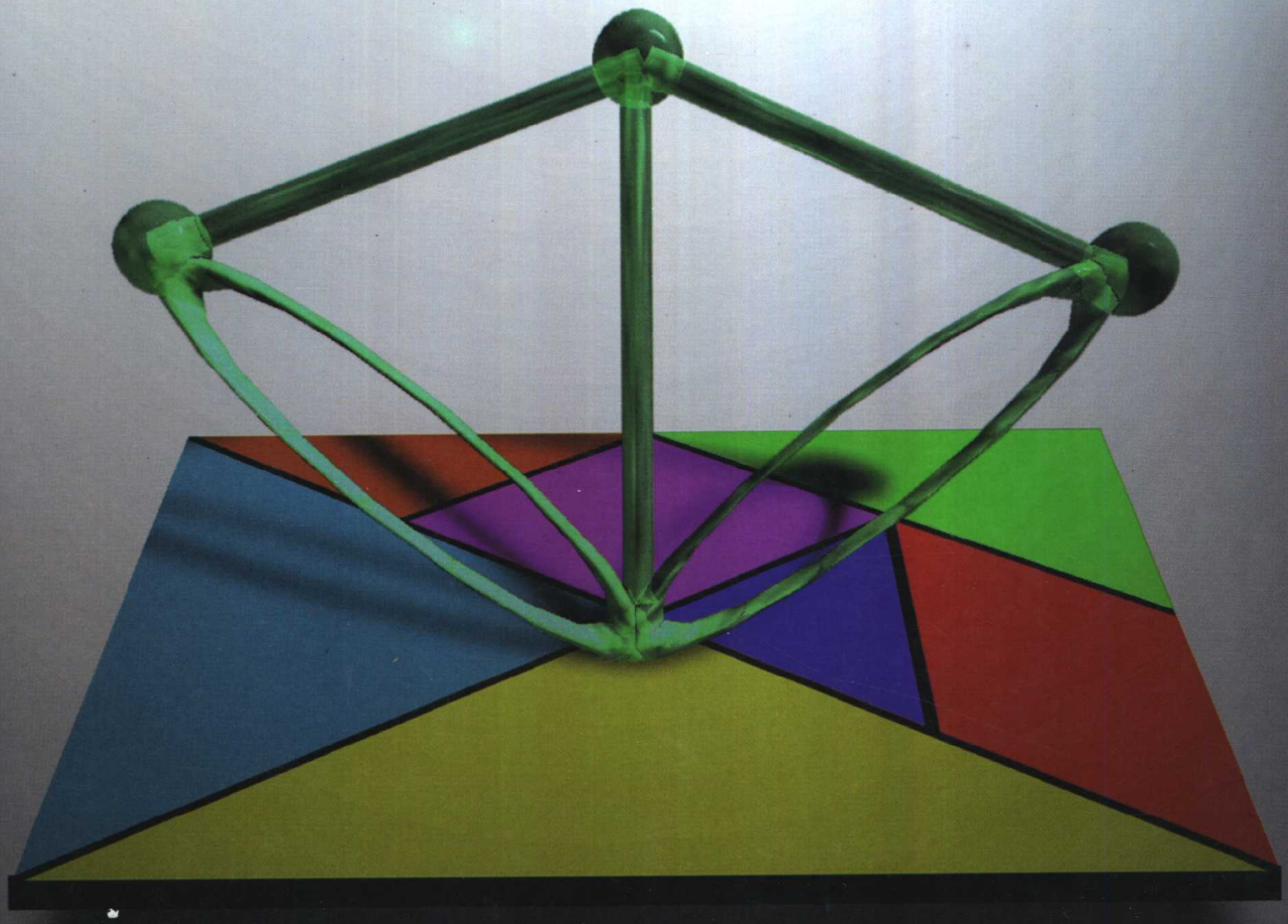
计算机科学组合学丛书

计算机密码学

—— 计算机网络中的数据保密与安全

（第3版）

卢开澄 编著



清华大学出版社

计算机科学组合学丛书

计 算 机 密 码 学

——计算机网络中的数据保密与安全

（第 3 版）

卢开澄　编著

清华大学出版社
北　京

内容简介

在电子商务和电子政务的兴起和发展过程中，近代密码学扮演了十分活跃的角色。本书是在第2版的基础上，结合这几年密码学技术的发展改写而成。全书共13章，叙述了密码学基本概念、分组密码、公钥密码、大数运算、密码协议、密钥管理等，第3版比第2版增加了大数运算、数字签名、密钥管理、密码协议等内容，尤其对AES的加密标准及部分候选算法做了详细的介绍，并加强了与网络通信的保密安全相关的内容。

