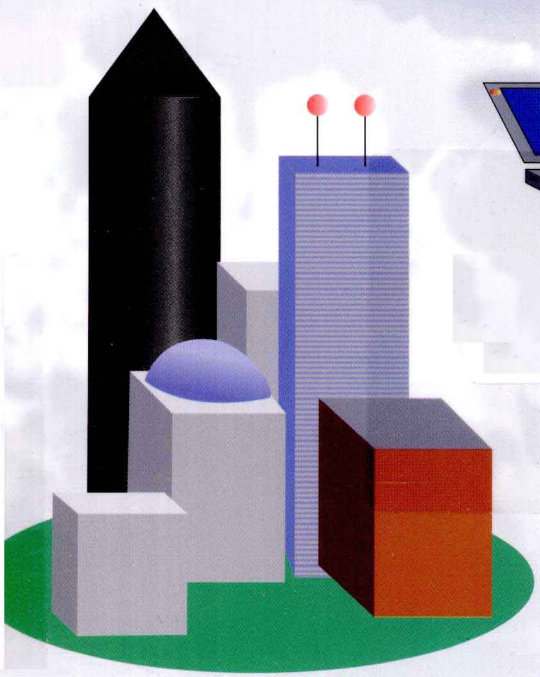
高等教育“十一五”国家级规划教材

Applied Cryptography

应用密码学

（第2版）

胡向东　魏琴芳　胡蓉　编著



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

高等教育“十一五”国家级规划教材

应用密码学

（第2版）

胡向东　魏琴芳　胡　蓉　编著

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

内 容 简 介

本书第 1 版为高等教育“十一五”国家级规划教材，是作者从事多年的应用密码学相关教学和科研工作实践的结晶。本书全面介绍了应用密码学的基本概念、基本理论和典型实用技术。全书共 17 章，内容涉及密码学基础、古典密码、密码学数学引论、对称密码体制、非对称密码体制、HASH 函数和消息认证、数字签名、密钥管理、流密码，以及密码学的新进展；书中还介绍了密码学在数字通信安全、工业网络控制安全、无线传感器网络感知安全、无线射频识别安全，以及电子商务支付安全等典型领域的应用方法和技术。语言简练，内容重点突出，逻辑性强，算法经典实用；突出的特色是将复杂的密码算法原理分析得深入浅出，着重培养现代密码学方面的工程应用技能，便于读者花少量的时间入门并尽快掌握应用密码学的精髓。

本书可作为高等院校密码学、应用数学、信息安全、通信工程、计算机、信息管理、电子商务、物联网、网络化测控等专业高年级本科生和研究生教材，也可供从事网络和通信信息安全相关领域应用和设计开发的研究人员、工程技术人员参考；尤其适合对学习密码学感到困难的初学者。

图书在版编目（CIP）数据

应用密码学 / 胡向东，魏琴芳，胡蓉编著. —2 版. —北京：电子工业出版社，2011.5
ISBN 978-7-121-13290-2

Ⅰ. ①应… Ⅱ. ①胡… ②魏…③胡… Ⅲ. ①密码－理论 Ⅳ. ①TN918.1

中国版本图书馆 CIP 数据核字（2011）第 062753 号

策划编辑：康 霞（kangxia@phei.com.cn）
责任编辑：康 霞
印 刷：北京天宇星印刷厂
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：24 字数：615 千字
印 次：2011 年 5 月第 1 次印刷
印 数：4 000 册 定价：46.00 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。

序

随着信息化在全球的发展，互联网、电信网、广播电视网正在走向三网融合，计算机、通信、数码电子产品也朝着3C融合的方向发展，人们的社会生活对网络的依赖越来越大，信息及信息系统的安全与公众利益的关系日益密切。当人类面对荒蛮外界时，人身安全是第一需求，人们需要相互传授安全防范的经验和技能。当人类步入信息社会之时，我们不难发现信息安全还是我们的第一需求，而且现在比过去任何时候都更需要普及信息安全的意识和知识。只有当这种意识和知识为工程技术人员真正掌握，并为公众所接受，整个社会的信息安全才有可靠的保障。

