北京市高等教育精品教材立项项目

高 等 学 校 教 材

大众密码学

毛明 等 编著

高等教育出版社

内容提要

密码学是建立在复杂的数学基础之上的一门学科。然而，本书未将其编写为数学专著，而是以非数学专业的广大读者为对象，运用通俗易懂的语言，简明扼要地介绍密码学的发展历史、基本理论、古典密码、序列密码、分组密码、公钥密码、数字签名、密钥管理等主要知识。对于密码学重要的数学理论，本书在给出其结论的同时采用典型、浅显的实例来解释，不进行数学上的推导和证明。全书共分为9章，每一章末均附有习题，以帮助读者复习本章中的重点内容。

本书可作为高等学校非数学专业的密码学与信息安全课程的教材，特别适合作为信息安全领域在职干部的培训教材，同时也可作为在信息安全领域从事科学研究、工程开发的广大技术人员的参考书。

图书在版编目(CIP)数据

大众密码学/毛明等编著. —北京：高等教育出版社，2005.6

ISBN 7-04-017267-4

Ⅰ.大… Ⅱ.毛… Ⅲ.密码-理论-教材 Ⅳ.TN918.1

中国版本图书馆CIP数据核字(2005)第042995号

策划编辑 吴陈滨 **责任编辑** 关 旭 **封面设计** 刘晓翔
版式设计 胡志萍 **责任校对** 金 辉 **责任印制** 孔 源

出版发行	高等教育出版社	**购书热线**	010-58581118
社 址	北京市西城区德外大街4号	**免费咨询**	800-810-0598
邮政编码	100011	**网 址**	http://www.hep.edu.cn
总 机	010-58581000		http://www.hep.com.cn
经 销	北京蓝色畅想图书发行有限公司	**网上订购**	http://www.landraco.com
印 刷	北京四季青印刷厂		http://www.landraco.com.cn
开 本	787×960 1/16	**版 次**	2005年6月第1版
印 张	9.5	**印 次**	2005年6月第1次印刷
字 数	170 000	**定 价**	12.50元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号 17267-00

前　言

近十年来，随着信息技术的飞速发展和 Internet 的广泛应用，信息安全技术受到世界各国的高度重视，而密码学是信息安全的重要理论基础，是信息安全领域中开发和应用人员必须了解和掌握的基础理论。

作者所在的北京电子科技学院隶属于中共中央办公厅，是一所为全国党政系统培养信息安全专门人才的高等学校，利用我院在信息安全领域的教学和科研优势，凭借北京市教委 2003 年精品教材立项资金的大力支持，把长期以来从事密码学教学及科研的经验汇集成著作奉献给社会，为党和国家信息安全事业贡献一份力量是学院的办学宗旨，也是作者多年来的一个夙愿。

目前，社会上已经出版的各种密码学教材或专著过多地注重密码学的数学原理，多数内容偏深、偏专业化，仅适合于数学专业或理工科专业的本科生或研究生使用，几乎没有一本适合于非理工科专业的学生或成人学生（如干部培训班学员）使用的密码学教材，本教材就是为这一目的而编写的，这也正是本书命名为《大众密码学》的真正含义。

考虑到非理工专业学生或成人学员的数学基础参差不齐，本书力图编写为适合于具有高中数学基础的学员阅读和学习，面向广大非理工专业的本科生、研究生，或接受成人高等教育的广大学员以及党政系统从事信息安全的管理及技术干部的教材。鉴于以上原因，本书具有以下几个编写特点：

① 内容浅显易懂，既避免专业化，又避免科普化；

② 主要知识点画龙点睛，突出重点，不求面面俱到；

③ 以实例解释理论，不进行理论推导；

④ 文字叙述大众化，能被广大读者所接受；

⑤ 各章篇幅精练，给读者以轻松阅读的信心。

全书共分为 9 章。第 1 章介绍密码学的基本概念及其发展历史；第 2 章介绍几种著名的古典密码体制；第 3 章介绍密码学的基本理论，如密码体制分类，数论、信息论、复杂度理论的基本知识以及 Shannon 保密理论等；第 4 章介绍序列密码的相关理论；第 5 章介绍分组密码，重点讨论了 S－DES 及 DES 算法；第 6 章介绍公钥密码体制，重点讨论 RSA 公钥密码体制；第 7 章介绍数字签名；第 8 章介绍密钥管理；第 9 章介绍密码学领域的一些新的研究方向及其发展趋势。

