.6　CPK 密钥交换 …… 148
7.3.7　安全性分析 …… 149
7.3.8　ECC CPK 小结 …… 150
思考和练习题 …… 150
实践/实验题 …… 150

第 8 章　鉴别协议 …… 151
8.1　鉴别的相关概念 …… 151
8.2　密码协议 …… 151
8.3　实体鉴别概述 …… 152
8.3.1　实体鉴别的基本概念 …… 152
8.3.2　实体鉴别和消息鉴别的区别和联系 …… 153
8.3.3　实体鉴别实现安全目标的方式 …… 153
8.3.4　实体鉴别的分类 …… 153
8.3.5　实体鉴别系统的组成 …… 153
8.3.6　实现身份鉴别系统的途径和要求 …… 154
8.4　鉴别机制 …… 154
8.4.1　口令机制 …… 155
8.4.2　一次性口令机制 …… 157
8.4.3　基于密码算法的鉴别机制 …… 158
8.4.4　零知识证明协议 …… 159
8.4.5　基于地址的机制 …… 159

8.4.6 基于设备的鉴别 …… 159
8.4.7 基于个人特征的机制 …… 160
8.5 鉴别与密钥交换协议设计中的问题 …… 160
8.6 鉴别与交换协议实例 …… 161
8.6.1 CHAP 协议 …… 161
8.6.2 S/KEY 协议 …… 162
8.6.3 Kerberos …… 163
8.6.4 X.509 鉴别服务 …… 166
思考和练习题 …… 167
实践/实验题 …… 167

第 9 章 访问控制 …… 168
9.1 访问控制的有关概念 …… 168
9.2 自主访问控制 …… 170
9.2.1 访问控制表 …… 170
9.2.2 能力表 …… 171
9.2.3 DAC 的授权管理 …… 172
9.3 强制访问控制 MAC …… 173
9.3.1 Bell-LaPadula 模型 …… 174
9.3.2 Biba 模型 …… 174
9.4 基于角色的访问控制 RBAC …… 175
9.4.1 RBAC 的概念和安全原则 …… 175
9.4.2 NIST-RBAC 参考模型 …… 176
9.5 其他访问控制策略 …… 178
9.5.1 使用控制 …… 178
9.5.2 基于任务的访问控制 …… 179
9.5.3 基于属性的访问控制 …… 180
9.6 Windows 2000/XP 的访问控制机制 …… 181
9.7 Linux 系统的访问控制机制 …… 182
思考和练习题 …… 183
实践/实验题 …… 183

第 10 章 安全电子邮件 …… 184
10.1 电子邮件原理 …… 184
10.2 PGP …… 185
10.2.1 使用 PGP 保护电子通信 …… 186
10.2.2 PGP 的密钥和密钥管理 …… 189
10.2.3 PGP 的其他功能 …… 192
10.3 S/MIME …… 193
10.3.1 RFC822 …… 193
10.3.2 MIME …… 193

10.3.3 S/MIME …… 194
思考和练习题 …… 194
实践/实验题 …… 195

第 11 章 网络安全协议 …… 196
11.1 TCP/IP 基础 …… 196
11.1.1 TCP/IP 的历史 …… 196
11.1.2 TCP/IP 层次模型 …… 196
11.1.3 IPv4 协议 …… 198
11.1.4 IPv6 数据报 …… 200
11.1.5 ARP 协议 …… 201
11.1.6 ICMP 协议 …… 202
11.1.7 TCP 协议 …… 203
11.1.8 UDP 协议 …… 204
11.1.9 TCP 和 UDP 端口 …… 204
11.2 Internet 安全性途径 …… 205
11.3 IP 的安全 …… 206
11.3.1 IPsec 概述 …… 206
11.3.2 IPsec 的文档组成 …… 207
11.3.3 安全关联 …… 208
11.3.4 鉴别头协议 …… 209
11.3.5 封装安全载荷协议 …… 211
11.3.6 安全关联组合 …… 214
11.3.7 密钥管理 …… 215
11.4 SSL/TLS …… 215
11.4.1 TLS 的体系结构 …… 216
11.4.2 TLS 的记录协议 …… 216
11.4.3 修改密码规范协议 …… 219
11.4.4 警报协议 …… 219
11.4.5 TLS 的握手协议 …… 219
11.4.6 TLS 的实现 …… 220
思考和练习题 …… 221
实践/实验题 …… 221

第 12 章 防火墙技术及应用 …… 222
12.1 防火墙概述 …… 222
12.1.1 防火墙的基本概念 …… 222
12.1.2 防火墙的作用和局限性 …… 222
12.1.3 防火墙的安全策略 …… 223
12.2 防火墙的体系结构 …… 223
12.2.1 包过滤型防火墙 …… 223

