第一图书网, tushu007.com

<<应用密码学：协议、算法与C源程序（ >

图书基本信息

书名：<<应用密码学：协议、算法与C源程序（原书第2版）>>

13位ISBN编号：9787111445333

10位ISBN编号：7111445333

出版时间：2014-1

出版时间：机械工业出版社

作者：（美）Bruce Schneier

译者：吴世忠,祝世雄,张文政 等

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

内容概要

.....我所读过的关于密码学最好的书.....该书是美国国家安全局最不愿意见到出版的书.....
—— 《Wired》
.....不朽的.....令人着迷的.....计算机程序员必读的密码学上决定性的著作.....
—— 《Dr.Dobb's Journal》
.....该领域勿庸置疑的一本权威之作。

—— 《PC Magazine》
.....编码高手的圣经。

—— The Millennium Whole Earth Catalog
密码学的应用领域远远不只是编码和解码信息，要了解有关密码学技术的数字签名的知识，本书是必读之作。
本书介绍了密码学协议的通用类型、特定技术，详细介绍了现实世界密码学算法的内部机制，包括DES和RSA公开密钥加密系统。
书中提供了源代码列表和大量密码学应用方面的实践活动，如产 生真正的随机数和保持密钥安全的重要性。

全书共分四个部分，定义了密码学的多个术语，介绍了密码学的发展及背景，描述了密码学从简单到复杂的各种协议，详细讨论了密码技术。
并在此基础上列举了如DES、IDEA、RSA、DSA等十多个算法以及多个应用实例，并提供了算法的源代码清单。

全书内容广博权威，具有极大的实用价值，是致力于密码学研究的专业及非专业人员一本难得的好书。

作者简介

Bruce Schneier 是国际知名的安全技术专家，被《经济学家》（The Economist）杂志称为“安全大师”（security guru）。
他是12本安全方面技术图书的作者，还是数百篇文章、杂文和学术论文的作者。
他的有影响力的通讯“Crypto-Gram”和博客“Schneier on Security”有超过25万的读者和浏览者。
他曾在国会作证，还经常做客电视台和广播电台，并在几个政府委员会供职。
他是哈佛大学法学院伯克曼互联网和社会中心的fellow, 新美国基金会开放科技中心的program fellow, 电子前哨基金会的董事会成员，电子隐私信息中心的咨询委员会成员，以及BT（原英国电信）的安全未来学家。

书籍目录

出版者的话
译者序
Whitfield Diffie序
前言
第1章　基础知识1
1.1　专业术语1
1.1.1　发送者和接收者1
1.1.2　消息和加密1
1.1.3　鉴别、完整性和抗抵赖1
1.1.4　算法和密钥2
1.1.5　对称算法3
1.1.6　公开密钥算法3
1.1.7　密码分析4
1.1.8　算法的安全性5
1.1.9　过去的术语6
1.2　隐写术7
1.3　代替密码和换位密码7
1.3.1　代替密码7
1.3.2　换位密码8
1.3.3　转轮机9
1.3.4　进一步的读物9
1.4　简单异或9
1.5　一次一密乱码本11
1.6　计算机算法12
1.7　大数13
第一部分　密码协议
第2章　协议结构模块16
2.1　协议概述16
2.1.1　协议的目的16
2.1.2　协议中的角色17
2.1.3　仲裁协议17
2.1.4　裁决协议19
2.1.5　自动执行协议20
2.1.6　对协议的攻击20
2.2　使用对称密码系统通信20
2.3　单向函数21
2.4　单向散列函数22
2.5　使用公开密钥密码系统通信23
2.5.1　混合密码系统24
2.5.2　Merkle的难题25
2.6　数字签名25
2.6.1　使用对称密码系统和仲裁者对文件签名26
2.6.2　数字签名树27
2.6.3　使用公开密钥密码系统对文件签名27
2.6.4　文件签名和时间标记27

