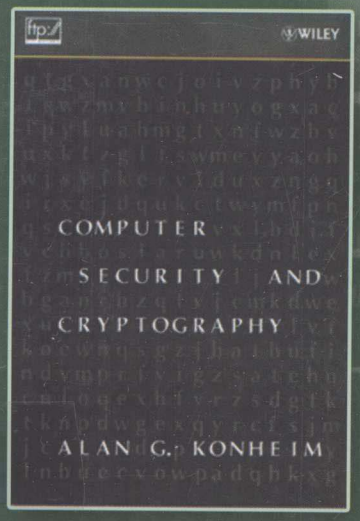
国外计算机科学教材系列

WILEY

计算机安全与密码学

Computer Security and Cryptography



[美] Alan G. Konheim 著

唐 明 王后珍 韩海清
李春雷 童 言 杨 启 译
张焕国 审校

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

国外计算机科学教材系列

计算机安全与密码学

Computer Security and Cryptography

[美] Alan G. Konheim 著

唐 明 王后珍 韩海清
李春雷 童 言 杨 启 译

张焕国 审校

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

内 容 简 介

本书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。

本书内容全面，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。本书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。

版权贸易合同登记号　图字：01-2009-1383

图书在版编目(CIP)数据

计算机安全与密码学/(美)康海姆(Konheim, A. G.)著；唐明等译. —北京：电子工业出版社，2010.11
(国外计算机科学教材系列)
书名原文：Computer Security and Cryptography
ISBN 978-7-121-12026-8

I. ①计… II. ①康… ②唐… III. ①电子计算机－安全技术－高等学校－教材②电子计算机－密码术－高等学校－教材 IV. ①TP309

中国版本图书馆 CIP 数据核字(2010)第 202029 号

策划编辑：谭海平
责任编辑：史　平
印　　刷：涿州市京南印刷厂
装　　订：涿州市桃园装订有限公司
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：28.25　　字数：755 千字
印　　次：2010 年 11 月第 1 次印刷
定　　价：55.00 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。

译 者 序

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。

从 1983 年到 2005 年，本书曾作为加利福尼亚大学计算机科学系研究生的高级选修课的教科书。选修该课程的学生包括计算机科学系、电气和计算机工程系以及数学系的学生。

由于作者在计算机安全与密码学方面具有广泛的工作经历和长达几十年的科研教学成果积累，使得本书的内容十分丰富，既有深入的理论分析，又有实际的应用技术。本书系统地介绍了密码学和计算机安全的基本原理和应用技术。全书的内容可以划分为以下四个部分。第一部分介绍古典密码，详细讨论了古典密码的设计原理和典型算法，以及古典密码的分析方法等。第二部分探讨第二次世界大战时期的密码，详细介绍了第二次世界大战时期德国和日本的密码和密码机及其分析方法等。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 公钥密码及椭圆曲线公钥密码(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。为了便于教学，书中给出大量例子，并配有许多习题，参考资料可以从如下网站得到：//ftp.wiley.com/public/sci_tech_med/computer_security。

本书内容全面，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。本书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。

本书的第 1 章、第 5 章、第 8 章、第 9 章、第 16 章、和第 18 章由唐明翻译，第 14 章和第 15 章由王后珍翻译，第 2 章、第 3 和第 4 章由李春雷翻译，第 17 章和第 19 章由韩海清翻译，第 11 章由王后珍和韩海清翻译，第 10 章、第 12 章和第 13 章由童言翻译，第 6 章和第 7 章由杨启翻译，全书由张焕国统稿和校审。研究生李幼名、黎勇和邓惠参与了书稿的整理工作。

由于译者的专业知识和外语水平有限，书中错误在所难免，敬请读者指正，译者在此先致感谢之意。

译者于武汉珞珈山

2010 年 7 月

序　言

成为一名密码学作者并不容易，事实上，作为一名作者，本就不容易。你必须思考想涉及的是什么样的学科。然后，必须决定以什么顺序表述它们。但绝非这么简单，因为最好的逻辑推演并不常是最适合教学的。接着就出现了最难的一部分：必须在空白的纸或者表格填上有意义的字母和数字。

