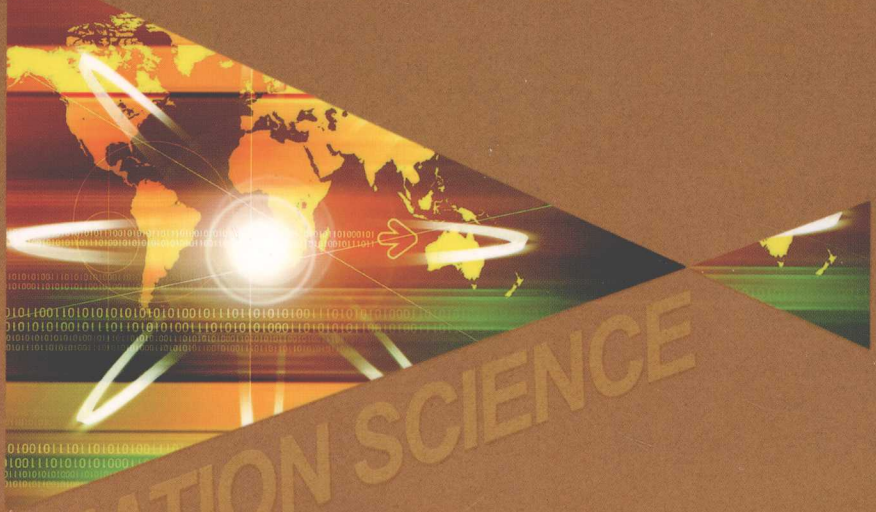
普通高等教育“十一五”国家级规划教材

高等院校信息科学系列教材



INFORMATION SCIENCE

现代密码学

（第二版）

陈鲁生　沈世镒　编著

科学出版社
www.sciencep.com

普通高等教育“十一五”国家级规划教材

高等院校信息科学系列教材

现代密码学

（第 二 版）

陈鲁生 沈世镒 编著

科学出版社

北 京

内 容 简 介

本书是一本关于现代密码学的基础教材. 本书延续了第一版既通俗易懂又有一定广度和深度的特点, 第二版更突出了实用性和可读性. 全书共分9章. 第1章介绍现代密码学中的一些基本概念和术语. 第2章介绍古典密码的加密方法和一些典型的古典密码体制, 以及古典密码的统计分析方法. 第3章介绍Shannon的密码学理论. 第4章和第5章分别讨论分组密码和公钥密码. 第6章介绍流密码和线性移位寄存器序列. 第7章和第8章分别讨论数字签名和Hash函数. 第9章介绍了一些重要的密码协议. 每章后面均附有习题, 其中部分习题是对正文内容的补充.

本书除校正了第一版中的一些排印错误外, 在内容上也做了一些修改和增补, 特别是对第四章中的分组密码的结构和工作模式进行了补充, 并在第五章中增加了公钥密码的一些数学基础.

本书可作为高等院校信息科学专业或其他相关专业的本科生教材, 也可作为相关领域中的教学、科研人员以及工程技术人员的参考书.

图书在版编目(CIP)数据

现代密码学/陈鲁生, 沈世镒编著. —2版. —北京: 科学出版社, 2008
普通高等教育"十一五"国家级规划教材. 高等院校信息科学系列教材
ISBN 978-7-03-022661-7
Ⅰ. 现… Ⅱ. ①陈… ②沈… Ⅲ. 密码-理论-高等学校-教材 Ⅳ. TN918.1
中国版本图书馆CIP数据核字(2008)第116430号

责任编辑: 鞠丽娜 / 责任校对: 柏连海
责任印制: 吕春珉 / 封面设计: 三函设计

科学出版社出版
北京东黄城根北街16号
邮政编码: 100717
http://www.sciencep.com

铭浩彩色印装有限公司印刷

科学出版社发行 各地新华书店经销
*
2008年8月第 一 版 开本: B5(720×1000)
2008年8月第一次印刷 印张: 13 1/4
印数: 1—4 000 字数: 262 000

定价: 22.00元
(如有印装质量问题, 我社负责调换〈环伟〉)

销售部电话 010-62134988 编辑部电话 010-62138978-8002(HI08)

序　　言

1998 年教育部进行高校专业调整时, 设立了“信息与计算科学”专业. 该专业的设立, 受到很多高等院校的热烈响应, 据不完全统计, 几年来已有约 280 所院校招收了该专业的本科生, 其中大部分院校计划开设信息科学方面的系列课程.