2.6.5 使用公开密钥密码系统和单向散列函数对文件签名28
2.6.6 算法和术语28
2.6.7 多重签名28
2.6.8 抗抵赖和数字签名29
2.6.9 数字签名的应用29
2.7 带加密的数字签名30
2.7.1 重新发送消息作为收据30
2.7.2 阻止重新发送攻击31
2.7.3 对公开密钥密码系统的攻击31
2.8 随机和伪随机序列的产生32
2.8.1 伪随机序列32
2.8.2 密码学意义上安全的伪随机序列33
2.8.3 真正的随机序列33
第3章 基本协议34
3.1 密钥交换34
3.1.1 对称密码系统的密钥交换34
3.1.2 公开密钥密码系统的密钥交换34
3.1.3 中间人攻击34
3.1.4 连锁协议35
3.1.5 使用数字签名的密钥交换36
3.1.6 密钥和消息传输36
3.1.7 密钥和消息广播37
3.2 鉴别37
3.2.1 使用单向函数鉴别37
3.2.2 字典式攻击和salt37
3.2.3 SKEY38
3.2.4 使用公开密钥密码系统鉴别38
3.2.5 使用联锁协议互相鉴别39
3.2.6 SKID40
3.2.7 消息鉴别40
3.3 鉴别和密钥交换40
3.3.1 Wide-Mouth Frog协议41
3.3.2 Yahalom协议41
3.3.3 Needham-Schroeder协议41
3.3.4 Otway-Rees协议42
3.3.5 Kerberos协议43
3.3.6 Neuman-Stubblebine协议43
3.3.7 DASS协议44
3.3.8 Denning-Sacco协议45
3.3.9 Woo-Lam协议45
3.3.10 其他协议46
3.3.11 学术上的教训46
3.4 鉴别和密钥交换协议的形式化分析46
3.5 多密钥公开密钥密码系统48
3.6 秘密分割49
3.7 秘密共享50
3.7.1 有骗子的秘密共享51

3.7.2 没有Trent的秘密共享51
3.7.3 不暴露共享的秘密共享51
3.7.4 可验证的秘密共享51
3.7.5 带预防的秘密共享52
3.7.6 带除名的秘密共享52
3.8 数据库的密码保护52
第4章 中级协议53
4.1 时间标记服务53
4.1.1 仲裁解决方法53
4.1.2 改进的仲裁解决方法53
4.1.3 链接协议54
4.1.4 分布式协议54
4.1.5 进一步的工作55
4.2 阈下信道55
4.2.1 阈下信道的应用56
4.2.2 杜绝阈下的签名56
4.3 不可抵赖的数字签名57
4.4 指定的确认者签名58
4.5 代理签名58
4.6 团体签名59
4.7 失败终止数字签名60
4.8 加密数据计算60
4.9 位承诺60
4.9.1 使用对称密码系统的位承诺61
4.9.2 使用单向函数的位承诺61
4.9.3 使用伪随机序列发生器的位承诺62
4.9.4 模糊点62
4.10 公平的硬币抛掷62
4.10.1 使用单向函数的抛币协议63
4.10.2 使用公开密钥密码系统的抛币协议64
4.10.3 抛币入井协议64
4.10.4 使用抛币产生密钥65
4.11 智力扑克65
4.11.1 三方智力扑克65
4.11.2 对扑克协议的攻击66
4.11.3 匿名密钥分配66
4.12 单向累加器67
4.13 秘密的全或无泄露68
4.14 密钥托管68
第5章 高级协议71
5.1 零知识证明71
5.1.1 基本的零知识协议71
5.1.2 图同构73
5.1.3 汉密尔顿圈73
5.1.4 并行零知识证明74
5.1.5 非交互式零知识证明75
5.1.6 一般性75

5.2 身份的零知识证明76
5.2.1 国际象棋特级大师问题77
5.2.2 黑手党骗局77
5.2.3 恐怖分子骗局77
5.2.4 建议的解决方法77
5.2.5 多重身份骗局78
5.2.6 出租护照78
5.2.7 成员资格证明78
5.3 盲签名79
5.3.1 完全盲签名79
5.3.2 盲签名协议79
5.3.3 专利81
5.4 基于身份的公开密钥密码系统81
5.5 不经意传输81
5.6 不经意签名83
5.7 同时签约83
5.7.1 带有仲裁者的签约83
5.7.2 无需仲裁者的同时签约：面对面83
5.7.3 无需仲裁者的同时签约：非面对面84
5.7.4 无需仲裁者的同时签约：使用密码系统85
5.8 数字证明邮件86
5.9 秘密的同时交换87
第6章 深奥的协议89
6.1 保密选举89
6.1.1 简单投票协议189
6.1.2 简单投票协议289
6.1.3 使用盲签名投票90
6.1.4 带有两个中央机构的投票90
6.1.5 带有单个中央机构的投票91
6.1.6 改进的带有单个中央机构的投票91
6.1.7 无需中央制表机构的投票92
6.1.8 其他投票方案95
6.2 保密的多方计算95
6.2.1 协议195
6.2.2 协议296
6.2.3 协议396
6.2.4 协议497
6.2.5 无条件多方安全协议97
6.2.6 保密电路计算97
6.3 匿名消息广播98
6.4 数字现金99
6.4.1 协议1100
6.4.2 协议2100
6.4.3 协议3101
6.4.4 协议4101
6.4.5 数字现金和高明的犯罪103
6.4.6 实用化的数字现金104