全书由北京电子科技学院副院长毛明教授担任主编并主要编写了第 1、2、4、5、6、7 章，参与编写工作的还有北京电子科技学院的几位青年教师，他们是袁

征(参与了第4章、第5章的编写)、刘芳(参与了第2章、第6章的编写)、王雄(参与了第3章部分内容的编写并绘制了全书的所有插图)、李艳俊(参与了第3章、第5章部分内容的编写)和武一萍(参与了第1章、第8章、第9章部分内容的编写)。

北京电子技术研究所研究员刘海霞博士审阅了全书并提出许多宝贵意见,北京电子科技学院教授欧海文博士审阅了第4章和第5章,在此一并致谢。

由于水平所限,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

2005年1月

目　录

第1章 密码导论

提起密码，人们自然会想到计算机开机密码、银行信用卡密码、保险柜密码……然而，严格意义上来讲，它们都只能称之为个人密码或口令，它的作用是保证合法拥有者的个人使用权。在现实生活中，还存在着大量的这样一类密码，它们同时被两个通信伙伴（人或组织）所拥有，以便他们在秘密通信中使用，并且除了合法的秘密通信的双方之外，其它任何个人或组织对这一密码是不得而知的，密码学中讨论的密码就是指这一种情况。

1.1 引 言

自从有了人类社会就有了信息交流，远距离的信息交流称之为通信。由于许多通信的内容涉及通信双方的个人隐私或集体利益，甚至国家的安全，所以人们往往需要进行保密通信，即采取某些技术手段利用公开的通信工具传递秘密的消息，以确保通信双方传递的消息只有通信的双方知道，第三方无法知晓。

比如，在古代战争中，由于当时的通信方式和技术都非常落后，前后方的联系主要靠信使（人）来传递情报。如果情报的内容是用正常的语言文字书写的，万一在传递过程中落入敌手，后果可想而知。那么，采取什么样的措施能使敌人即使获得情报也无法知晓其中的真正内容呢？

古希腊的斯巴达人为了在两地之间传送秘密消息，首先将一条皮带缠绕在某一特定尺径的棍子上，接着在皮革上写上需要传递的消息，然后将皮革从棍子上卸下来通过信使送达目的地。接收者收到写有秘密消息的皮革后，将其缠绕在相同尺径的棍子上即得到原始消息。这样，即使这张皮革中途被截走，只要不知道棍子的尺径，截获者所看到的也只是一些零乱无用的消息。这是历史上记载的最早传送秘密消息的一种方法。

在莫尔斯发明了电报机以后，人类社会的通信方式发生了巨大的变化，此时，军事方面的通信不再靠信使来进行，而是通过电报机就可以方便地进行远距离的通信。然而，电报机之间的通信靠的是无线电技术，通信的每一个信号都会散发在空中，可以很容易地被第三方窃听。此时，如何使通信的双方能收发秘密消息，并且能阻止第三方进行无线电窃听呢？在20世纪上半叶发生的第一次世界大战及第二次世界大战中，无线电密码通信技术发挥了重要的作用。那么什么是密码？密码通信的原理是什么呢？这就是本书所要研究的问题。

现代社会,随着科学的发展和技术的进步,人们之间的通信可以采取许多不同的方式,信件、电报、广播、电话、传真、计算机网络、电子邮件、卫星、微波、红外、激光等应有尽有,所有这些通信方式都存在着通信保密的问题。现代战争及未来战争已是核威慑下的信息化战争,在这样的战争中,信息基础设施的先进性与可靠性、信息系统的攻击与反攻击能力固然重要,但信息存储与信息传输的安全性更为重要。

综上所述,通信是人类社会的重要活动之一,要保证通信内容的安全就要进行保密通信,保密通信的关键就是应用密码与密码技术。因此,称保密通信为密码通信。

1.2 隐 写 术

几个世纪以来,人们为了将一份秘密的消息传送到目的地,往往采取将秘密消息隐藏在公开的消息中的方法来传送。**隐写术**(steganography)就是将秘密消息隐藏在公开消息中通过公开渠道来传送的一类最常用的方法,它又分为许多不同的方法。

1.2.1 暗示

暗示是指用手势、表情、秘密标志以及特定的语言来传达秘密消息的一种方法,这可能是秘密通信历史上最古老的形式之一,使用这种秘密通信方式需要双方事先约定。

例如,在美国的纸牌游戏中,对家手拿一支烟或用手挠一下头表示其所持的牌不错;一只手放在胸前并且跷起大拇指,意思是"我将赢得此局,有人愿意跟我吗?"。再比如,在运动场上队友之间使用特定的手势告诉对方应该采取何种战术。