自50多年前香龙的“保密通信的信息理论”一文问世以来，密码学逐步从经验艺术走上了严谨科学的道路，成为了当今社会信息安全技术的坚实基石。不了解密码学，也很难真正驾驭信息安全。另一方面，互联网等当代信息技术领域提出的一系列信息安全新课题（其中许多还是有趣的科学问题和严肃的社会问题）反过来又推动着密码学不断深入发展和广泛应用，使密码学洋溢着生机和魅力。

密码学及其应用是跨学科的交叉研究领域，其成果和思想方法的意义已经不限于数学，甚至也不仅仅限于信息安全。国外从20世纪70年代起，密码和编码理论及技术逐渐成为许多工程学科的基础课程。事实上，它们不仅对理工科学生的训练有益，法律、管理等文科的学生也能从中吸收到思想和心智的知识养分。

现代密码学的确是建立在数学理论的基础之上的，但使用它的人绝不限于数学家，当代工程技术人员对它的需求也许更为迫切，它的应用和发展更需要普及和深入到越来越多的交叉领域中去。为了能够达到精确、简洁、优美的目的，密码学常常需要从形式化的数学层面来刻画；同时密码学也需要人们从工程应用的角度来理解它，甚至需要从逻辑常识和宽广的知识背景的角度来介绍它和思考它，才能领会它的精髓，丰富它的内涵，灵活它的使用。

然而由于历史原因，适合工程技术人员的密码学中文教程相对较少，现代密码学的抽象形式使许多其他专业背景的人对它望而生畏，这就阻碍了它精妙思想和方法的普及。今天，网络安全等领域提出了越来越多的密码技术应用问题，客观上对应用密码学这种体裁的专著有了更广泛、更迫切的需要。

《应用密码学》使工科背景的读者多了一个选择，在一定程度上弥补了上述遗憾。这本书的许多内容来源于作者在工程学科的密码学教学实践，注重从工程技术人员和学生易于接受的方式来介绍密码学的要领，不拘泥于细腻的理论证明和形式上的严谨。书中的一些重点章节还设置了许多有价值的具体实例，全书配有计算机CAI教学课件，这些对读者当不无裨益。针对当前网络安全的热点问题，作者在书中也适时地介绍了一些新的典型应用，抛砖引玉，使书的内容增色不少。

本书似在追求一种信念：更多人的实践和思考有助于推动密码学的发展，多种风格、面向多种应用领域的应用密码学知识能够为密码学大厦添砖加瓦。读后有感，是为序。

中国科学院成都计算机应用研究所研究员、博导

2011.3

前　言

本书第1版是高等教育“十一五”国家级规划教材。已先后被东华大学、上海交通大学、中山大学、湖南大学、山东大学、贵州大学、黑龙江大学、西南科技大学、桂林电子科技大学、内蒙古科技大学、烟台大学、解放军信息工程大学、海军舰艇学院、北京工业大学、南京工业大学、湖北工业大学、安徽师范大学、杭州师范大学、曲阜师范大学、成都东软信息技术职业学院等国内数十所高校选用。

该教材经过近四年的教学实践，其间积累了较丰富的教学经验；同时，国内的网络通信与信息技术应用得到了快速发展，如“工业化与信息化融合”、“传感网、物联网、云计算等国家新兴战略性产业的兴起”，“智慧地球”、“传感中国”等理念的提出，第三次信息技术浪潮呼之欲出。信息技术正在快速地改变着人们的工作模式和生活习惯，越来越多的信息安全问题如影随行，密码学在信息安全中的重要地位与日俱增。

本书的目标定位和特色

为了更好地适应教学工作的需要，也为了更好地展现密码学的核心内容与典型应用，在征集学生和教师等广大读者意见的基础上，结合新的教学目标定位与密码技术应用需要，对《应用密码学》第一版的内容进行了系统优化与全面梳理，在充分保留第1版“先进性”、“典型性”、“易学性”、“有趣性”等特色基础上，在新版中力图重点体现以下特色：