本书可作为计算机专业或其他专业关于“网络通信保密安全”相关课程的教材或参考书。

图书在版编目(CIP)数据

计算机密码学——计算机网络中的数据保密与安全/卢开澄编著. —3版. —北京：清华大学出版社，2003

(计算机科学组合学丛书)

ISBN 7-302-07536-0

Ⅰ.计… Ⅱ.卢… Ⅲ.计算机网络－密码术 Ⅳ.TP393.08

中国版本图书馆CIP数据核字(2003)第090[redacted]号

出 版 者：清华大学出版社　　北京清华大学学研大厦

http://www.tup.com.cn　　100084

社 总 机：010-62770175　　010-62776969

组稿编辑：薛 慧　张 民

文稿编辑：付宇光　张 民

封面设计：卢开澄　傅瑞学

印 刷 者：北京昌平环球印刷厂

装 订 者：北京国马印刷厂

发 行 者：新华书店总店北京发行所

开　　本：185×260　**印张**：31.75　**字数**：731千字

版　　次：2003年12月第3版　2003年12月第1次印刷

书　　号：ISBN 7-302-07536-0/TP·5548

印　　数：1～5000

定　　价：46.00元

计算机科学组合学丛书序

电子计算机的出现是20世纪的大事，它改变了我们这个世界的面貌。可以毫不夸张地说，它的影响遍及所有的角落，几乎无处不在。数学更不例外。严格地说，电子计算机本身就是近代数学的辉煌成就。将计算机与数学割裂开来，既不合理也不可能。组合学就是在计算机科学蓬勃发展的刺激下而崛起的，从而成为近若干年来最活跃的数学分支。它研究的问题有的可追溯到欧拉和哈密顿等18世纪的数学家，但它成为一新的分支还是近若干年的事。它从与计算机科学相结合中获得了广阔的发展空间，从而也为计算机科学奠定了理论基础。

什么是计算机科学呢？有的学者将它定义为研究算法的一门学科。研究算法无疑是计算机科学的重要领域，也是本丛书的核心内容，贯穿始终。组合学家在20世纪70年代初建立的算法复杂性“NP理论”，至今仍然令无数计算机科学工作者与数学工作者为之折腰。

计算机科学里的组合学内容十分广泛。本丛书涉及组合分析、图论、组合算法、近代密码学、组合优化、编码理论及算法复杂性等7部分。

组合分析是算法的理论基础。组合分析与组合算法犹如数学分析与计算数学，众所周知，前者是后者的理论根基。

图论原本是组合数学这个“家族”的主要成员，只因它已成长壮大，故自立门户独立出去。

算法复杂性的NP理论是近30年的一大成就。研究表明，对于一类叫做NPC类的困难问题，至今都不存在有效算法，但它们难度相当，只要其中任何一个找到多项式解法，则全体都获得解决；或证明它们根本不存在有效办法。不论是前者还是后者都还看不见露到海平面上的桅杆塔，它吸引了众多的有志之士。密码学是其中十分引人入胜的分支。如若设计好的密码，对它的破译等价于某一NPC类困难问题，无疑这样的密码将是牢不可破的。

在计算机网络深入普及的信息时代，信息本身就是时间，就是财富。信息的传输通道是脆弱的公共信道，信息存储于“不设防”的计算机系统中，如何保护信息的安全使之不被窃取及不至于被篡改或破坏，已成为当今普遍关注的重大问题。密码是有效而且可行的办法。在计算机网络的刺激下，近代密码学便在算法复杂性理论的基础上建立起来了。密码作为一种技术，自从人类有了战争，不久便有了它。但作为一门学科则是近20多年的事，甚至于它已成为其他学科的基础。密码也从此走出“军营”，进入百姓家。

实际中的“优化”问题是大量的，半个多世纪以来它曾经几度辉煌。近来在计算机科学的影响下，又出现了若干闪光点，十分耀眼，引人注目。

实际上密码也是一种编码。如果说密码学研究的编码是保证通信的保密与安全，则

编码理论研究的是通信中如何纠错与检错。计算机纠错码是既实用、理论上又饶有趣味的分支。

本丛书是作者在清华大学计算机科学与技术系长期工作的总结。它不是一部“长篇记述”，而是互相关联又彼此相对独立的，因此难免有少量交叉。它们涉及的面非常广泛，囿于作者的水平，缺点和错误在所难免，敬请读者不吝指正。谢谢。