12.2.2 双宿/多宿主机模式 …… 224
12.2.3 屏蔽主机模式 …… 224
12.2.4 屏蔽子网模式 …… 224
12.3 防火墙相关技术 …… 225
12.3.1 静态包过滤防火墙 …… 225
12.3.2 状态监测防火墙 …… 229
12.3.3 应用级网关防火墙 …… 230
12.3.4 电路级网关防火墙 …… 231
12.3.5 深度包检查技术 …… 231
12.3.6 分布式防火墙 …… 232
12.3.7 其他防火墙技术 …… 233
12.4 防火墙的实现和维护 …… 233
12.5 总结和展望 …… 234
思考和练习题 …… 234
实践/实验题 …… 234
第 13 章 黑客攻击与防范技术 …… 235
13.1 认识黑客 …… 235
13.2 攻击的概念和分类 …… 235
13.2.1 攻击方式的分类原则 …… 236
13.2.2 攻击方式分类方法 …… 236
13.2.3 基于多维属性的攻击分类 …… 238
13.3 信息收集技术 …… 241
13.3.1 初始信息的收集 …… 242
13.3.2 网络地址范围的探查 …… 244
13.3.3 查找活动的机器 …… 245
13.3.4 查找开放端口和入口点 …… 246
13.3.5 操作系统辨识 …… 252
13.3.6 针对特定应用和服务的漏洞扫描 …… 253
13.4 口令攻击 …… 253
13.5 欺骗攻击 …… 254
13.5.1 IP 欺骗 …… 254
13.5.2 邮件欺骗 …… 256
13.5.3 TCP 会话劫持 …… 257
13.6 拒绝服务攻击 …… 257
13.6.1 拒绝服务攻击的类型 …… 257
13.6.2 Ping of Death …… 258
13.6.3 IP 碎片 …… 258
13.6.4 UDP 洪泛 …… 259
13.6.5 SYN 洪泛 …… 259

13.6.6 Smurf …… 260
13.6.7 Land …… 261
13.6.8 分布式拒绝服务攻击 …… 261
13.7 缓冲区溢出攻击 …… 262
思考和练习题 …… 263
实践/实验题 …… 263

第 14 章 计算机病毒及其防治 …… 264
14.1 计算机病毒的定义 …… 264
14.2 计算机病毒的基本特征 …… 264
14.3 计算机病毒的分类 …… 265
14.3.1 按照计算机病毒攻击的操作系统分类 …… 265
14.3.2 按照计算机病毒的链接方式分类 …… 266
14.3.3 按照寄生方式和传染途径分类 …… 266
14.3.4 三类特殊的病毒 …… 267
14.4 计算机病毒的命名 …… 268
14.4.1 常用的命名方法 …… 268
14.4.2 国际上对病毒命名的惯例 …… 268
14.5 计算机病毒的发展历程 …… 269
14.5.1 第一阶段 …… 269
14.5.2 第二阶段 …… 269
14.5.3 第三阶段 …… 269
14.5.4 第四阶段 …… 270
14.6 计算机病毒的基本原理 …… 271
14.6.1 计算机病毒的逻辑结构 …… 271
14.6.2 计算机病毒的工作流程 …… 272
14.6.3 计算机病毒存在的理论基础 …… 273
14.7 特洛伊木马 …… 274
14.7.1 木马的定义 …… 274
14.7.2 木马的特性 …… 274
14.7.3 木马的组成 …… 274
14.7.4 木马的类型 …… 275
14.8 计算机病毒防治对策 …… 275
14.8.1 怎样发现计算机病毒 …… 275
14.8.2 计算机病毒防治技术 …… 276
思考和练习题 …… 278
实践/实验题 …… 278

第 15 章 入侵检测技术 …… 279
15.1 入侵检测概述 …… 279
15.1.1 入侵检测的概念 …… 279

15.1.2 入侵检测的起源和发展 …… 280
15.2 入侵检测系统的功能组成 …… 280
15.2.1 信息收集 …… 280
15.2.2 信息分析 …… 281
15.2.3 结果处理 …… 281
15.3 基于主机及基于网络的入侵检测系统 …… 281
15.3.1 基于主机的入侵检测系统 …… 281
15.3.2 基于网络的入侵检测系统 …… 283
15.4 异常检测和误用检测 …… 285
15.4.1 异常检测 …… 285
15.4.2 误用检测 …… 287
15.5 入侵检测的响应 …… 287
15.5.1 针对入侵者的措施 …… 288
15.5.2 对系统的修正 …… 288
15.5.3 收集攻击者的信息 …… 288
15.6 入侵检测的标准化工作 …… 289
15.6.1 通用入侵检测框架 CIDF …… 289
15.6.2 入侵检测交换格式 …… 290
15.7 入侵防御系统 …… 290
思考和练习题 …… 290
实践/实验题 …… 290