（1）**本书定位于突出现代密码学原理和方法的工程应用。**主要面向工科电气信息类专业学生和一般工程技术人员；着眼于介绍现代密码学的基本概念、基本原理和典型实用技术，不涉及复杂的数学推导或证明。方便读者“学以致用”、突出培养读者现代密码学方面的工程技能是本教材的基本追求。

（2）**本书旨在以读者易于理解和掌握的方式构建教材内容体系，表述密码学知识。**许多读者（特别是初学者）对密码学知识学习起来感觉非常困难，本书基于作者多年的教学实践经验积累，对读者学习需求和本教材的重难点有非常准确的把握，因此，编著本书重在方便读者掌握现代密码学基本知识后的工程应用，重在引导读者用少量的时间尽快掌握应用密码学的核心内容，提高学习效率，在内容的安排和密码算法的选取方面特别设计，内容重点突出、算法经典实用。同时，针对读者难以理解和掌握复杂的密码学数学知识问题，本书在表述上删繁就简，紧盯核心，将算法原理与举例紧密结合，且例题求解过程具体明了，深入浅出的介绍确保读者学习轻松自如。

（3）**本书努力追求使读者对应用密码学知识具备触类旁通，举一反三的能力。**任何课堂教学或教材都具有一定的学时或篇幅局限性，另一方面，许多密码算法具有相似的原理，因此，本书不会、也不可能追求内容上的面面俱到，而是以精选的具有良好代表性的经典、实用密码算法为对象，力争从工程应用的角度把密码学基本原理讲清楚、讲透彻，并深入分析它们在多个不同典型领域中的应用方法，以此推动“学用结合”、“能力与素质并进”；对密码

学典型算法和密码学基本知识及其应用的剖析，这是一种方法学，读者在深入理解与把握的基础上，将学会分析问题和解决问题的方法，具备继续深造、触类旁通、举一反三的能力，这正是本书希冀达到的最重要的目标！

本书的组织

本书从密码故事开始，全面介绍了应用密码学的基本概念、基本理论和典型实用技术。结构上分为密码学原理、密码学应用与实践两大部分；全书共 17 章，内容涉及密码学基础、古典密码、密码学数学引论、对称密码体制、非对称密码体制、HASH 函数和消息认证、数字签名、密钥管理、流密码以及密码学的新进展；书中还介绍了密码学在数字通信安全、工业网络控制安全、无线传感器网络感知安全、无线射频识别安全以及电子商务支付安全等典型领域的应用方法和技术。每章末都给出了适量的思考题和习题作为巩固知识之用，并附有参考答案。为了方便使用，对于较高要求的部分用符号“*”标识。

教师可在 48～64 学时内讲解全部或选讲部分内容，还可以配以适当的上机操作进行动手实践，在有限的时间内快速掌握应用密码学的核心内容，提高学习效率。

本书另配有相应的 CAI 课件和两个密码故事片，请从 http://www.hxedu.com.cn 免费下载。

第 2 版修订的内容

（1）删。本书删除了第 1 版中不易理解且不影响密码学基本知识介绍的部分内容，包括最优化正规基表示的 $GF(2^m)$ 域、AES 的 Square 结构，以及椭圆曲线密码体制部分与最优化正规基相关的例题、量子测不准原理的数学描述。

（2）增。为了使全书的内容体系更完善，新增了密码故事、密码学与无线射频识别安全、安全机制与安全服务之间的关系、P 盒的分类、SMS4 算法 A5/1 算法、Kerberos 等。

（3）改。为了使全书的内容更优化、表述更容易理解，这一方面涉及的变化较多，主要包括密码学的发展历史、安全攻击的主要形式、密码分析的分类、网络通信安全模型、非对称密码模型、代替与换位密码、欧几里德算法、群的概念、分组密码的操作模式、DES、AES 的举例、RSA 算法的有效实现、RSA 的数字签名应用、ECC 的举例、SHA-512 中例题的寄存器值变化过程、数字签名的特殊性、流密码模型、RC4 算法的伪码描述、PGP 的密钥属性、数据融合安全等。