为了配合高等院校在学科专业设置上的改革与深化, 来自几十所高等院校的有关专业的部分领导和教师, 于 1999 年、2000 年召开了第一、二届“信息科学专业发展与学术研讨会”, 与会者热烈讨论并探讨了许多与信息学科的学科发展和建设有关的基本问题. 会议一致认为教材建设是目前最为紧迫的任务, 因此成立了教材编审协调组来组织该系列教材的编写.

2001 年教材编写协调组召集了有多位经验丰富的教师和出版社参加的教材建设会议. 会议明确了教材建设是一项长期的工作, 并决定首先编写和出版这套教材来满足近期急需. 为了保证教材的质量, 会议对每本教材的要求、内容和大纲进行了具体研讨, 并请具有多年教学经验的重点院校教授担任各教材的负责人.

为了贴近教学的实际, 每部教材都配有习题或思考题, 同时对内容也做了结构化安排, 以便教师能根据实际情况部分选讲. 本套教学用书不仅适用于教学, 也可供相关读者参考.

在本套教材编写和出版过程中, 作者对内容的取舍、章节的安排、结构的设计以及表达方式等方面多方听取意见, 并进行了反复修改. 在感谢作者们辛勤劳作的同时, 编委会还特别感谢科学出版社的鞠丽娜编辑, 她不辞辛劳, 在统筹印刷出版、督促进度、征求意见、组织审校等方面做了大量工作. 这套教材能在保证质量的前提下, 及时与读者见面, 和她的努力是分不开的.

从长远的教学角度考虑, 为了适应不同类型院校、不同要求的课程需要, 教材编审协调组将不断组织教材的修订、编写 (译), 从而使信息科学教学用书做到逐步充实、完善、提高和多样化. 在此衷心希望采用本套系列用书的教师、学生和读者对书中存在的问题及时提出修改意见和建议.

高等院校信息科学系列教材编委会

2002 年 3 月

第二版前言

随着计算机和通信网络的迅速发展, 信息的安全性越来越受到人们的重视. 密码学是信息安全的基础. 近三十年来, 密码学的理论和应用得到了长足的发展, 其内容变得越来越丰富.

本书作为信息科学系列教材之一已出版 6 年多了, 在此期间已重印 7 次, 受到国内多所高校师生的欢迎. 本书于 2006 年被列入普通高等教育“十一五”国家级规划教材. 借此机会, 我们根据在南开大学数学科学学院为信息科学专业的本科生讲授现代密码学的教学实践和有关反馈信息, 对第一版中的内容做了一些修订. 讲授本书内容大约需要 54 个课时. 如果教师在本书基础上, 适当增加一些内容, 本书也可以很容易地扩充为一门 72 课时的密码学课程教材.

对于本次修订, 我们增加了一些内容, 主要在内容组织上进行了一些修改, 对分组密码的结构和工作模式进行了补充, 增加了公钥密码的一些数学基础. 另外, 我们还增加了一些例题和习题, 在文字表达上也做了一些修改.

本书的修订被列入“南开大学教材资助立项项目”, 并得到了一定的资助支持, 在此向相关人员和单位表示感谢.

尽管本书做了一些修订, 但书中难免存在不妥之处. 敬请读者批评指正.

作 者

2008 年 6 月

第一版前言

随着电子计算机和通信网络的广泛应用, 信息的安全性已受到人们的普遍重视. 信息安全已不仅仅局限于政治和军事以及外交等领域, 而且现在与人们的日常生活也息息相关. 现在, 密码学理论和技术已得到了迅速的发展, 它是信息科学和技术中的一个重要研究领域.

多年来, 我们一直在南开大学为信息科学专业的本科生和研究生讲授现代密码学课程. 本书就是在此基础上编写而成的, 目的是为高等院校信息科学专业或相关专业的本科生提供一本关于现代密码学的教材.