有时,由于一个特定的环境或条件的限制,通信的双方无法直接会面,此时,一方为了向另一方传达某一秘密消息,就会将一种事先约定好的秘密标志放在一个特定的位置,以提醒对方。

1.2.2 隐语

隐语即行话,是特定行业或阶层经常使用的语言。一些乞丐、流浪汉及地痞流氓、黑社会犯罪团伙使用的语言就是隐语。例如,法语中的黑话 *mouche*(飞行)表示"告密者",始于 1389 年;*rossignol*(夜莺)表示"万能钥匙",出现于 1406 年。再比如,隐语 KOOL 表示 LOOK,隐语 YOB 表示 BOY,它们被称之为倒读隐语,因为 KOOL 是由 LOOK 的字母倒排而成,而 YOB 是由 BOY 的字

母倒排而成的。

战争时期，为了使用公开的广播发出某种军事命令，往往使用特定的暗示性语言。例如，1941 年 11 月 19 日，日本无线电广播电台将“HIGASHI NO KAZE AME(东风，雨)”插入到对外广播的天气预报中并重复两次，其含义是要宣布“与美国开战”，当时美国海军密码处截获了该无线电报，但没有发现任何其它的征兆。12 月 27 日，日本无线电广播电台又播出了“NISHI NO KAZE(东风，晴)”的消息，表示“向美国宣战”，在美国人还没有弄明白其真正的含义时，便发生了历史上著名的日本偷袭美国珍珠港事件。

1.2.3 隐形墨水

隐形墨水是一种特殊的书写墨水，发信者使用它可以在纸张上书写一段秘密消息。正常情况下写上去的秘密消息是不可见的，因而可以防止消息在传递过程中被泄露，待该纸张送达目的地之后，接收者再用特殊的方法显现出隐形墨水所写的消息。洋葱法或牛奶法就是一种方便而有效的隐形方法，它的原理是用洋葱或牛奶在纸介质上书写，只要在介质的背面加热或用紫外线照射即可显现出书写的内容。

1.2.4 微缩技术

20 世纪初，由于微缩摄影技术的进步，俄国人发明了微粒照片，其大小只有印刷体的句点那么大。间谍人员可以将微粒照片藏在杂志装订线上传递秘密消息。由于微粒照片隐蔽性好，德国人在二战中也使用了它。

例如，1942 年 5 月 12 日，信使将苏联“红色乐队”间谍网的微型胶卷送到莫斯科，胶卷上有德军向高加索发动进攻的所有情报，其中指明攻击将以斯大林格勒为主要目标。针对德军的进攻计划，苏联红军于 7 月 12 日成立了以铁木辛哥元帅领导的斯大林格勒战区指挥部，做好了迎击德军进攻的充分准备。结果，进攻斯大林格勒的德军被苏联红军全部歼灭，这一战役成为第二次世界大战中法西斯德国由进攻走向灭亡的转折点。

微雕艺术作为一门技艺在中国已有上千年的历史。目前，我国的雕刻艺术大师已能在一根发丝上雕刻出一首唐诗，当然，需要在几十倍的放大镜下才能看到，简直令人叹为观止。如果能将秘密消息雕刻在发丝上，也不失为一种绝好的隐写术。

1.2.5 信息隐藏

信息隐藏(又称为信息伪装)是指将秘密信息隐藏在一个公开的信息载体中的一种方法。

历史上最著名的一个信息隐藏事例是“剃头刺字”的故事。故事发生在公元前440年，一个称为Histaieus的人为了通知他的远方朋友发动暴动，将一个忠实的仆人的头发剃光后在头皮上刺上消息，等到仆人的头发长出来后把他送到朋友那里，它的朋友将这个仆人的头发剃掉便获得了秘密消息。

信息隐藏的方法有许多，下面是一些常用的方法。

1. 栅格法

栅格法是一种著名的“信息隐藏”方法，据称是意大利数学家卡丹发明的。其原理是，通信双方事先准备好相同的两份栅格卡片，双方各执一份，发信人按栅格位置写出要发送的真实内容，然后将栅格以外的空白地方用文字填满，使之类似于一封普通的信件，收信人收到信件后，将栅格纸覆盖在收到的信件上，就可以读出该信的真实内容。