本书的适用对象

本书可作为高等院校密码学、应用数学、信息安全、通信工程、计算机、信息管理、电子商务、物联网、网络化测控等专业高年级本科生和研究生教材，也可供从事网络和通信信息安全相关领域管理、应用和设计开发的研究人员、工程技术人员参考；尤其适合对学习密码学感到困难的初学者。

致谢

本书由重庆邮电大学胡向东教授组织编著，第3、4、10、12章由魏琴芳编著，第15章由胡蓉编著，其余章节的编著、CAI课件和习题答案的制作由胡向东、张玉函、汤其为、白润资、丰睿、余朋琴、万天翔等完成，胡向东负责全书的统稿。作者要特别感谢参考文献中所列各位作者，包括众多未能在参考文献中一一列出资料的作者，正是因为他们在各自领域的独到见解和特别的贡献为作者提供了宝贵的资料和丰富的写作源泉，使作者能够在总结教学和科研工作成果的基础上，汲取各家之长，形成一本定位明确、适应需求、体现自身价值、独具特色并广受欢迎的应用密码学教材。电子工业出版社的康霞编辑等为本书的高质量出版倾注了大量心血，在此对他们付出的辛勤劳动表示由衷的感谢。本书的编著出版受到重庆市科委自然科学基金计划项目（CQ CSTC 2009BB2278）和国家自然科学基金项目的资助。

应用密码学地位特殊、若隐若现、内涵丰富、应用广泛、发展迅速，对本书的修订再版是作者在此领域的再一次努力尝试；限于作者的水平和学识，书中难免存在疏漏和错误之处，诚望读者不吝赐教，以利修正，让更多的读者获益。我们的联系方式是：huxd@cqupt.edu.cn。

编著者

2011年3月

目　录

开篇　密码学典故

上篇　密码学原理

开篇　密码学典故

第0章　密 码 故 事

密码学是一门古老而年轻的科学，密码学经历了几千年的演化与发展，形成了丰富的内涵，并得到了广泛的应用。密码学起源于信息隐藏，就是为了达到机密信息不被非授权地获知的目的而采取的某种手段或方式；现代密码学主要基于数学或物理的方法进行某种变换来实现。密码学曾经高深莫测、讳莫如深，主要用于国家外交或军事等重要领域；现在密码学与百姓的平常生活和工作息息相关，已成长为网络信息安全的基石；密码学在长期的发展过程中衍生出了许多或惊险刺激、或温婉动人的故事。为了激发出读者浓厚的兴趣以学好这门课程，我们就从“讲故事”开始吧。

0.1　重庆大轰炸背后的密码战[1]

1938 年 4 月的一个上午，山城重庆大雾弥漫。国民党密电组组长、无线电专家魏大铭看着桌上摆放的一沓密码电报，一筹莫展。就在刚才，他又一次接到国民党军事委员会技术研究室的通知，责令密电组尽快对截获的神秘电码进行破译。

早在 2 月 18 日上午，密电组就截获了一份由潜伏在重庆的日本间谍发出的密码电报。该电报以杂乱排列的日文字母呈现出前所未有的编码方式。密码员还未来得及反应，十几份类似的电报随着长短声的交错，出现在他们的眼前。密电组的破译专家们立刻投入到紧张的工作中。半个小时过去了，密电破译依然毫无头绪。这时，城市上空传来了由远及近的飞机轰鸣声。尖厉的空袭警报响彻重庆上空。9 架日军的轰炸机投下十几枚炸弹，对重庆实施了抗战以来的第一次轰炸。由于事前没有捕捉到任何关于袭击的蛛丝马迹，国民党情报部门官员们大为光火。他们将目光投向了那似乎无法破译的密码。

1938 年 8 月，国民政府迁都重庆，蒋介石坐镇重庆，筹划正面战场的抗战事宜。一时间，日机频频飞临重庆上空，实施狂轰滥炸。在很长一段时间里，国民党的情报机关发现了一个异常现象，日军与重庆当地的一些隐蔽电台通信频繁，所用密码十分奇特，难以破译。他们断定重庆屡遭轰炸，日机难以被击落与潜伏在当地的日本特务提供情报有关，可他们一时束手无策，难以找到对付的办法。