本书系统地介绍现代密码学的基本内容. 全书共分九章. 第一章介绍密码学中的一些基本概念. 第二章介绍古典密码, 讨论了古典密码的基本加密方法和分析方法, 并介绍了一些典型的古典密码体制. 第三章介绍 Shannon 的密码学理论. 第四章讨论分组密码, 主要介绍数据加密标准 DES 和高级加密标准 AES, 这是两种不同类型的分组密码. 第五章讨论公钥密码, 介绍三种常见的公钥密码体制, 并对公钥密码中用到的大素数的生成方法进行了讨论. 第六章介绍序列密码和线性移位寄存器序列. 第七章和第八章分别讨论数字签名和 Hash 函数. 第九章介绍一些重要的密码协议.

在本书的编写过程中, 我们力求简明扼要, 容易理解. 对书中介绍的密码体制的数学背景, 我们都做了简明扼要的介绍. 书中所用到的数学结论基本上都做了证明, 只有少数的数学结论由于证明过于复杂或者牵扯到更多的数学知识, 我们只给出结论, 而没有给出证明, 有兴趣的读者可以参阅相应的文献. 众所周知, 如果不理解相应的数学基础, 要理解一个密码体制是困难的. 我们假定本书的读者具备简单的概率论, 高等代数, 有限域以及数论等基本知识. 另外, 了解一点有关计算复杂性的知识对于理解各种密码体制和密码协议是有用的. 由于严格地定义计算复杂性需要用到理论计算机科学中的一些知识, 所以本书对此只做了一点简单的直观描述, 感兴趣的读者可以参阅有关的文献.

本书适合高等院校信息科学和计算机科学以及通信等专业的高年级本科生使用, 也可供相关领域中的教学和科研人员以及工程技术人员参考.

由于时间仓促, 书中难免有疏漏和不当之处, 敬请读者批评指正.

作 者

2002 年 5 月

目　录

第1章 引 言

密码学的研究与应用已有几千年的历史, 其基本目的就是让通信双方能够在一个不安全的信道上进行保密通信. 任何第三方即使在信道上截获了通信双方的通信内容, 也无法知道所截获内容的准确含义.

现代密码学较之古典密码学已有了很大的发展, 内容更加丰富多彩. 本章主要介绍密码学的一些基本概念和术语.

1.1 密码学的发展概况

密码学是一门既古老又年轻的学科, 其历史可以追溯到几千年以前.

古代的行帮暗语 (黑话) 和一些文字猜迷游戏等, 实际上就是对信息的加密. 这种加密方法通过原始的约定, 把需要表达的信息限定在一定的范围内流通.

古典密码主要应用于政治和军事以及外交等领域. 可以说, 自从有了战争, 就有了保密通信. 交战双方都为了保护自己的通信安全, 以及窃取对方的情报而研究各种信息加密技术和密码分析技术. 第二次世界大战期间, 同盟军方面情报战的胜利大大地缩短了战争的进程, 信息战的胜利对于反法西斯战争的胜利起了重大的作用.

在 1949 年之前, 密码技术基本上可以说是一门技巧性很强的艺术, 而不是一门科学. 在这一时期, 密码专家常常是凭借直觉和信念来进行密码设计和分析, 而不是推理证明.

在 1949 年, C. E. Shannon 发表了“保密系统的通信理论”一文, 为密码学奠定了坚实的理论基础, 使密码学成为一门真正的科学. 但从 1949 年至 1975 年, 密码学的理论研究工作进展不大.

1976 年, W. Diffie 和 M. E. Hellman 发表了“密码学中的新方向”一文, 提出了一种崭新的密码设计思想, 导致了密码学上的一场革命. 他们首次证明了从发送端到接收端无密钥传输的保密通信是可能的, 从而开创了公钥密码学的新纪元. 1977 年, 美国国家标准局 (National Bureau of Standards) 正式公布实施数据加密标准 DES(data encryption standard), 将 DES 算法公开, 从而揭开了密码学的神秘面纱. 从此, 密码学的研究进入了一个崭新的时代.

随着计算机科学的蓬勃发展, 我们这个社会已开始进入信息时代. 电子计算机和通信网络的广泛应用, 一方面为人们的生活和工作提供了很大的方便, 另一方面

也提出了许多亟待解决的问题, 其中信息的安全性就是一个突出的问题. 因此, 密码学理论和技术已成为信息科学和技术中的一个重要研究领域. 随着计算机网络的迅速发展, 特别是近年来电子商务的兴起, 现代密码学的应用已不仅仅局限于政治和军事以及外交等领域, 其商用价值和社会价值也已得到了充分的肯定.