作　者

前　言

自从人类有了战争，就有了密码，所以密码作为一种技术源远流长，可以追溯到远古时代，而且还有过自己的辉煌经历。但成为一门学科则是近20余年的事，这是受计算机科学蓬勃发展的刺激结果。今天在计算机被广泛应用的信息时代，信息本身就是时间，就是财富。大量信息用数据形式存放在计算机系统里。信息的传输则通过公共信道。这些计算机系统和公共信道是不设防的，是很脆弱的，容易受到攻击和破坏，信息的丢失不容易被发现，而后果是极其严重的。如何保护信息的安全已不仅仅是军事和政府部门感兴趣的问题，各企事业单位也愈感迫切。因为在网络化的今天，计算机犯罪每年使他们遭受的损失极其巨大，而且还在发展中。密码是有效而且可行的保护信息安全的办法，有效是指密码能做到使信息不被非法窃取、不被篡改或破坏，可行是说它需要付出的代价是可以接受的。

密码形成一门新的学科是在20世纪70年代。它的理论基础之一应该首推1949年Shannon的一篇文章"保密通信的信息理论"，这篇文章过了30年后才显示出它的价值。现在，密码学有了突飞猛进的发展，而且成为有些学科的基础。特别是"电子商务"和"电子政府"的提出，使得近代密码学的研究成为热门的课题。也大大地扩大了它的发展空间。

在近代密码学上值得一书的大事有两件：一是1977年美国国家标准局正式公布实施了美国的数据加密标准(DES)，公开它的加密算法，并批准用于非机密单位及商业上的保密通信。密码学的神秘面纱从此被揭开。二是Diffie和Hellman联合写的一篇文章"密码学的新方向"，提出了适应网络上保密通信的公钥密码思想，掀起了公钥密码研究的序幕。受他们的思想启迪，各种公钥密码体制被提出，特别是RSA公钥密码的提出在密码学史上是一个里程碑。可以这么说："没有公钥密码的研究就没有近代密码学。"

在密码学的发展过程中，计算机科学和数学工作者作出了卓越的贡献。数学中许多分支如数论、概率统计、近世代数、信息论、椭圆曲线理论、算法复杂性理论、自动机理论、编码理论等都可以在其中找到各自的位置。它的踪影遍及数学许多分支，而且还推动了并行算法的研究，从而成为近若干年来非常引人入胜的领域。但还应该强调指出的是密码学毕竟不等于数学，它还有自己的空间。

中国不能没有自己的密码系统，中国也必须有自己的数据加密标准。近年来，我国引进了很多设备，惟有密码设备不能依靠引进，开展这方面的研究是当务之急。

本书是作者在清华大学计算机系从事数据安全的教学科研基础上写成的，文中有不妥之处，欢迎读者批评指正。

作　者

2003年9月

目　录

第 1 章　传统密码与密码学基本概念

1.1　引　　论

密码学以研究秘密通信为目的，即研究对传输信息采取何种秘密的变换以防止第三者对信息的窃取。

在今天的信息社会里，通信安全保密问题的研究已不仅仅出于军事、政治和外交上的需要。科学技术的研究和发展及商业等方面，无一不与信息息息相关。所以信息就是生命，信息就是时间，信息就是财富。由于信息是共享的，信息的扩散会产生社会影响，所以保护信息的安全是信息时代的迫切需要。

保护信息的安全无疑是十分重要的，然而信息的丢失不容易被发现。同时它又是具有时间性的。同一信息在不同时间里的价值也是不一样的，有时候获得信息的时间比信息本身还重要。

信息的存储和传输是通过载体进行的，例如，信使便是以人作为载体的。近代通信的载体有电波或电信号、磁盘等。

保密有载体保密和通信保密两种。密码学主要研究通信保密，而且仅限于数据通信保密。此外，还有语音保密和图像传输保密等。语音保密是研究电话通信的保密技术，不在本书讨论范围内。

近年来，密码学研究之所以十分活跃，主要原因是它与计算机科学的蓬勃发展息息相关。此外还由于电信事业以及防止日益严重的计算机犯罪的需要。由于公共和私人部门的一些机构愈来愈多地应用电子数据处理，将数据存储在数据库中，因此防止非法泄露、删除、修改等是必须正视的问题。特别是，电子资金传输系统是一个由通信网络互相联结的金融机构，并通过这种网络传输大量资金，这是密码通信通向民用的典型例子。因此，信息的安全性也成为全社会关心的问题，密码学从此也成为一门新的学科，引起了数学家和计算机科学工作者日益浓厚的兴趣。

一般说来，由数据库收集或存储的大量数据，或在传输过程中的数据，由于传输中的公共信道和存储的计算机系统非常脆弱，容易受到两种形式的攻击：一种是从传输信道上截取信息，或从存储的载体上偷窃或非法复制信息，我们称之为被动攻击，其结果是导致数据的暴露和对私有权的侵犯；另一种是对在传输过程中或对存储的数据进行非法删除、更改或插入等操作，这称之为主动攻击，其结果可能引起数据或文件的混乱，严重时可能导致信息处理系统完全失控。对于这两种可能遭受到的攻击除了制定法律外，还需要有合适的保护措施，密码技术就是一种有效的方法。事实证明，这也是最经济可行的方法，它使得在一种潜在不安全的环境中保证通信的安全。正是因为密码对于通信安全的极端重要性，所以应该强调说，不安全的密码技术比没有还要坏，因为它给人们以安全的假象。