同年 10 月 4 日上午，28 架日军飞机对重庆发动猛烈袭击，平民死伤 60 余人。面对咄咄逼人的日军和无从下手的密码，密电组陷入了困境。蒋介石对此十分重视，下令求助于美国情报部门，解决这一难题。国民党驻美国华盛顿使馆军事副武官肖勃将一个关键人物——赫

[1] 本故事可结合“探索·发现－密码疑案”纪录片的观看。

图 0-1　赫伯特·亚德利

伯特·亚德利（如图 0-1 所示）推荐到魏大铭面前。

赫伯特·亚德利（Herbert O. Yardley,1889—1958）是美国军事情报处（现美国国家安全局的前身）和“美国黑室”（The American Black Chamber,专门负责破译情报部门获得的密码信息）的创建人，他因为超强的密码破译能力被业内誉为“美国密码之父”，他对日军密码已经研究了十几年，并卓有建树。同年 11 月，化名为“罗伯特·奥斯本”的亚德利在国民党军事委员会技术研究室的邀请下，穿越重重险阻抵达重庆。国民党军方授予他少校军衔，让他一面传授无线电密码通信破译技术，一面协助侦破重庆的日本间谍案，并安排 30 多名留日学生，组成了专门破译神秘电码的情报小组。

日本人曾经为了提高发报速度，以 10 个字母代替 10 个数字进行电报编码。亚德利通过观察发现，这些同样仅使用了日文 48 个字母中的 10 个字母的密码电报也属于这一类型。他把字母转换为数字，对已有的电报进行了初步破译。亚德利凭借自己的经验断定，这是向日军反映重庆的云高、能见度、风向、风速的气象密码电报，相同的数字如每份中均有出现的“027”代表重庆，“231”代表早 6 时，“248”则为正午。但是，由于缺少之前重庆的气象资料，从第 3 组密码开始，每组数字代表的具体意义无法推测出来。

1939 年 1 月 12 至 15 日，机会来了。亚德利小组分别在每日早 6 时、正午以及傍晚 6 时连续截获 8 份密码电报。第一、二组数字的规律和亚德利之前的推断并无二致，大部分电报的第三组密码为“459”，唯独第 6 份为“401”，这些都各自代表什么含义呢？无意间，他的目光落在“401”下方的密码截获日期上。这份密码是当天中午截获的，那时，迷雾多日的重庆市区突然晴空万里。下午，日军派出 27 架轰炸机，炸死炸伤百姓 200 余人。“459”代表着天气不佳，“401”则代表天气晴朗，可以轰炸。密码终于解开了！

密码虽然解开了，但亚德利想到，如果不将间谍抓住，日军很有可能换用新的密码来继续获取我方信息。在接下来的两个月里，小组 3 次截获密码电报，并通过早已准备好的测向仪，捕捉到了发报信号的具体发射源。很快，搜索人员在重庆市南岸区的南山上抓获了伪装成当地人的日本间谍。前不久此人才由侦察机偷送至重庆，负责向位于汉口的日本空军基地发送气象密码电报。

亚德利本想让间谍继续在每天的固定时间向日本空军基地发报，以避免日方发现间谍被俘，改换新的密码。但不料国民党情报部门很快秘密枪决了日本间谍，亚德利只好亲自向日军发送电报，用假情报暂时拖延敌人的轰炸。与此同时，小组截获了大量以更为复杂难解的新密码编写的电报。亚德利据此判断还有更为深藏不露的间谍埋伏在重庆城内，敌人可能会展开新一轮的攻势。但还未等他将这一信息向上级反映，5 月 3 日上午 9 时，日军飞机从武汉直扑重庆，共投下了 100 多枚炸弹，第二天，20 多架日机再袭重庆。抗战历史上悲惨的“五三”、“五四”惨案就这样以 6000 余重庆民众的鲜血为代价发生了。