1.2 保密系统

简单地说, 一个保密系统主要由明文信源、信道、加密器、解密器以及密钥源等五个基本部分组成, 如图 1.1 所示.

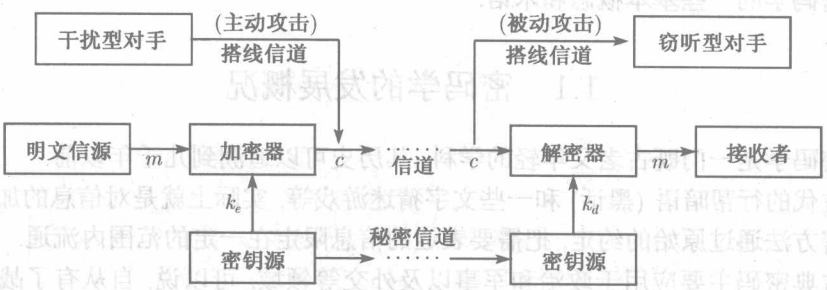


图 1.1　保密系统模型

明文信息的产生和发送者称为明文信源 (source). 我们一般称由明文信源产生的信息为消息 (message). 由明文信源输出的消息要经过某种通信渠道传送给称为信宿的接收者 (receiver). 譬如, 在一个电话通信系统中, 打电话的用户就是这个通信系统的信源, 而接听电话的用户就是这个通信系统的信宿.

所谓信道 (channel) 就是将明文信源消息传送给接收者的渠道. 譬如, 在有线电话通信系统中, 电话线就是信道. 实际的信道可以是电缆、光纤、高频无线电连接和卫星通信连接等.

加密器将明文信源输出的消息变换为密文, 然后再输出到信道. 解密器接收信道的输出, 并恢复出原始的明文信源消息. 密钥源用于产生加密器和解密器所使用的密钥.

另外, 存储系统也可以看做是一种特殊的保密系统. 对于保密的存储系统我们也可以用图 1.1 来进行描述. 譬如, 计算机存储系统、录音机存储系统等. 这时的信道就是存储介质, 信道的输入就是往存储介质上写入加密信息, 信道的输出就是从存储介质上读取密文并恢复明文.

保密系统的使用者通常称为用户 (user). 保密系统的破坏者有时称为对手 (adversary). 对手分为“窃听型”和“干扰型”两种. “窃听型”对手只是截取信道上传

送的信息, 然后进行分析. 而“干扰型”对手则会篡改信道上传送的信息.

1.3 密码体制

没有加密的信息称为明文 (plaintext). 加密后的信息称为密文 (ciphertext). 从明文到密文的变换称为加密 (encryption). 从密文到明文的变换称为解密 (decryption).

加密和解密都是在密钥 (key) 的控制下进行的. 给定一个密钥, 就可确定一对具体的加密变换和解密变换.

一个密码体制 (cryptosystem) 通常由五部分组成:

1) 明文空间 $\mathcal{M}$: 全体明文的集合.
2) 密文空间 $\mathcal{C}$: 全体密文的集合.
3) 密钥空间 $\mathcal{K}$: 全体密钥的集合. 通常每个密钥 k 都由加密密钥 k_e 和解密密钥 k_d 组成, $k=\langle k_e, k_d\rangle$. k_e 与 k_d 可能相同, 也可能不同.
4) 加密算法 $\mathcal{E}$: 由加密密钥控制的加密变换的集合.
5) 解密算法 $\mathcal{D}$: 由解密密钥控制的解密变换的集合.

设 $m\in\mathcal{M}$ 是一个明文, $k=\langle k_e, k_d\rangle\in\mathcal{K}$ 是一个密钥, 则

$$c=E_{k_e}(m)\in\mathcal{C},$$

$$m=D_{k_d}(c)\in\mathcal{M},$$

其中 E_{k_e} 是由加密密钥 k_e 确定的加密变换, D_{k_d} 是由解密密钥 k_d 确定的解密变换. 在一个密码体制中, 要求解密变换是加密变换的逆变换. 因此, 对任意的 $m\in\mathcal{M}$ 都有

$$D_{k_d}(E_{k_e}(m))=m$$

成立.