6.4.7 其他数字现金协议104
6.4.8 匿名信用卡105
第二部分 密码技术
第7章 密钥长度108
7.1 对称密钥长度108
7.1.1 穷举攻击所需时间和金钱估计109
7.1.2 软件破译机110
7.1.3 神经网络111
7.1.4 病毒111
7.1.5 中国式抽彩法111
7.1.6 生物工程技术112
7.1.7 热力学的局限性113
7.2 公开密钥长度113
7.2.1 DNA计算法117
7.2.2 量子计算法117
7.3 对称密钥和公开密钥长度的比较118
7.4 对单向散列函数的生日攻击118
7.5 密钥应该多长119
7.6 小结120
第8章 密钥管理121
8.1 产生密钥121
8.1.1 减少的密钥空间121
8.1.2 弱密钥选择122
8.1.3 随机密钥123
8.1.4 通行短语124
8.1.5 X9.17密钥产生125
8.1.6 DoD密钥产生125
8.2 非线性密钥空间125
8.3 传输密钥126
8.4 验证密钥127
8.4.1 密钥传输中的错误检测128
8.4.2 解密过程中的错误检测128
8.5 使用密钥128
8.6 更新密钥129
8.7 存储密钥129
8.8 备份密钥130
8.9 泄露密钥131
8.10 密钥有效期131
8.11 销毁密钥132
8.12 公开密钥的密钥管理133
8.12.1 公开密钥证书133
8.12.2 分布式密钥管理134
第9章 算法类型和模式135
9.1 电子密码本模式135
9.2 分组重放136
9.3 密码分组链接模式138
9.3.1 初始化向量138

9.3.2 填充139
9.3.3 错误扩散140
9.3.4 安全问题140
9.4 序列密码算法140
9.5 自同步序列密码141
9.6 密码反馈模式142
9.6.1 初始化向量143
9.6.2 错误扩散143
9.7 同步序列密码144
9.8 输出反馈模式145
9.8.1 初始化向量145
9.8.2 错误扩散145
9.8.3 安全问题146
9.8.4 OFB模式中的序列密码146
9.9 计数器模式146
9.10 其他分组密码模式147
9.10.1 分组链接模式147
9.10.2 扩散密码分组链接模式147
9.10.3 带校验和的密码分组链接147
9.10.4 带非线性函数的输出反馈147
9.10.5 其他模式148
9.11 选择密码模式148
9.12 交错149
9.13 分组密码与序列密码150
第10章 使用算法151
10.1 选择算法151
10.2 公开密钥密码系统与对称密码系统152
10.3 通信信道加密153
10.3.1 链链加密153
10.3.2 端端加密154
10.3.3 两者的结合155
10.4 用于存储的加密数据156
10.4.1 非关联密钥156
10.4.2 驱动器级与文件级加密156
10.4.3 提供加密驱动器的随机存取157
10.5 硬件加密与软件加密158
10.5.1 硬件158
10.5.2 软件159
10.6 压缩、编码及加密159
10.7 检测加密159
10.8 密文中隐藏密文160
10.9 销毁信息161
第三部分 密码算法
第11章 数学背景164
11.1 信息论164
11.1.1 熵和不确定性164
11.1.2 语言信息率164

