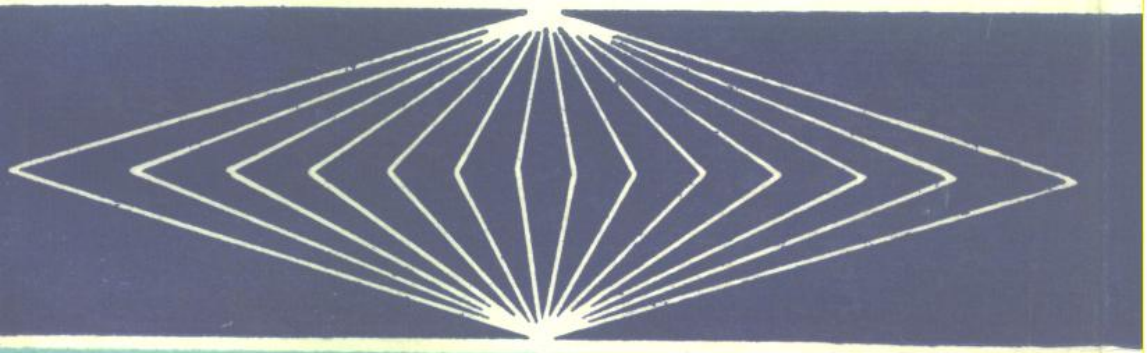
信息加密技术

卢铁城 编著

XINXIJIAMIJISHU



XINXIJIAMIJISHU

四川科学技术出版社

信息加密技术

卢铁城 编著

四川科学技术出版社

1989年·成都

责任编辑：解励诚
特约编辑：黄　河
封面设计：吕小晶
技术设计：康永光

信息加密技术

卢铁城　编著

四川科学技术出版社出版发行
（成都盐道街3号）
新华书店重庆发行所经销
重庆印制一厂印刷
ISBN 7-5364-1375-0/TP·25

1989年10月第一版　开本 850×1168　1/32
1989年10月第一次印刷　字数 290 千
印数　1—2000 册　印张 11.75 插页 4
定价：　5.50 元

前　言

现代社会正在进入信息社会，信息的重要性越来越为更多的人们所认识，在某种意义上可以说，信息就是财富，就是技术，就是速度，就是胜利。信息（如语言、文字、数据、图像等）需要利用通信网络（如电话、电报、传真、微波、卫星、光纤等）传送和交换，需要利用计算机处理和存储。显然，一部分信息由于其重要性，在一定时间内必须严加保密，严格限制其被利用的范围。利用密码对各类电子信息进行加密，以保证在其处理、存储、传送和交换过程中不会泄露，是迄今为止对电子信息实施保护，保证信息安全的唯一有效措施。

通信保密和数据安全对于军事、公安、外交等有着极端重要的意义，它直接关系到国家安危和战争的胜负。同时，在信息量激增，计算机被广泛应用的今天，信息的安全、保密已为越来越多的人所关心，密码技术的应用已渗透到许多重要领域。

电话将为每个人提供方便的通信；高速的“电子邮政”可能会取代传统的“书面邮政”，商业上可能用“电子邮政”来签署、交换各类合同；银行和金融界中电子资金传递系统和信用卡将被广泛应用，……。显然，在这类商业或个人通信中，人们常常希望能对他们的通信内容实施加密保护和有效地证实鉴别。

计算机系统要求只有合法用户才能接入系统；广大用户希望自己输入、处理和存储的信息，能不被他人（含系统操作人员）利用；软件工作者希望他们辛勤劳动创造出来的系统软件和应用软件不会被其他人无偿占有，……凡此种种，人们都要求利用密

码对重要信息实施保护。

各类重要的遥控信号需要加密，以防敌人施放干扰信号，扰乱对目标的控制；遥测信号也需要加密，否则传回的信号易为敌方利用；雷达敌我识别系统的询问和应答信号，必须实施加密，否则敌人能产生有效的欺骗应答。

近代科学技术的发展，一方面计算机速度越来越高，存储量越来越大，性能愈趋完善，这就为密码分析工作者提供了强有力的破密分析手段，从而使过去传统的加密方法不再满足保密和鉴别的要求。另一方面，正由于计算机技术和大规模集成电路的发展，也为信息加密工作者创建各种新型的保密性强、鉴别性能好的密码通信体制提供了切实的可能性。因此，加密和破密这对矛盾的尖锐斗争，实际应用的需要和现实技术提供的可能性，正推动着信息加密技术进行一次根本性的变革，正吸引越来越多的人从事这方面的研究。

鉴于在通信、计算机、雷达、导航、遥控、遥测等领域内的工程技术人员和高年级学生，对通信和计算机的基本知识（也包括信息论）已有所掌握，但在过去教学计划中未把数论和近世代数列为必修课程，为便于本书的教学或自学，为使读者能深入掌握近代许多新的密码体制，本书第一章比较详细地讲述了近代信息加密技术中的数论基础，介绍了整数的整除性、同余、平方剩余、原根、幂剩余函数、群、环、域的基本概念，伽罗瓦域和多项式。