Alan Konheim 为此吃过许多次苦头。他写了很多篇技术文章，这表明他已经在技术上掌握了该学科。而且他著名的《密码学导论》一书一度通过了著作权认定。在接下来的几年中，他体会到了那本书上什么真正起到了作用，而什么没有，并且将之运用到工作上，产生了一种良好的教学方法。

几个世纪以来，不言自明的是加密者和解密者必须有同样的密钥，只是作用相反而已。公开密钥加密技术的发明消除了这个公理。它已经改变了密码学的实际应用，为其注入了新的活力。其中许多一直扎根于古典的、对称的或系统的密码学。通信行业的巨大扩张也将其子领域——保密通信带进了一个巨大的新的发展空间。曾经属于军队、外交官和间谍的专属领域密码现在已经变得无处不在。人们在没有意识到的情况下使用它。例如，每次某个人使用自动柜员机(ATM)的时候，他的事务处理都是加密的。网上银行交易也是如此。任何时候任何人把他的电子银行卡号安全地发送给 E-bay 或 Amazon，他们都要使用密码。这个领域已经走出了隐秘状态。美国国家安全局曾经被神秘地对外宣称是“不存在的部门”，而现在电影和晚间新闻里经常出现 CIA 和 FBI 等字眼。“9.11”之后，布什政府的无证监听更是进一步使密码学、NSA 和隐私这样的词汇出现在公众视野中。密码学研究学会每年出 4 次期刊。长期笼罩它的神秘迷雾已渐渐被主导它的数学逻辑所驱散。Alan Konheim 知道这一切，因为他当时正是 IBM 关于密码学领域的领导者，并且一直紧跟这一领域的最新发展，从而在其文章中展示这些进展。他的教学经验告诉他，学生们有可能会提出什么样的问题，以及他们在理解的过程中会遇到什么问题。他以前的写书经验教会他如何有效地解释复杂的问题，写作质量和恰到好处的写作范围，使得这本书十分优秀。密码学领域的初学者和老手们都会像我一样喜欢它。

David Kahn

前　言

国家安全和计算机安全

2001 年 9 月 11 日，“安全”这个词进入了美国人民民族意识的最显著位置。直至现在仍是如此。2004 年的总统选举在很大一方面是根据哪个候选人被认为最能控制保障全美国人民的安全所决定的。某些极端主义团体表达出对美国生活及文化的憎恨，美国人对此很是疑惑不解。美国国家安全局/中央安全局的任务包括保护美国的通信安全及采集外国的情报。

尽管密码学在这些领域都发挥着十分重要的作用，但本书并不涉及此方面的内容。本书探讨的是密码学在我们日常生活中发挥的作用。现在没有什么活动不依靠计算机进行。由于自动提款机方便而又实用，导致旅行支票的使用越来越少。银行和信用卡公司存储并维护着大量数据，而这些机构对用户数据管理不善的新闻经常出现。身份窃取正逐渐盛行。信用卡公司现在敢于为身份窃取的保险做宣传广告，以此保护他们在法律上有义务捍卫但却保卫不了的信息。

密码学在很多领域发挥作用。但是就像座椅的安全带一样，它不能完全保护我们。在接下来的章节中，我将提出有关加密的基本思想，然后阐明一些与之相互配合来保护我们的方法。

为什么要学习密码学

密码学和高性能计算系统之间存在共生关系。当代计算机在 20 世纪密码专家的指令下创造出来。随着加密系统的作用对象从机械转变到电子系统上，其复杂性提升了，所以也需要制定更有效的方法，用密码分析法破译它。

每个加密系统都有有限数量的密钥，一般都能被试验分析出来。方法就是用所有可能的密钥解密密文，直到出现一些可识别的文本。在很多经典的加密系统中，密钥的测试可以手动操作。激励计算机发展的因素正是能够测试所有可能的密钥来解密密码的需求。现代密码体制的情况是，可能的密钥数目太大，以至于对它们穷举试验不可行，即便使用计算机也是有限制的。而且为了成功，在密钥测试前必须先做一些分析。