11.1.3 密码系统的安全性165
11.1.4 唯一解距离165
11.1.5 信息论的运用166
11.1.6 混乱和扩散166
11.2 复杂性理论167
11.2.1 算法的复杂性167
11.2.2 问题的复杂性168
11.2.3 NP完全问题170
11.3 数论170
11.3.1 模运算170
11.3.2 素数172
11.3.3 最大公因子172
11.3.4 求模逆元173
11.3.5 求系数175
11.3.6 费尔马小定理175
11.3.7 欧拉φ函数175
11.3.8 中国剩余定理175
11.3.9 二次剩余176
11.3.10 勒让德符号177
11.3.11 雅可比符号177
11.3.12 Blum整数 179
11.3.13 生成元179
11.3.14 伽罗瓦域中的计算180
11.4 因子分解181
11.5 素数的产生182
11.5.1 Solovag-Strassen183
11.5.2 Lehmann183
11.5.3 Rabin-Miller184
11.5.4 实际考虑184
11.5.5 强素数185
11.6 有限域上的离散对数185
第12章 数据加密标准187
12.1 背景187
12.1.1 标准的开发187
12.1.2 标准的采用188
12.1.3 DES设备的鉴定和认证189
12.1.4 1987年的标准189
12.1.5 1993年的标准190
12.2 DES的描述190
12.2.1 算法概要191
12.2.2 初始置换192
12.2.3 密钥置换192
12.2.4 扩展置换193
12.2.5 S盒代替193
12.2.6 P盒置换195
12.2.7 末置换196
12.2.8 DES解密196

12.2.9 DES的工作模式196
12.2.10 DES的硬件和软件实现196
12.3 DES的安全性198
12.3.1 弱密钥199
12.3.2 补密钥200
12.3.3 代数结构201
12.3.4 密钥的长度201
12.3.5 迭代的次数202
12.3.6 S盒的设计202
12.3.7 其他结论203
12.4 差分及线性分析203
12.4.1 差分密码分析203
12.4.2 相关密钥密码分析206
12.4.3 线性密码分析206
12.4.4 未来的方向208
12.5 实际设计准则208
12.6 DES的各种变型209
12.6.1 多重DES209
12.6.2 使用独立子密钥的DES209
12.6.3 DESX209
12.6.4 CRYPT(3)209
12.6.5 GDES210
12.6.6 更换S盒的DES210
12.6.7 RDES211
12.6.8 snDES211
12.6.9 使用相关密钥S盒的DES213
12.7 DES现今的安全性213
第13章 其他分组密码算法215
13.1 Lucifer算法215
13.2 Madryga算法215
13.2.1 Madryga的描述216
13.2.2 Madryga的密码分析217
13.3 NewDES算法217
13.4 FEAL算法218
13.4.1 FEAL的描述218
13.4.2 FEAL的密码分析220
13.4.3 专利222
13.5 REDOC算法222
13.5.1 REDOC III222
13.5.2 专利和许可证223
13.6 LOKI算法223
13.6.1 LOKI91223
13.6.2 LOKI91的描述223
13.6.3 LOKI91的密码分析224
13.6.4 专利和许可证225
13.7 Khufu和Khafre算法225
13.7.1 Khufu225

13.7.2 Khafre226
13.7.3 专利226
13.8 RC2算法226
13.9 IDEA算法227
13.9.1 IDEA227
13.9.2 IDEA的描述228
13.9.3 IDEA的速度229
13.9.4 IDEA的密码分析230
13.9.5 IDEA的操作方式和变型231
13.9.6 敬告使用者231
13.9.7 专利和许可证232
13.10 MMB算法232
13.11 CA-1.1算法233
13.12 Skipjack算法234
第14章 其他分组密码算法（续）236
14.1 GOST算法236
14.1.1 GOST的描述236
14.1.2 GOST的密码分析237
14.2 CAST算法238
14.3 Blowfish算法239
14.3.1 Blowfish的描述239
14.3.2 Blowfish的安全性241
14.4 SAFER算法241
14.4.1 SAFER K-64的描述241
14.4.2 SAFER K-128242
14.4.3 SAFER K-64的安全性243
14.5 3-Way算法243
14.6 Crab算法243
14.7 SXAL8/MBAL算法245
14.8 RC5算法245
14.9 其他分组密码算法246
14.10 分组密码设计理论246
14.10.1 Feistel网络247
14.10.2 简单关系247
14.10.3 群结构248
14.10.4 弱密钥248
14.10.5 强的抗差分攻击和线性攻击248
14.10.6 S盒的设计248
14.10.7 设计分组密码250
14.11 使用单向散列函数250
14.11.1 Karn250
14.11.2 Luby-Rackoff251
14.11.3 消息摘要密码251
14.11.4 基于单向散列函数的密码安全性252
14.12 分组密码算法的选择252
第15章 组合分组密码254
15.1 双重加密254