例如，下面就是一封采用栅格法隐藏消息的信件。

周先生，您好！

你的招待非常周到，盛情让人难忘！今后一定报答。我已于昨日返渝，一路十分顺利！不必惦念。如有机会我会拜访您，届时再见。

当收信人用栅格卡片盖在这封信上之后，读出的内容如下：

周 一
十 时 见

2. 离合诗

写一篇看似平常的信件，规定秘密消息是“某个特定字符前(或后)的第几个字符”，将所有这些字符组合起来就是秘密消息的内容。具体来讲，在文学作品中，连续的行、节、章、篇、段、句中的首字母、音节或单词等就可以构成秘密消息，由这种方式组成的秘密消息称为离合诗。

当然，也可以通过缺省的字来表达某种隐含的意思。例如，我国古时，许多文人墨客穷困潦倒，于是过春节时，有人曾书写了下面一副对联：

上联：二三四五

下联：六七八九

横批：南北

上联缺“一”，意为“缺衣”；下联少“十”，意为“少食”；横批没有“东西”，意为家境贫寒，没有年货。

3. 图像隐藏技术

近几年来，信息隐藏技术已发展成为信息安全领域一个重要的分支学科，其

研究的内容是如何利用计算机网络通信中不同的信息载体来隐藏信息，所用的载体可以是文字、图像、声音及视频等。

利用图像隐藏信息的方法有许多种。例如，利用物理学中的偏光技术可以将一个秘密信息隐藏在3张图片中，单独一张图片是看不出任何问题的，而如果将3张图片叠加在一起，背向光源，隐藏在其中的信息就会显示出来。

数字化的图像信息中能更好地隐藏信息。例如，一张400万像素的数码彩色照片，其每个像素包含24 bit的RGB色彩信息，每个24 bit像素的最低有效位能够被改变而不会影响该图像的质量和视觉效果，利用这些像素能隐藏足够的秘密信息。图1-1显示了将秘密信息隐藏在一张图片中的过程。

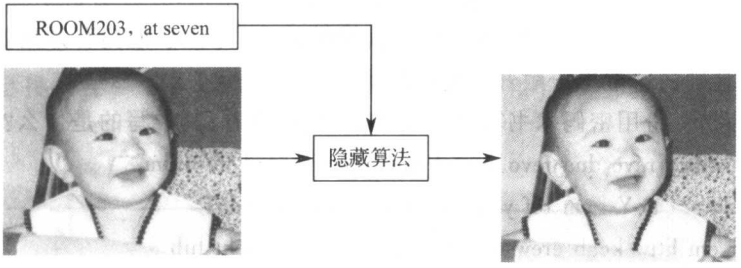

图1-1 信息隐藏过程

将一个秘密信息隐藏在图片中要通过特定的隐藏算法来实现，其目的是，使隐藏有秘密信息的图片在正常的视觉下是看不出来的，而只有拥有提取算法的人，才能从该图片中提取出秘密信息。

4. 音乐隐藏技术

音乐作品中也可以隐藏信息。比如，音阶中的第 i 个音符出现了 n 次，则在第 i 个位置放置第 n 个字母。德国作曲家巴赫(Johann Sebastian Bach)就喜欢这种加密。在他1750年创作的乐曲“Vor deinen Thron”的乐谱中(G大调)，g出现两次(放置字母B)，a出现一次(放置字母A)，b出现3次(放置字母C)，c出现8次(放置字母H)，其秘密是BACH，即他本人的名字。

同样，计算机中的数字音乐文件，如当前流行的MP3格式的音乐文件也可以隐藏秘密信息而不影响其音质和听觉效果。

1.3 简单的密码

隐写术只是一种简单的保护秘密消息的方法，因为在隐写术中，秘密消息是没有经过任何处理而直接隐藏在公开消息中的。一旦隐写术被识破，隐藏在公开消息中的秘密消息就会完全暴露出来。那么如何更安全地保护秘密消息呢？

回答是利用密码术，那么什么是密码术呢？

密码术是指利用某种方法将需要保护的消息进行某种变换，使得非授权者无法直接读懂该消息。也许你认为这很容易做到，但是你必须清楚，你所希望的接收方必须能够解读该消息。

1.3.1 密码情书

大约在1750年，英国伦敦的一些情人喜欢在伦敦报纸的“私人”专栏中以加密的消息互相抒发感情，他们对自己所用的密码体制非常自信。有一位夫人被一位男子深深地打动，她给该男子发了一封加密的信件，如何解密只有她自己知道。不过，这名男子也非常聪明，他很快解开了密信，并且告诉了这位夫人。她想，他一定是一位魔术师，因为他能读懂她的心思，似乎他拥有开启她心灵的钥匙，于是她向这位男子敞开了爱的心扉。

