

<<计算机安全与密码学>>

图书基本信息

书名：<<计算机安全与密码学>>

13位ISBN编号：9787121120268

10位ISBN编号：7121120267

出版时间：2010-11

出版时间：康海姆(Alan G.Konheim)、张焕国、唐明、王后珍 电子工业出版社 (2010-11出版)

作者：(美) 康海涛 著
唐明

页数：436

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>

<<计算机安全与密码学>>

前言

21世纪是信息的时代，信息已成为重要的战略资源。

信息的获取、存储、处理和信息的安全保障能力已成为一个国家综合国力的重要组成部分。

如果信息系统的安全受到危害，将会危及国家安全，引起社会混乱，从而造成重大损失。

因此，确保信息系统的安全已成为世人关注的社会问题，并成为信息科学技术领域中的研究热点。

在信息安全科学技术的发展与应用过程中，信息安全已经发展成为一个独立的学科门类。

信息安全学是研究信息获取、信息存储、信息传输及信息处理领域的安全威胁与安全保障问题的一门新兴学科。

密码学和以计算机安全为代表的信息系统安全，是信息安全学科的重要组成部分。

发展我国信息安全事业，人才培养是关键，而人才培养的基础是教育。

目前，在我国已有70多所高等学校建立了信息安全专业。

无论是计算机安全，还是密码学，都是信息安全专业的重要学习内容。

除了高校之外，如何有效地提高我国广大计算机用户的信息安全意识及对信息安全风险的基本防护能力，已经成为我国信息安全事业中的一个十分迫切的问题。

信息安全人才培养以及信息安全意识和风险防护能力的提高，都需要实施相应的教育，因此都需要教材。

为此，我们组织翻译出版了本书。

本书的作者Alan G. Konheim是一位著名的密码专家。

他在1960年完成研究生学业后，便到IBM Thomas J. Watson研究中心成为专职研究人员，并且在其中的数学研究部门工作了22年，主要从事数学在计算机科学中的应用研究。

从20世纪60年代中期，他开始担任数学科学的密码研究计划的负责人，并领导进行了数据加密标准（DES）的评估工作。

1982年，他离开IBM Thomas J. Watson研究中心，到加利福尼亚大学圣巴巴拉分校计算机科学系担任教授。

在那里他讲授“汇编语言”、“性能评估”和“计算机网络与密码学”等课程，于2005年退休。

1981年他曾经出版《密码学初步》一书，后来又拍成电影。

他还先后在美国国家安全局和美国国防部分析研究所的通信研究分部工作过，并担任过美国国家安全局的技术顾问。

<<计算机安全与密码学>>

内容概要

《计算机安全与密码学》系统地介绍了密码学和计算机安全的基本原理及应用技术。全书的内容可划分为以下四个部分。

第一部分介绍古典密码。

第二部分探讨第二次世界大战时期的密码。

第三部分分析现代密码，主要介绍了数据加密标准（DES）、高级数据加密标准（AES）、公钥密码的原理及大整数因子分解和离散对数问题、背包公钥密码、RSA公钥密码、椭圆曲线公钥密码（ECC）等。

第四部分描述密码技术的应用，主要介绍了数字签名与认证、密钥交换、操作系统口令、电子商务保护、ATM卡和智能卡等。

为便于教学，书中给出了大量例子，并配有许多习题，参考资料可以从网站得到。

《计算机安全与密码学》内容全面，讲述深入浅出，理论结合实际，适合课堂教学和自学，是一本难得的好书。

《计算机安全与密码学》可作为研究生和高年级本科生的教材，也可供从事信息安全、计算机、通信、电子工程及电子商务等领域的科技人员参考。

<<计算机安全与密码学>>

作者简介

作者：（美国）康海姆（Alan G.Konheim）译者：唐明 王后珍 韩海清 等 合著者：张焕国康海姆(Konheim A.G.)，在1960年毕业后，我成为IBM的Thomas J.Watson研究中心（位于纽约的约克敦）的一名研究员。

在IBM数学科学部的22年中，我研究数学在计算机问题中的应用。

20世纪60年代中期开始，我成为数学加密项目的负责人；特别是针对DES算法的评价。

由于向往和我妻子Carol一同度过美丽的时光，我于1982年离开了IBM的实验室，转而接受了UCSB（加州大学圣巴巴拉分校）的教授职位。

在UCSB的24年里，我教授汇编语言、计算机网络和密码学。

我拓展了CMPSC 178（密码学导论），并且在UCSB开讲此课程21次，在以色列理工大学（位于以色列的海法）、拉特罗布大学（位于澳大利亚的墨尔本）和夏威夷大学（位于火奴鲁鲁）开讲此课程3次。