15.2 三重加密255
15.2.1 用两个密钥进行三重加密255
15.2.2 用三个密钥进行三重加密256
15.2.3 用最小密钥进行三重加密256
15.2.4 三重加密模式256
15.2.5 三重加密的变型257
15.3 加倍分组长度258
15.4 其他多重加密方案259
15.4.1 双重OFB/计数器259
15.4.2 ECB+OFB259
15.4.3 xDESi260
15.4.4 五重加密261
15.5 缩短CDMF密钥261
15.6 白化261
15.7 级联多重加密算法261
15.8 组合多重分组算法262
第16章 伪随机序列发生器和序列密码263
16.1 线性同余发生器263
16.2 线性反馈移位寄存器265
16.3 序列密码的设计与分析270
16.3.1 线性复杂性271
16.3.2 相关免疫性271
16.3.3 其他攻击272
16.4 使用LFSR的序列密码272
16.4.1 Geffe发生器272
16.4.2 推广的Geffe发生器273
16.4.3 Jennings发生器273
16.4.4 Beth-Piper停走式发生器274
16.4.5 交错停走式发生器274
16.4.6 双侧停走式发生器275
16.4.7 门限发生器275
16.4.8 自采样发生器276
16.4.9 多倍速率内积式发生器276
16.4.10 求和式发生器276
16.4.11 DNRSG277
16.4.12 Gollmann级联277
16.4.13 收缩式发生器277
16.4.14 自收缩式发生器277
16.5 A5算法278
16.6 Hughes XPD/KPD算法278
16.7 Nanoteq算法278
16.8 Rambutan算法279
16.9 附加式发生器279
16.9.1 Fish发生器279
16.9.2 Pike发生器280
16.9.3 Mush发生器280
16.10 Gifford算法280

16.11 M算法281
16.12 PKZIP算法281
第17章 其他序列密码和真随机序列发生器283
17.1 RC4算法283
17.2 SEAL算法284
17.2.1 伪随机函数族284
17.2.2 SEAL的描述284
17.2.3 SEAL的安全性285
17.2.4 专利和许可证285
17.3 WAKE算法285
17.4 带进位的反馈移位寄存器286
17.5 使用FCSR的序列密码293
17.5.1 级联发生器293
17.5.2 FCSR组合发生器293
17.5.3 LFSR/FCSR加法/奇偶级联294
17.5.4 交错停走式发生器294
17.5.5 收缩式发生器295
17.6 非线性反馈移位寄存器295
17.7 其他序列密码296
17.7.1 Pless发生器296
17.7.2 蜂窝式自动发生器296
17.7.3 1/p发生器296
17.7.4 crypt(1)297
17.7.5 其他方案297
17.8 序列密码设计的系统理论方法297
17.9 序列密码设计的复杂性理论方法298
17.9.1 Shamir伪随机数发生器298
17.9.2 Blum-Micali发生器298
17.9.3 RSA298
17.9.4 Blum、Blum和Shub298
17.10 序列密码设计的其他方法299
17.10.1 Rip van Winkle密码299
17.10.2 Diffie随机序列密码300
17.10.3 Maurer随机序列密码300
17.11 级联多个序列密码300
17.12 选择序列密码300
17.13 从单个伪随机序列发生器产生多个序列301
17.14 真随机序列发生器302
17.14.1 RAND表302
17.14.2 使用随机噪声303
17.14.3 使用计算机时钟303
17.14.4 测量键盘反应时间304
17.14.5 偏差和相关性304
17.14.6 提取随机性305
第18章 单向散列函数307
18.1 背景307
18.1.1 单向散列函数的长度308