第二章介绍了信息加密技术中的常用基本算法，求最大公约数、最小公倍数、乘逆的欧几里德算法，求高次幂和高次幂剩余的算法，建立素数表的算法，因数分解算法，判别平方剩余和平方非剩余的算法，找原根的算法，大素数的快速判别算法。掌握了这些基本算法，读者就能方便地写出各种加密和解密方案的计算机程序，在计算机上进行模拟验证。

第三章介绍信息加密的基本方法。尽管单表密码、多表密码、多字母代换、换位密码、代码密码、机械密码、Vernam密码已被一一淘汰，但介绍这些密码，使读者了解密码技术如何在与破密斗争中由简到繁不断发展，从而掌握对信息实施加密变换的基本思路和脉络。本章后面几节介绍的单向密码，移位寄存器序列、序列密码和分组密码在当代信息加密技术中获得了广泛应用。

1977年美国国家标准局（NBS）采纳一种非线性加密算法作为美国的——“数据加密标准”（简称DES），1980年12月美国国家标准协会又采纳DES作为美国的商用加密算法。由于DES的高度保密性和采用大规模集成电路实现的简易性，因而被视作密码学发展史上的一个里程碑。因此，本书第四章单独介绍了数据加密标准的组成，工作原理和使用方式。

1976年美国学者Diffie和Hellman提出了利用公开密钥实现信息加密和数字签名的新思想，1978年后相继出现了实现这个新思想的多种实验性方案，尽管迄今尚无一致公认的标准算法，但密码学界普遍认为公钥密码体制和数字签名是密码学发展史上的又一个里程碑，甚至认为是密码技术上的一次革命，预言到90年代将获普遍应用。因此，第五章单独讲述〈公钥密码体制〉，介绍了它的基本工作原理，以及五种具体的实施方案，其中包括著名的RSA公钥密码体制、密锁背包体制和RSA的改进方案。

密码体制的一切秘密寓于密钥之中。因此，第六章讲述了〈密钥管理〉，在介绍加密和密钥的关系后，系统介绍了密钥的产生、检验、保护、分配和分散保管的基本方法。

鉴于复杂性理论是一个较新的数学分支，近代密码体制的设计和分析中又经常以计算复杂性为依据。因此，附录一简单介绍了〈复杂性理论〉的基本概念。

为了帮助读者较快地熟悉密码技术中的常用基本算法，掌握

如何在计算机上验证各种加密方案，附录二给出了笔者编写的RSA公钥密码体制改进方案的Fortran程序及其计算机运行的输出结果。

一般说来，完全照搬他人成熟的密码体制方案，很难设计出一个保密强度高的密码体制。因此，本书介绍的各种加密方法和密码体制，对读者说来，只能起到掌握原理，启发思维的作用。读者只有针对具体需要，创造性地综合应用各种加密技术，才能设计出自己特有的密码体制。

为了适应信息加密技术应用领域的不断扩大，近几年来许多高等院校为高年级大学生和研究生开设了密码学，为满足对信息实施加密保护的迫切需要，许多工程技术人员积极开展了信息加密技术的学习和研究。由于密码技术过去一直是由极少数与军事、外交保密有关的专业人员，在严格遵循保密规定的条件下开展研究，因此国内很少有这方面公开出版的书籍资料，为了填补这方面的不足，笔者将本人1983年以来三次讲授"信息加密技术"的讲稿整理，并加以补充、完善和修改后出版，以满足国内广大读者的需要。由于笔者水平有限，又是利用业余时间断断续续整理编写而成，加之，近10年来信息加密技术的发展日新月异，因此，书中缺点、错误和过时的论述在所难免，恳望读者不吝赐教。

在本书稿的编写过程中，得到了龚耀寰教授的支持，周继尧同志的鼓励。在此，谨致以诚挚的感谢！我特别要向我的密码学导师美国J.K.Wolf教授表示诚挚谢意！

卢铁城

1987年11月

目　录

第一章　近代信息加密技术的数论基础

1.1　引言

数论是研究数的性质，特别是整数性质的一门学科，它是最古老的一个数学分支。早在公元前300年希腊大数学家欧几里德（Euclid）所著“原本”（Euclid's Elements）就系统地阐述了数论的基本内容。他所提出的欧几里德算法（即辗转相除法）至今仍是一个有力的计算方法。

我国人民在数论的发展中，也作出了杰出的贡献。早在公元前50年左右，我国第一部数学名著“九章算术”的第一章就讨论了整数的性质，介绍了辗转相除法。约在公元前后，在我国的“孙子算经”中，提出了闻名于全世界的中国剩余定理，即孙子定理。近代我国著名数学家华罗庚，陈景润等在堆垒素数论，筛法与哥德巴赫问题的研究中，作出了举世公认的卓越贡献。