密钥空间中不同密钥的个数称为密码体制的密钥量. 它是衡量密码体制安全性的一个重要指标.

如果一个密码体制的加密密钥与解密密钥相同, 则称其为单密钥密码体制或对称密码体制; 否则, 称其为双密钥密码体制或非对称密码体制.

在一个双密钥密码体制中, 如果由加密密钥 k_e 计算解密密钥 k_d 是困难的, 公开 k_e 不会损害 k_d 的安全性, 则可以将加密密钥 k_e 公开. 这样的密码体制称为公钥密码体制 (public-key cryptosystem).

1.4 密码分析

密码分析指的就是对密码体制的攻击. 一个好的密码体制至少应该满足下述两

个条件：

1) 在已知明文 m 和加密密钥 k_e 时, 计算 $c = E_{k_e}(m)$ 容易. 在已知密文 c 和解密密钥 k_d 时, 计算 $m = D_{k_d}(c)$ 容易.

2) 在不知解密密钥 k_d 时, 不可能由密文 c 推知明文 m.

对于一个密码体制, 如果能够根据密文确定明文或密钥, 或者能够根据一些明文和相应的密文确定密钥, 则我们说这个密码体制是可破译的; 否则, 称其为不可破译的.

密码分析者攻击密码体制的方法主要有以下三种：

1) 穷举攻击：密码分析者通过试遍所有的密钥来进行破译. 显然, 可以通过增大密钥量来对抗穷举攻击.

2) 统计分析攻击：密码分析者通过分析密文和明文的统计规律来破译密码. 对抗统计分析攻击的方法是设法使明文的统计特性与密文的统计特性不一样.

3) 解密变换攻击：密码分析者针对加密变换的数学依据, 通过数学求解的方法来设法找到相应的解密变换. 为对抗这种攻击, 应该选用具有坚实的数学基础和足够复杂的加密算法.

密码分析者通常可以在下述四种情况下对密码体制进行攻击：

1) 唯密文攻击 (ciphertext-only attack)：密码分析者仅知道一些密文.

2) 已知明文攻击 (known-plaintext attack)：密码分析者知道一些明文和相应的密文.

3) 选择明文攻击 (chosen-plaintext attack)：密码分析者可以选择一些明文, 并得到相应的密文.

4) 选择密文攻击 (chosen-ciphertext attack)：密码分析者可以选择一些密文, 并得到相应的明文.

其中唯密文攻击的强度最弱, 其他情况下的攻击强度依次增加.

除了上述四种攻击情况外, 还有另外两种攻击情况：

1) 自适用选择明文攻击 (adaptive-chosen-plaintext attack)：这是选择明文攻击的一种特殊情况, 指的是密码分析者不仅能够选择要加密的明文, 还能够根据加密的结果对以前的选择进行修正.

2) 选择密钥攻击 (chosen-key attack)：这种攻击情况在实际应用中比较少见. 它仅表示密码分析者知道不同密钥之间的关系, 并不表示密码分析者能够选择密钥.

应当指出, 对任何一种攻击方法, 我们都假定密码分析者事先知道所使用的密码体制, 这一点称为 Kerckhoff 假设, 是由 Auguste Kerckhoff(1835—1903) 提出的. 在设计密码体制时, 应当记住的一点是：永远不要低估密码分析者的能力.

1.5　密码体制的安全性

对于一个密码体制, 如果密码分析者无论截获了多少密文以及无论用什么方法进行攻击都不能破译, 则称其为绝对不可破译的密码体制. 绝对不可破译的密码在理论上是存在的. 但是, 如果能够利用足够的资源, 那么任何实际的密码都是可以破译的. 因此, 更有实际意义的是在计算上不可破译 (computationally unbreakable) 的密码. 所谓计算上不可破译是指密码分析者根据可利用的资源来进行破译所用的时间非常长, 或者破译的时间长到使原来的明文失去保密的价值.

评价密码体制的安全性有一些不同的途径. 现在我们简单介绍评价密码体制安全性的三个不同的概念.