18.1.2 单向散列函数综述308
18.2 Snefru算法308
18.3 N-Hash算法309
18.4 MD4算法311
18.5 MD5算法312
18.5.1 MD5的描述312
18.5.2 MD5的安全性315
18.6 MD2算法315
18.7 安全散列算法316
18.7.1 SHA的描述316
18.7.2 SHA的安全性318
18.8 RIPE-MD算法319
18.9 HAVAL算法319
18.10 其他单向散列函数319
18.11 使用对称分组算法的单向散列函数320
18.11.1 散列长度等于分组长度的方案320
18.11.2 改进的Davies-Meyer322
18.11.3 Preneel-Bosselaers-Govaerts-Vandewalle322
18.11.4 Quisquater-Girault322
18.11.5 LOKI双分组323
18.11.6 并行Davies-Meyer323
18.11.7 串联和并联Davies-Meyer323
18.11.8 MDC-2和MDC-4324
18.11.9 AR散列函数325
18.11.10 GOST散列函数325
18.11.11 其他方案326
18.12 使用公开密钥算法326
18.13 选择单向散列函数326
18.14 消息鉴别码326
18.14.1 CBC-MAC327
18.14.2 消息鉴别算法327
18.14.3 双向MAC327
18.14.4 Jueneman方法327
18.14.5 RIPE-MAC328
18.14.6 IBC-Hash328
18.14.7 单向散列函数MAC328
18.14.8 序列密码MAC329
第19章 公开密钥算法330
19.1 背景330
19.2 背包算法331
19.2.1 超递增背包331
19.2.2 由私人密钥产生公开密钥332
19.2.3 加密332
19.2.4 解密332
19.2.5 实际的实现方案333
19.2.6 背包的安全性333
19.2.7 背包变型333

19.2.8 专利333
19.3 RSA算法334
19.3.1 RSA的硬件实现335
19.3.2 RSA的速度336
19.3.3 软件加速336
19.3.4 RSA的安全性337
19.3.5 对RSA的选择密文攻击337
19.3.6 对RSA的公共模数攻击338
19.3.7 对RSA的低加密指数攻击338
19.3.8 对RSA的低解密指数攻击339
19.3.9 经验339
19.3.10 对RSA的加密和签名攻击339
19.3.11 标准339
19.3.12 专利340
19.4 Pohlig-Hellman算法340
19.5 Rabin算法340
19.6 ElGamal算法341
19.6.1 ElGamal签名342
19.6.2 ElGamal加密342
19.6.3 速度343
19.6.4 专利343
19.7 McEliece算法343
19.8 椭圆曲线密码系统344
19.9 LUC算法345
19.10 有限自动机公开密钥密码系统345
第20章 公开密钥数字签名算法347
20.1 数字签名算法347
20.1.1 对通告的反应347
20.1.2 DSA的描述349
20.1.3 快速预计算350
20.1.4 DSA的素数产生351
20.1.5 使用DSA的ElGamal加密351
20.1.6 使用DSA的RSA加密352
20.1.7 DSA的安全性352
20.1.8 攻击k353
20.1.9 公共模数的危险353
20.1.10 DSA中的阈下信道353
20.1.11 专利354
20.2 DSA的变型354
20.3 GOST数字签名算法355
20.4 离散对数签名方案356
20.5 Ong-Schnorr-Shamir签名方案357
20.6 ESIGN签名方案358
20.6.1 ESIGN的安全性358
20.6.2 专利359
20.7 细胞自动机359
20.8 其他公开密钥算法359

第21章 鉴别方案361
21.1 Feige-Fiat-Shamir算法361
21.1.1 简化的Feige-Fiat-Shamir身份鉴别方案361
21.1.2 Feige-Fiat-Shamir身份鉴别方案362
21.1.3 例子362
21.1.4 加强方案363
21.1.5 Fiat-Shamir签名方案363
21.1.6 改进的Fiat-Shamir签名方案364
21.1.7 其他加强方案364
21.1.8 Ohta-Okamoto身份鉴别方案364
21.1.9 专利364
21.2 Guillou-Quisquater算法364
21.2.1 Guillou-Quisquater身份鉴别方案365
21.2.2 Guillou-Quisquater数字签名方案365
21.2.3 多重签名365
21.3 Schnorr算法366
21.3.1 鉴别协议366
21.3.2 数字签名协议366
21.3.3 专利367
21.4 将身份鉴别方案转为数字签名方案367
第22章 密钥交换算法368
22.1 Diffie-Hellman算法368
22.1.1 三方或多方Diffie-Hellman368
22.1.2 扩展Diffie-Hellman369
22.1.3 Hughes369
22.1.4 不用交换密钥的密钥交换369
22.1.5 专利369
22.2 站间协议369
22.3 Shamir的三次传递协议370
22.4 COMSET协议371
22.5 加密密钥交换371
22.5.1 基本EKE协议371
22.5.2 用RSA实现EKE372
22.5.3 用ElGamal实现EKE372
22.5.4 用Diffie-Hellman实现EKE372
22.5.5 加强的EKE372
22.5.6 扩充的EKE373
22.5.7 EKE的应用373
22.6 加强的密钥协商374
22.7 会议密钥分发和秘密广播374
22.7.1 会议密钥分发375
22.7.2 Tatebayashi-Matsuzaki-Newman376
第23章 协议的专用算法377
23.1 多重密钥的公开密钥密码系统377
23.2 秘密共享算法377
23.2.1 LaGrange插值多项式方案377
23.2.2 矢量方案378