为了追求懒散的生活，我于2005年7月1日从UCSB退休。

由Wiley & Sons Inc.于1981年出版的《密码学导论》，可能被拍成了电影。

1984年我在国家安全局度过了一个夏天。

接下来的三个夏天都在国防分析研究所（位于新泽西的普林斯顿）从事通信分析的研究。

1997 ~ 1999年间我成为国家安全局的顾问。

<<计算机安全与密码学>>

书籍目录

第1章 概论 1 1.1 密码学字典 1 1.2 密码系统 3 1.3 密码分析 3 1.4 侧信息 5 1.5 thomas jefferson和m-94密码机 5 1.6 密码学及其历史 6 1.7 密码学与计算机 6 1.8 美国国家安全局 7 1.9 巨人 8 1.10 自然语言的基本特征 10 1.11 在密码分析中一个推理过程的例子 11 1.12 警告 12 参考文献 14 第2章 列移位 15 2.1 shannon对加密变换的分类 15 2.2 列移位 15 2.3 基于已知明文分析的一些示例 21 2.4 基于已知明文分析的一些示例 21 2.5 明文的语言模式 25 2.6 k维模式的计数 27 2.7 利用滑动窗口计数获得马尔可夫模型参数 28 2.8 马尔可夫得分 29 2.9 adfgvx置换系统 40 2.10 结尾 41 2.11 列移位的一些问题 42 参考文献 53 第3章 单表代替 54 3.1 单表代替 54 3.2 凯撒密码 55 3.3 利用同构的已知明文分析 56 3.4 假设的x2测试 57 3.5 同构表的裁剪 58 3.6 单表代替的部分最大可能估计 62 3.7 隐藏的马尔可夫模型 66 3.8 n维ascii的hill加密 76 3.9 高斯消元 86 3.10 问题 93 参考文献 95 第4章 多表代替 97 4.1 工作密钥 97 4.2 blaise de vigen è re密码 97 4.3 gilbert s. vernam密码 98 4.4 一次一密 99 4.5 通过相关已知周期找到vernam-vigen è re密码的密钥 100 4.6 重合 103 4.7 venona 106 4.8 多表代替问题 109 参考文献 111 第5章 统计测试 112 5.1 密码体制的弱点 112 5.2 kolmogorov-smirnov检验 112 5.3 nist提议的统计检验 113 5.4 分析判断 114 5.5 问题 117 参考文献 123 第6章 密码机的出现 124 6.1 转子 124 6.2 转子系统 125 6.3 转子的专利 126 6.4 共轭的特性 127 6.5 单转子系统的分析：仅知密文 128 6.6 排列中的位移序列 130 6.7 arthur scherbius 132 6.8 enigma机的密钥分配协议 134 6.9 enigma的密码分析 136 6.10 使用已知明文来分析enigma密文 137 6.11 the lorenz schl ü sselzusatz 139 6.12 sz40针轮 140 6.13 sz40的密码分析问题 143 6.14 使用已知明文分析sz40密文 144 参考文献 157 第7章 日本密码机 158 7.1 日语通信习惯 158 7.2 半转子 159 7.3 “红色”加密机的构造 161 7.4 基于已知明文分析“红色”加密机的密文 167 7.5 改进后的“红色”加密机的元音和辅音 174 7.6 “攀登itaka山”——战争 175 7.7 “紫色”加密机的构成 175 7.8 “紫色”加密机的密钥 180 7.9 基于已知明文分析“紫色”加密机：找出v-stepper 182 7.10 基于已知明文分析“紫色”找出c-stepper 198 参考文献 202 第8章 序列密码 203 8.1 序列密码 203 8.2 反馈移位寄存器 203 8.3 上的多项式代数 205 8.4 线性反馈移位寄存器的特征多项式 208 8.5 最大长度lfsr序列的性质 211 8.6 线性等价 215 8.7 多个线性反馈移位寄存器的组合 215 8.8 lfsr的矩阵表示 216 8.9 ascii明文序列加密的已知明文分析 217 8.10 非线性反馈移位寄存器 226 8.11 非线性密钥序列的生成 228 8.12 非规则时钟 229 8.13 rc4 232 8.14 问题 235 参考文献 235 第9章 分组密码：lucifer，des和aes 237 9.1 lucifer 237 9.2 des 240 9.3 des中的s盒、p盒和初始置换 242 9.4 des密钥安排 245 9.5 des加密的样例 247 9.6 链接 249 9.7 des是否为一个随机的映射 250 9.8 输出反馈模式的des 252 9.9 des的密码分析 253 9.10 差分密码分析 254 9.11 des攻击机 261 9.12 现在的情形 262 9.13 未来的先进数据加密标准 263 9.14 谁是胜出者 264 9.15 rijndael算法运算 265 9.16 rijndael密码 272 9.17 rijndael算法的强度：模式传播 273 9.18 一个分组密码何时安全 275 9.19 生成对称群 276 9.20 一类分组密码 278 9.21 idea分组密码 279 参考文献 280 第10章 公开密钥密码的范例 282 10.1 开始 282 10.2 密钥分发 283 10.3 电子商务 284 10.4 公钥密码系统：容易计算和难以计算的问题 284 10.5 pkc能否解决密钥分配问题 288 10.6 附笔 289 参考文献 290 第11章 背包密码系统 291 11.1 子集和背包系统 291 11.2 模运算和欧几里得算法 293 11.3 模运算背包问题 296 11.4 陷门背包 296 11.5 ascii明文的背包加、解密过程 300 11.6 merkle-hellman背包系统的密码分析(模映射) 304 11.7 丢番图逼近 309 11.8 格的短向量 312 11.9 背包密码系统类 314 11.10 习题 314 问题 314 参考文献 318 第12章 rsa密码体制 319 12.1 关于数论的题外话 319 12.2 rsa 320 12.3 使用rsa对ascii字母进行加解密的过程 321 12.4 对rsa的攻击 325 12.5 rsa的williams变种 325 12.6 多精度模运算 329 参考文献 330 第13章 素数和因子分解 331 13.1 数论和密码学 331 13.2 素数和埃拉托色尼筛法 331 13.3 pollard的p-1方法 333 13.4 pollard的p-算法 334 13.5 二次剩余 337 13.6 随机因子分解 341 13.7 二次过筛法 342 13.8 整数的素性检测 344 13.9 rsa的挑战 346 13.10 完全数和mersenne素数 347 13.11 多精度运算 348 13.12 习题 349 参考文献 351 第14章 离散对数问题 352 14.1 模p的离散对数问题 352 14.2 已知p-1的因子，求解模p的dlp的方法 353 14.3 求解离散对数的adelman亚指数算法 356 14.4 大步小步算法 357 14.5 index-calculus算法 357 14.6 pollard- 算法 360 14.7 扩域 362 14.8 离散对数的研究进展 364 参考文献 364 第15章 椭圆曲线密码学 365 15.1 椭圆曲线 365 15.2 实数域上的椭圆群 366 15.3 lenstra的因子分解算法 367 15.4 (p > 3)上的椭圆群 368 15.5 域上的椭圆曲线 370 15.6 椭圆曲线群中的计算 371 15.7 超奇异椭圆曲线 374 15.8 利用椭圆曲线实现diffie-hellman密钥交换协议 375 15.9 menezes-vanstone椭圆曲线密码系统 375 15.10 椭圆曲线数字签名方