1) 计算安全性 (computational security): 如果我们使用最好的算法来破译一个密码体制至少需要 n 次操作, 而 n 是一个非常大的数, 则我们称这个密码体制是计算上安全的. 计算上安全的密码体制就是计算上不可破译的密码体制. 遗憾的是, 到目前为止, 还没有一个实际的密码体制被严格证明是绝对的计算上安全的. 在实际中, 我们通常针对某些特定的攻击类型来研究密码体制的计算安全性. 譬如, 证明一个密码体制对于穷举攻击是否是计算上安全的. 当然, 一个密码体制对于一种攻击类型是计算上安全的, 并不意味着对于其他类型的攻击也是计算上安全的.
2) 可证明安全性 (provable security): 如果一个密码体制的安全性可以归结为某一个数学问题, 而这个数学问题目前是难解的, 则我们称这个密码体制是可证明安全的. 譬如, 我们可以证明, 如果一个给定的大整数无法有效地分解为素因子的乘积, 则给定的密码体制就是不可破译的. 应当指出, 可证明安全性只是说明一个密码体制的安全性是与一个数学难题相关的, 并没有完全证明这个密码体制是安全的.
3) 无条件安全性 (unconditional security): 对于一个密码体制, 如果密码分析者即使具有无限的计算能力, 也无法破译该密码体制, 则我们称这个密码体制是无条件安全的. 无条件安全性通常是针对某些攻击而言的. 譬如, 我们可以证明, 某些密码体制在唯密文攻击的情况下是无条件安全的. 但这不能保证在其他类型的攻击下, 该密码体制还是安全的. 因此, 所谓的无条件安全也是有前提的.

分析一个密码体制的安全性是一件困难的事情, 因为我们现在并没有一个通用的方法来分析任意一个给定的密码体制是否安全. 我们现在所做的通常只是分析一个密码体制是否能抵抗所有已知的攻击方法, 或者在某些前提条件下是否是安全的. 因此, 在实际应用中, 一个密码体制在使用一段时间后, 会更换一些新的参数,

或者更换新的密码体制. 当然, 密钥肯定是要经常变换的.

习 题

1.1 我们日常生活中用到的一些密码 (password), 譬如, 电子邮箱的登录密码 (password) 是否是安全的? 能否抵抗穷举攻击? 如何防范穷举攻击?

1.2 对于任何一个密码体制 $\mathcal{S}=(\mathcal{M},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$, 明文 $m\in\mathcal{M}$, 密钥 $k=\langle k_e,k_d\rangle\in\mathcal{K}$, 我们知道

$$D_{k_d}(E_{k_e}(m))=m$$

一定成立. 试问:

$$E_{k_e}(D_{k_d}(m))=m$$

是否也一定成立? 即加密变换与解密变换是否一定是可交换的?

第2章　古典密码

本章介绍古典密码体制中的基本加密运算、几种典型的古典密码体制以及关于古典密码体制的一些破译方法. 虽然古典密码大都比较简单而且容易破译, 但研究古典密码的设计原理和分析方法对于理解和设计以及分析现代密码是十分有益的.

2.1　古典密码中的基本加密运算

明文字母表 X 是指明文空间 $\mathcal{M}$ 中出现的所有不同的字母的集合. 密文字母表 Y 是指密文空间 $\mathcal{C}$ 中出现的所有不同的字母的集合.

对于一个密码体制, 如果明文字母对应的密文字母在密文中保持不变, 则称其为单表密码体制; 如果明文中不同位置的同一明文字母在密文中对应的密文字母不同, 则称其为多表密码体制.

设 q 是一个正整数, $Z_q=\{0,1,2,\cdots,q-1\}$, 则 Z_q 在模 q 加法和模 q 乘法运算下构成一个交换环. 记

$$Z_q^*=\{\,k\in Z_q \mid \gcd(k,q)=1\,\},$$

则 Z_q^* 在模 q 乘法运算下构成一个乘法群, 其中 $\gcd(k,q)$ 表示 k 和 q 的最大公因子.

2.1.1　单表古典密码中的基本加密运算

1. *加法密码*

设 $X=Y=Z_q$, $\mathcal{K}=Z_q$. 对任意 $m\in X$, $k\in\mathcal{K}$, 密文

$$c=E_k(m)=(m+k) \bmod q.$$

显然, 加法密码的密钥量为 q.

2. *乘法密码*

设 $X=Y=Z_q$, $\mathcal{K}=Z_q^*$. 对任意 $m\in X$, $k\in\mathcal{K}$, 密文

$$c=E_k(m)=km \bmod q.$$