计算机和密码学的结合为数学提供了非凡的实际应用，同时发展了作为工程与科学的基本原理的推理能力。当一位学生第一次查看下面这段密文：

To-drijohrunurmanpmlgchd-ehapuotp,te-nmabsno-nitioippmbo-a-a

sTasm-h-op-ms-vye-m.ikndu-n-atscegnetoin-l-rs-v-e-u-ta-olati

s-t-sccw——eorrgdhgngP.r-stenvercenhnerhchoie-nun-sr-tois-rma

eaeeadadrssou-o-etat-iefeotifc-m-a——ergua-eiuo-oixeordalmyes

他会觉得很疑惑。虽然可以发现一些单词碎片，但是怎么才能恢复原文呢？当学生学会审慎地研究密文后，往往能破译它。密码学教会学生，他们可以多么聪明。当然，老师应该像教育部的电视广告那样告诫他们的学生：如果他们在研究一篇密文上花费超过 4 个小时，那就应该寻求导师的帮助。

虽然计算机安全今天肯定是一个热门话题，但公众讨论往往伴随了大量天花乱坠的描述。人们对密码学印象深刻，新闻发布时肆意使用“牢不可破”这个术语。1924 年发明的

手动密码机 Kryha 拥有超过 4.57×10^{50} 个密钥，但它并不能提供很好的安全保护。调用很多经验知识来“证明”一个加密方案强度的方法，通常不能衡量它的真正强度。

本书为了解数据安全的中心问题提供了工具。为讲师提供了广泛的主题，以此培养学生能够批判性地评价各种影响保密、身份认证和数字签名的有效性因素，使学生对决定算法强度和协议履行的因素变得敏感，为学习密码分析的学生提供实际动手操作的经验。

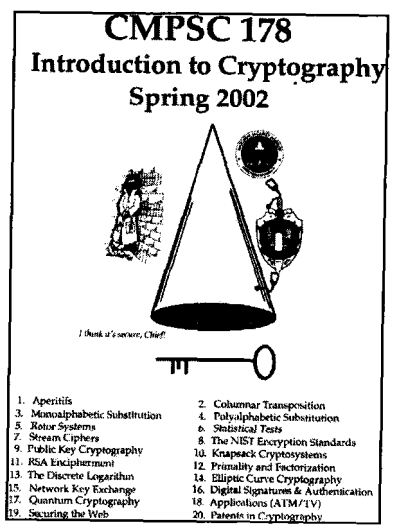
这本书的目的是解释保密的本质，以及密码学在提供保密及其派生物(身份验证和数字签名)时的实际限制。

我所掌握的技术

本书的部分内容已经用做 UCSB 的 CMPSC 178 的教科书(《密码学导论》)。从 1983 年到 2005 年，这是圣巴巴拉市加利福尼亚大学计算机科学系本科计划中的高年级选修课程。CMPSC 178 是十周四个单元的课程。课堂讲座是由一位助教主持的课程讨论。CMPSC 178 一般由大三、大四的计算机科学系、电子和计算机工程系以及数学系的学生参加，预备的先修科目是 CMPSC 10(Java 编程语言课程)和 PSTAT 120A 或 121A(概率和统计的入门级课程)。

8~9 个作业要求学生编程实现各种密码体制的密码分析及其他与密码相关的题目。虽然在课堂上我分发了一份密文作业的硬拷贝，但是密文的性质要求学生必须从我的网站上复制密文文件。在计算机安全和密码学课程中也要遵循着相同的步骤，作为练习的密文可以从 Wiley 的网站 ftp://ftp.wiley.com/public/sci_tech_med/computer_security 下载。

右侧是我的“CMPSC 178 Reader”一书封面的副本。我的一位同事说我的纽约式幽默不会被加州的学生理解。他们可能将会无法掌握椭圆曲线加密的意义，但是显然许多人研究到深夜后理解了。