23.2.3 Asmuth-Bloom378
23.2.4 Kamin-Greene-Hellman379
23.2.5 高级门限方案379
23.2.6 有骗子情况下的秘密共享379
23.3 阈下信道380
23.3.1 Ong-Schnorr-Shamir380
23.3.2 ElGamal381
23.3.3 ESIGN381
23.3.4 DSA382
23.3.5 挫败DSA阈下信道383
23.3.6 其他方案384
23.4 不可抵赖的数字签名384
23.5 指定的确认者签名386
23.6 用加密数据计算387
23.7 公平的硬币抛掷387
23.7.1 利用平方根的硬币抛掷387
23.7.2 利用模p指数运算的硬币抛掷388
23.7.3 利用Blum整数的硬币抛掷389
23.8 单向累加器389
23.9 秘密的全或无泄露389
23.10 公正和故障保险密码系统391
23.10.1 公正的Diffie-Hellman391
23.10.2 故障保险的Diffie-Hellman392
23.11 知识的零知识证明392
23.11.1 离散对数的零知识证明392
23.11.2 破译RSA能力的零知识证明393
23.11.3 n是一个Blum整数的零知识证明393
23.12 盲签名394
23.13 不经意传输394
23.14 保密的多方计算394
23.15 概率加密396
23.16 量子密码学397
第四部分 真实世界
第24章 实现方案实例402
24.1 IBM秘密密钥管理协议402
24.2 MITRENET403
24.3 ISDN403
24.3.1 密钥403
24.3.2 呼叫404
24.4 STU-III404
24.5 Kerberos405
24.5.1 Kerberos模型405
24.5.2 Kerberos工作原理406
24.5.3 凭证406
24.5.4 Kerberos第5版消息407
24.5.5 最初票据的获取407
24.5.6 服务器票据的获取407

24.5.7 服务请求408
24.5.8 Kerberos第4版408
24.5.9 Kerberos的安全性408
24.5.10 许可证409
24.6 KryptoKnight409
24.7 SESAME409
24.8 IBM通用密码体系410
24.9 ISO鉴别框架411
24.9.1 证书411
24.9.2 鉴别协议412
24.10 保密性增强邮件413
24.10.1 PEM的有关文件413
24.10.2 证书413
24.10.3 PEM的消息414
24.10.4 PEM的安全性416
24.10.5 TIS/PEM416
24.10.6 RIPEM417
24.11 消息安全协议417
24.12 Pretty Good Privacy417
24.13 智能卡419
24.14 公开密钥密码学标准420
24.15 通用电子支付系统421
24.16 Clipper422
24.17 Capstone424
24.18 AT&T 3600型电话保密设备424
第25章 政治426
25.1 国家安全局426
25.2 国家计算机安全中心427
25.3 国家标准技术所428
25.4 RSA数据安全有限公司430
25.5 公开密钥合作商430
25.6 国际密码研究协会432
25.7 RACE完整性基本评估432
25.8 对欧洲的有条件访问432
25.9 ISO/IEC 9979433
25.10 专业人员、公民自由和工业组织433
25.10.1 电子秘密信息中心433
25.10.2 电子战线基金会433
25.10.3 计算机协会434
25.10.4 电气和电子工程师学会434
25.10.5 软件出版商协会434
25.11 sci.crypt434
25.12 Cypherpunks434
25.13 专利434
25.14 美国出口法规435
25.15 其他国家的密码进出口439
25.16 合法性问题440

附录A　源代码441
参考文献484
Matt Blaze跋544

第一图书网, tushu007.com
<<应用密码学：协议、算法与C源程序（ >

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com