第 16 章 信息安全评估标准 …… 291
16.1 评估标准的发展历程 …… 291
16.2 TCSEC …… 292
16.2.1 无保护级 …… 293
16.2.2 自主保护级 …… 293
16.2.3 强制保护级 …… 294
16.2.4 验证保护级 …… 295
16.3 信息技术安全评估通用准则(CC) …… 295
16.3.1 CC 的范围 …… 295
16.3.2 CC 的组成 …… 295
16.4 GB 17859—1999 …… 296
16.5 GB/T 22239—2008 …… 297
16.5.1 GB/T 22239—2008 简介 …… 297
16.5.2 《基本要求》的框架结构 …… 298
16.5.3 《基本要求》的技术要求 …… 298
16.5.4 《基本要求》的管理要求 …… 300
思考和练习题 …… 301

第 17 章 数据库系统的安全 …… 302
17.1 数据库安全基本条件和安全威胁 …… 302

17.2 数据库安全层次 …… 302
17.2.1 应用层 …… 302
17.2.2 系统层 …… 303
17.2.3 数据层 …… 303
17.3 安全数据库技术及进展 …… 304
17.4 密码学安全数据库 …… 306
17.4.1 数据库加密粒度的选择 …… 306
17.4.2 基于数据加密的访问控制 …… 307
17.4.3 秘密同态加密算法 …… 308
17.4.4 在加密数据上实现查询 …… 308
17.4.5 次序保留的加密数据库 …… 309
17.5 主要商用安全数据库 …… 310
思考和练习题 …… 311
实践/实验题 …… 311

参考文献 …… 312

第1章 绪 论

1.1 信息和信息安全的概念

1.1.1 信息的定义

信息一词，对我们都不陌生，打开电视、翻开报纸或者连上互联网就会接收到大量信息。人们每天都在接收、使用和交流信息。那么什么是信息呢？一个广义的说法是，信息就是消息。一切存在都有信息。人的五官生来就是为了感受信息的，是信息的接收器，它们所感受到的一切，都是信息。对于大量五官不能直接感受的信息，人类正通过各种手段，发明各种仪器来感知和发现它们。

1928 年，L. V. R. Hartley 在《贝尔系统技术杂志》(BSTJ)上发表了一篇题为“信息传输”的论文，在论文中，他把信息理解为选择通信符号的方式，并用选择的自由度来计量这种信息的大小。但他的定义没有涉及信息的内容、价值和统计性质。

1948 年，信息论的创始人美国数学家 C. E. Shannon 发表了一篇题为“通信的数学理论”的论文，以概率论为基础，给出了信息测度的数学公式，明确地把信息量定义为随机不定性程度的减少。Shannon 指出，通信系统所处理的信息在本质上都是随机的，可以用统计的方法进行处理，但这一概念同样没有包含信息的内容和价值。

1948 年，控制论的创始人 N. Wiener 出版了专著《控制论：动物和机器中的通信与控制问题》，从控制论的角度出发，认为信息是在人们适应外部世界，并且这种适应反作用于外部世界的过程中，同外部世界进行互相交换内容的名称。虽然这一定义包含了信息的内容与价值，但没有将信息与物质、能量区别开。

信息的定义有很多种，人们从不同侧面揭示了信息的特征与性质，但同时也存在这样或那样的局限性。

1988 年，我国信息论专家钟义信教授在《信息科学原理》一书中把信息定义为：事物运动的状态和状态变化的方式。信息的这个定义具有最大的普遍性。

1.1.2 信息的属性和价值

由于信息是事物运动的状态和状态变化的方式，而事物运动的状态和状态变化的方式是无限的，因此，信息具有无限性。

信息不是有形的自然实体，自身不能独立存在。但为了传播与被利用，它必须依附于各种载体，如图书、期刊、录音带、录像带、光盘等，同样的信息内容可以不同的载体形态出现，所以信息是无形的。

由于事物本身是不断发展变化的，随着时间和空间的推移，信息也会随之变化。此时此地信息资源价值连城，彼时彼地则可能一文不值。所以信息具有时效性。

信息并不因为分享者的人数多寡而使各自得到的信息量增或减，而是可以存储多次和传输利用的；不同的用户可以在同一时间共享同一内容的信息。