我在 1997 年取消了课堂上的期中和期末考试，因为没有课程内的问题可以真正用来在课堂上检测学生。取而代之，我要求他们交一份学期论文，论文题目由学生自己选择，然后由我审核批准。学期论文是基于来自至少两篇论文的相关材料的一些密码学主题的简短报告(10 页以下)。学期论文不必只包含一个单一方程或只涉及理论问题。事实上，我鼓励学生寻找在本质上具有历史性的主题，这些主题涉及实际应用或社会问题。学期论文必须包括一份对论文的总结和学生对论文贡献的评价。学期论文在最后一堂课上交。我提供了参考材料的清单，而网络提供了更广泛的主题和材料的来源。

除了介绍性的材料，厚实的数学背景也是必要的，包括概率论和统计学。现代密码学在很大程度上取决于数论的基础知识，但是大多数工程专业和计算机科学专业的学生没有这样的准备。如果这种数学背景被强加作为前提，潜在的读者又会减少。因此，我在课程中增加了相应的数学主题。

该课程大纲会在第一讲的课堂上布置，这也许是该课程范围的一种扩展。

《计算机安全与密码学》是“CMPSC 178 Reader”的扩展版本。经修改后，它变得更加适合广泛的读者。教师应为学生选择对应他们兴趣的那些课程。

本书的组织

书中有三种类型的章节：

1. 发展技术细节的内容。
2. 描述一个密码系统和说明分析方法的内容。
3. 描述一个密码系统、说明分析方法及提供用来测试学生理解程度的问题的内容。

经典密码学

1. Aperitifs 密码
2. Columnar 置换密码
3. 单一字母替换密码
   (a) Cribing&Scoring 单一字母替换
   (b) 希尔替换
   (c) 马尔可夫加密模型
4. 多字母替换密码
5. 统计检验密码

二战密码

6. 密码机的出现
   (a) 德国 Enigma 密码机(德国转轮密码机)
   (b) Lorenz Schlusselzusatz(Lorenz 的机械式一次一密密码)
7. 日本密码机
   (a) 日本 RED 密码机
   (b) 日本 PURPLE 密码机

现代密码学

8. 流密码
9. NIST 加密标准
   (a) LUCIFER
   (b) DES
   (c) AES
   (d) 分组密码设计
10. 公共密钥密码学范式
11. Paragigm 密码体制
12. RSA 密码体制
13. 素数和整数分解
14. 离散对数问题
15. 椭圆曲线密码体制
16. 密钥在网络上的交换
17. 数字签名和认证
18. 应用密码学

(a) UNIX 口令
(b) ATM 卡
(c) 安全接口和智能卡
(d) 保护网(电子商务)
19. 密码学专利

致谢

我亏欠了许多人，也就是那些帮助和鼓励我完成这本书的人。

- 我 46 年的同事和朋友，近日从 IBM Thomas J. Watson 研究中心(Yorktown Heights, New York)退休的 Roy L. Adler 博士。他读了本书的各章节，并为我提供了 IBM 加密工作的大量可靠的材料。
- 我 36 年的同事和朋友，乔治·华盛顿大学名誉教授 Raymond Pickholtz 博士。他拜访 UCSB 数次，阅读了本书的所有章节并提供了建议。
- I. Benjamin Blady 先生和 Sara Beth Mitchell 夫人，他们非常好地替我完成了第 19 章密码学专利的编写。
- 我的儿子 Keith，他在图形图像方面帮助了我许多；还有我的儿子 Jay，他简化了我从 MAC 到 PC 转换的工作；以及我的儿子 Seth，他读了本书前面的一些章节并明智地催促我调整自己的思路。
- Carol，陪伴我近 50 年的妻子，我对她广泛的才能感到惊讶。没有她的鼓励、支持与建议，我是无法完成这本书的。

我已经在 UCSB 修改 CMPSC 178 有 21 次了，在澳大利亚、以色列和夏威夷还各有一次。这是一个从学生的问题、建议和批评中获得的好处。1842 年，在 Penses, Essais, Maximes et Correspondanee J. Joubert，法国哲学家 Joseph Joubert 说过：教学是第二次学习！

Alan G. Konheim

作 者 简 介

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。

目　录