<<计算机安全与密码学>>

法 377 15.11 certicom挑战 377 15.12 美国国家安全局与椭圆曲线密码体制 378 参考文献 378 第16章 网络中的密钥交互 379 16.1 网络中的密钥分配 379 16.2 美国专利770 379 16.3 欺骗 380 16.4 diffie-hellman协议的扩展el gamal协议 381 16.5 shamir提出的自治密钥交换协议 383 16.6 x9.17密钥交换结构 384 16.7 needham-schroeder密钥分配协议 386 参考文献 392 第17章 数字签名和认证 393 17.1 签名的必要性 393 17.2 对网络交易的威胁 393 17.3 保密、数字签名和认证 394 17.4 数字签名的要求 395 17.5 公钥密码和签名系统 395 17.6 rabin的二次剩余签名协议 396 17.7 hash函数 397 17.8 md5 399 17.9 安全hash算法 400 17.10 nist的数字签名算法 401 17.11 el gamal的签名协议 402 17.12 fiat-shamir身份认证和签名方案 402 17.13 不经意传输 404 参考文献 405 第18章 密码学应用 406 18.1 unix的口令加密 406 18.2 磁条技术 408 18.3 保护atm机的交易 409 18.4 基于密钥的访问控制卡 415 18.5 智能卡 416 18.6 你能相信谁：kohnfelder证书 418 18.7 x.509认证协议 419 18.8 安全套接层 421 18.9 在网络上进行安全的信用卡支付 425 参考文献 427 第19章 密码的相关专利 428 19.1 什么是专利 428 19.2 取得专利的可能性的想法 428 19.3 专利的格式 429 19.4 可取得专利权与不可取得专利权的主题 430 19.5 侵权 430 19.6 专利在密码技术中的角色 431 19.7 美国专利3 543 904 431 19.8 美国专利4 200 770 432 19.9 美国专利4 218 582 433 19.10 美国专利4 405 829 433 19.11 pks/rsadsi诉讼 434 19.12 leon stambler 435 参考文献 436

<<计算机安全与密码学>>

章节摘录

插图：

<<计算机安全与密码学>>

编辑推荐

《计算机安全与密码学》：国外计算机科学教材系列

<<计算机安全与密码学>>

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>