密码技术还有效地被用于信息鉴别、数字签名等，用以防止电子欺骗，这对信息处理

系统的安全起到极其重要的作用。

近代密码学研究并非是传统密码技术的旧话重提，它有其自己的特点。快速电子计算机和现代数学方法一方面为加密技术提供了新的概念和工具，另一方面也给破译者以有力武器。总之，较之传统的密码系统有更丰富多彩的内容。

密码加密算法的对立面就是密码分析，也就是密码的破译技术研究。加密与破译是一对矛盾，了解破译对研究加密是非常必要的。

1.2 基本概念

什么是密码？简单地说它就是一组含有参数 k 的变换 E。设已知信息 m，通过变换 E_k 得密文 c，即

$$c=E_k(m)$$

这个过程称之为加密，参数 k 称之为密钥。加密算法 E 确定之后，由于密钥 k 不同，密文 c 也不同。

当然不是所有含参数 k 的变换都可以作为密码，它要求计算 $E_k(m)$ 不困难，而且若第三者不掌握密钥 k，即使截获了密文 c，他也无法从 c 恢复信息 m，也就是反过来从 c 求 m 极为困难。以后称 m 为明文。

通信双方一方为发信方，简称发方，另一方为收信方，简称收方。传统的保密通信机理可用图 1.1 表示。

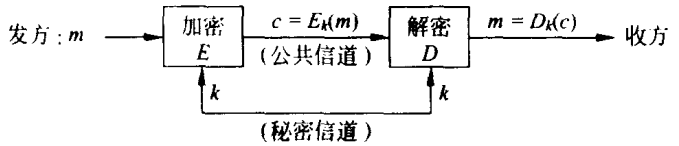


图 1.1

从密文 c 恢复明文 m 的过程称之为解密。解密算法 D 是加密算法 E 的逆运算，解密算法也是含参数 k 的变换。传统密码加密用的密钥 k 与解密用的密钥 k 是相同的，所以有时也叫对称密码。通信双方用的密钥 k 是通过秘密方式由双方私下约定产生的，只能由通信双方秘密掌握。如果丢失了密钥，则密码系统不攻自破。密钥的重要性可想而知。举一个最简单的例子。设已知明文 m 为

during the last twenty years there has been an explosion of public academic research in cryptography

明文的意思是“近 20 年对密码学的公开研究已急剧增加”。

先将明文分成 5 个字符一组得

durin gthel asttw entyy earst hereh asbee nanex plosi onofp ublic acade micre searc hincr yptog raphy

再将每组按相反顺序写下，例如 durin，倒过来写成 nirud，于是得密文 c 如下：

nirudlehtgwttsayytnetsraehereheebsaxenanisolppfonocilbuedacaercimcraes

rcnihgotpyyhpar

这里加密算法便是将明文先分组再逆序书写，密钥是每组的字符长。本例 $k=5$。若不知道加密算法，该密文相对于明文面目全非，从而达到加密的目的。当然这个加密算法不是很安全的，破译不难。

1.3 若干传统密码与其破译技术

在这一节将介绍若干经典、传统的密码，附带讨论其中若干破译技巧。本书重点讨论加密算法。加密与破译是一对矛和盾，整个密码学也分成两大分支：加密方法与密码分析。密码分析则是研究破译的一门技术。但了解破译技术对研究加密算法是必要的。加密是一门科学，密码分析也是一门学问。有的加密算法对不掌握密码分析方法的人乍一看十分神秘，似乎“牢不可破”，其实不堪一击。前面已强调过，不可靠的密码比没有密码还坏。

1.3.1 密码举例

最早的一种密码是在公元前两世纪，由一位希腊人提出来的。他将 26 个字母排列在一个 5×5 的方格里，其中 i 和 j 填在同一格，如下所示：

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	ij	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

于是每个字母对应一数 $\xi\eta$，其中 ξ 是该字母所在行的标号，η 是列标号。如 c 对应 13，r 对应 42 等。使用这种密码可以将明文

secure message transmission is of extreme importance in information based society

转换为密文

43 15 13 45 42 15 32 15 43 43
11 22 15 44 42 11 33 43 32 24
43 43 24 34 33 24 43 34 21 15
53 44 42 15 32 15 24 32 35 34
42 44 11 33 13 15 24 33 24 33
21 34 42 32 11 44 24 34 33 12
11 43 15 14 43 34 13 24 15 44
54

在古代这种棋盘密码曾被广泛应用。