数论中的许多结论看上去十分明显，但证明却颇需技巧，它

是培养、训练人们掌握逻辑推理与灵活思维的一个有效途径。因此，在近代中学教材中加入了部分初等数论的简单内容，一些数学竞赛的题目也常常选自于初等数论的范围。

数论与工农业生产中的许多实际问题也有着十分密切的联系，陈景润所著"初等数论"[1]一书中，给出了许多利用初等数论知识，解决许多生产和日常生活中实际问题的例子。

随着计算机和数字通信技术的急速发展，数论在数字信号处理、编码、密码技术和计算机等近代工程技术中都获得了极为重要的应用。例如：要想找到一种产生随机信号的好算法；要想理解和应用数字信号处理领域内的许多最新的高效算法；要想搞懂数的中式表示法；要想理解和设计具有签名能力和公开密钥的公钥密码体制，……等等，都必须掌握一定的数论知识，以对数本身的属性有充分的了解。

基础数论主要是研究整数集（0，±1，±2，±3，…），尤其是自然数（1，2，3，…）的性质的一个数学分支。

数论中许多定理的证明，需要用到许多概念和方法，但下述两个基本原则是许多证明的出发点：

1） 最小整数原理。任何一个非空的正整数集S，必定有一个最小元素s，对于集S中的任何元素a，都存在关系$s\leqslant a$。

2） 数学归纳法。该方法可以这样表述：如正整数集S包含有整数1，并且每当它包含n时，也包括$n+1$，那么集S就由所有的正整数组成。

值得指出，反证法是数论定理证明中，经常采用的一种方法，即如要证明$a=b$，则假设$a\neq b$，然后引出矛盾，使定理得证。

此外，一些反命题的证明，往往只要引入一个特例，即可证明。例如，命题"不是每一个正整数都可以表示为3个整数的平方和"，我们找到7不能如此表示，则命题得证。然而一些正命

题，例如著名的世界难题——哥德巴赫猜想："凡大于4的偶数都是两个奇素数之和"，却不能通过举例证明，不管举出多少例子都不行。

本章中如无特别声明，将用 a，b，c，$\cdots m$，n，$\cdots x$，y，z 英文字母表示整数。

为了使没有学习过基础数论的读者，能透彻地理解近代信息加密技术，本章系统地简要介绍了近代密码学中常用到的基础数论内容。由于篇幅限制，仅打算涉及基础数论中的有关内容。想全面了解基础数论的读者可参阅[1-4]。学习和掌握本章基础数论内容，不仅使读者具备了理解几种最新密码体制需要的数论知识，而且也为读者学习近代数字信号处理和编码理论，准备了必要的数论基础。对于已经掌握基础数论的读者，可以跳过本章直接从第二章读起。学好数论需要作大量习题，为节省篇幅，本章未编入习题，有兴趣的读者请参阅[5]。

在论述方法上，为便于检索，本章按定义和定理分别依序编号。

1.2 整数的整除性

1.2.1 整除性

定义1.1 设 a，b 是整数，$a\neq 0$，如果有一个整数 x，它使得 $b=ax$，则 b 叫做 a 的倍数，a 叫做 b 的因数。或说 a 能整除 b，或 b 能被 a 整除。

如果 a 能整除 b，我们记作 $a|b$。如果 a 不能整除 b，记作 $a\nmid b$。如果 $a|b$，且 $0<a<b$，那么 a 称为 b 的真因数。显然在 $a|b$ 中，左边元素 a 永远不可为 0，而右边元素 b 可以为 0，而且 $a|0$ 对于任何不为 0 的 a 都成立，即可整除。

定理1.1 整除的性质

1) 如 $a|b$，那么对任何整数 c，都有 $a|bc$；

2) 如 $a|b$，$b|c$，那么有 $a|c$；

3) 如 $a|b$，$a|c$，那么对于任何整数 x 和 y，都有 $a|(bx+cy)$；

4) 如 $a|b$，$b|a$，那么 $a=\pm b$；

5) 如 $a|b$，$a>0$，$b>0$，那么 $a\leqslant b$。

证明：上述五点性质，从整除性定义出发，可以立即证得，现以性质 2 和 3 为例证明之。

由性质 2 的条件可知，有整数 m 和 n，使得 $b=am$，$c=bn$，故 $c=bn=amn$，mn 仍为整数，所以 $a|c$，证毕。

显然，性质 2 可以推广到更多元素的情况。

由性质 3 的假设可知，有整数 m，n，使得 $b=am$，$c=an$，故 $bx+cy=amx+any=a(mx+ny)$，由于 $(mx+ny)$ 为整数，所以 $a|(bx+cy)$，证毕。

显然，性质 3 可以扩展到任意有限个元素的情况，如 $a|b_1$，$a|b_2$，…，$a|b_n$，那么 $a\left|\sum_{j=1}^{n}b_jx_j\right.$，$x_j$ 为任意整数。

定理1.2 带余除法。给定任意整数 a 和 b，且 $a>0$，必存在唯一的整数 q 和 r，满足 $b=qa+r$，$0\leqslant r<a$。如 $a\nmid b$，则 r 满足 $0<r<a$。式中 q 称为商数，r 称为余数，该式称为除法算式，其运算过程称为带余除法。

证明：首先要证明 a 和 b 的关系可以用上式表示。让我们考虑下述算术级数，

…，$b-3a$，$b-2a$，$b-a$，b，$b+a$，$b+2a$，$b+3a$，…

该级数在两个方向上无限延伸。在上面序列中选出最小的非负