亚德利决心尽快抓住间谍。就在这时，一个令人费解的现象引起了他的注意。国民党在重庆四周花大力气部署的高炮防空部队，每当日机飞临，均以猛烈的炮火反击，可战果甚小，很少有敌机被击落。为什么竟没有打下几架敌机？这其中必有玄机。

亚德利假扮为美国来的皮货商，通过熟人，结识了驻守在重庆的国民党某高射炮团的一位营长，此人绰号“独臂大盗”。两人相谈十分投机，但“独臂大盗”对于亚德利关于为何高射炮打不中目标的尖锐问题，总是报以不置可否的一笑。

与此同时，新的挑战又摆在了亚德利面前，新密码混合了数字和英文字母。通过重新的排列，他发现电报中开始出现诸如“her”、“light”等具有实际意义的单词，可是这些单词从何而来，又有什么含义呢？一份密码中出现的“he said”引起了亚德利的思考：这样引起对话的词组最常见的地方就是在小说中。亚德利认为这种新密码的来源很可能是一本英文小说，如果能够找出这本小说就能够顺藤摸瓜，找到隐藏在幕后的间谍。可是，上哪里去找这本小说呢？从军事委员会技术研究室传回的消息让亚德利大为振奋。调查显示，“独臂大盗”有时公然使用附近一个川军步兵师的无线电台和他在上海的一个“朋友”互通密电。他很有可能是一名汉奸。亚德利把目光放在了“独臂大盗”身上。

亚德利利用“独臂大盗”请客的时机，让一位英文极好的中国朋友——徐贞小姐（此人是“独臂大盗”的朋友，但她是一个具有爱国热情的女子）事先记下在电报中出现过的单词，再潜入“独臂大盗”的书房，试试能否找到包含这些单词的英文小说。紧张的搜寻之后，在美国女作家赛珍珠那本著名小说《大地》的内页，她找到了这些用笔画过的单词。《大地》以中国社会生活为背景写成，并因此获得诺贝尔文学奖，震撼了国际文坛，可她做梦也不会想到，日本间谍会盗用这部名作设计出轰炸重庆的通信密码。从《大地》入手，亚德利和他的小组破译了新的密码。根据密码和调查得知，“独臂大盗”是汪精卫安插在重庆的耳目，此人出身土匪，会说流利的英语，他经不住日本特务的拉拢，想尽办法，勾结蒋介石的德国顾问赫尔·韦纳，形成一个间谍网，大肆搜集重庆方面的情报，不但为日军指示轰炸目标，而且还将重庆高射炮最高射距 12 000 英尺的重要信息，用密码电台告知日本特务机关，致使日机进入重庆上空后均在 12 000 英尺以上飞行，避开中国高炮部队的打击，疯狂投掷炸弹，屡屡得手，来去自由。

密码的秘密终于被破解。“独臂大盗”被逮捕，不久便被枪决。随着“独臂大盗”的落网，潜伏在重庆的日本间谍网遭到致命打击，此后，日军对重庆的轰炸越来越多地付出了沉重代价，日军的轰炸行动也有所收敛。破获这样微妙的无线电通信密码，这在国际特工史上是不多见的，亚德利功不可没，蒋介石亲自召见他以示嘉勉。徐贞也在破获此案中立下汗马功劳，由于她在离开“独臂大盗”的书房时被仆人发现，为了摆脱日伪特务机关的跟踪追杀，徐贞决定前往中国香港。可是，在她渡过嘉陵江前往机场时，日伪特务制造了她所乘的舢板翻沉事故，她被淹没在滔滔江水中，就此为国捐躯。

1940 年 7 月，亚德利回到美国；为了保密，美方没有透露他的消息。直到 42 年后的 1982 年出版的亚德利回忆录——《中国黑室—谍海奇遇》（1985 年军事译文出版社正式翻译出版，如图 0-2 所示）中才公布了此事的详细经过，此时，亚德利已去世 24 年。现在在重庆南山抗战遗址博物馆中还能找到亚德利当年工作过的痕迹，“密码之父”巧解气象密码在第二次世界大战中的中国留下一段神奇佳话。