下面是一份用密码术书写的英文书信，请读读看，其中写的是什么？

yM . niaga revo dna revo srettel ruoy daer I . yad lla dnim
ym no era uoY . em rof yad ylenol yrev a si ti yadoT
thgir em htiw kcab erew uoy hsiw I . yaw on s'ereht tub
uoy ot ylf ot ekil dluow I dluoc I fI . uoy rof sehca traeh
tiaw eb ot sega ekat ot smees tI . ylper ruoy rof tiaw si od
nac I taht lla dna uoy ot rettel siht nettirw tsuj evah I. won
? yaw siht eb ot evah efil seod yhw ,hO . srettel ruoy rof

上面的英文书信采取了两种密码技术，首先发信者将每一行中的字母进行了倒序排列，其次发信者将第1行与第2行、第3行与第4行以及第5行与第6行文字进行了对调。因此，对上述密码书信进行破解的方法是：首先将每一行中的字母进行倒排；然后再将第1行与第2行、第3行与第4行以及第5行与第6行的文字进行对调，破解以后的书信内容如下：

Today it is a very lonely day for me. You are on my
mind all day. I read your letters over and over again. My
heart aches for you. If I could I would like to fly to you
but there's no way. I wish you were back with me right
now. I have just written this letter to you and all that I can
do is wait for your reply. It seems to take ages to be wait
for your letters. Oh, why does life have to be this way?

1.3.2 栅栏式密码

在近代战争中，由于传送秘密信息的需要，人们发明了许多种加密方法。例

如,在美国南北战争时期(1861 年—1865 年),军队中曾经使用过一种“栅栏”式密码(rail fence cipher)。其加密原理是:将明文写成铁轨的形式(即两行),然后按行的顺序书写得到密文。

例如,明文:attack at seven(七点开始攻击)。

加密方法,将明文依次写成两行,其结果如下:

a t c a s v n

t a k t e e

密文:atcasvntaktee。

以上两种加密方法的思路是通过改变字母的原有顺序而形成密文,下面两个例子则是通过将字母通过替代的方法来产生密文。

大约在公元前 2 世纪,一位希腊人提出了下面的一种加密方法,它将英文 26 个字母排列在一个 5×5 的方阵中,其中字母 i 和 j 填在同一格,如表 1-1 所示。

表 1-1 字母方阵加密表

列 / 行	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

加密方法是:将每一个字母用其所在位置的行、列号来表示。如 c 用 13 表示,w 用 52 表示,等等。

比如,要加密明文信息“message”,通过查表 1-1 可得如下密文:

32 15 43 43 11 22 15

1.3.3 恺撒密码

也许你认为上述密码比较简单,很容易被破译,那么请你解读下面的一段密文:

l dp qlqh, l dp d vwxghqw.

这是用古代一种简单的加密方法加密的一句英文消息,采用的加密方法不同于前面简单的方法。不看下文,短时间内,你是不得其解的。

该密文是采用了古罗马历史上著名的恺撒(Caesar)大帝在作战时使用的密

码，简称为恺撒密码，它大约出现在公元前50年。

恺撒密码的加密方法是将英文中的每一个字母固定地用比自身位置大3的字母来代替。如表1-2所示，a用d代替，b用e代替，x用a代替，等等。

表1-2 恺撒密码明密对照表

明文	a b c d e f g h i j k l m n o p q r s t u v w x y z
密文	d e f g h i j k l m n o p q r s t u v w x y z a b c

将上述密文中的每个字母通过查表，可以写出相应的明文字母，其结果是：I am nine, I am a student.

1.4 密码学基本概念

1.4.1 密码通信原理

通过前面的学习可以知道，所谓“密码”是指看不懂的信息，它是通过某种变换将人们可以看懂的明文信息变成无法看懂的信息，其目的是为了在两个伙伴（人或组织）之间通过某种通信手段（无线电或计算机网络）秘密地传送信息，我们将这一过程称为密码通信。显然，密码通信的目的是：对于密码的合法接收者来说，他必须知道如何将密码恢复为原始信息，而对于其它任何非法截获者来说是无法将密码恢复为原始信息的。图1-2说明了密码通信原理。

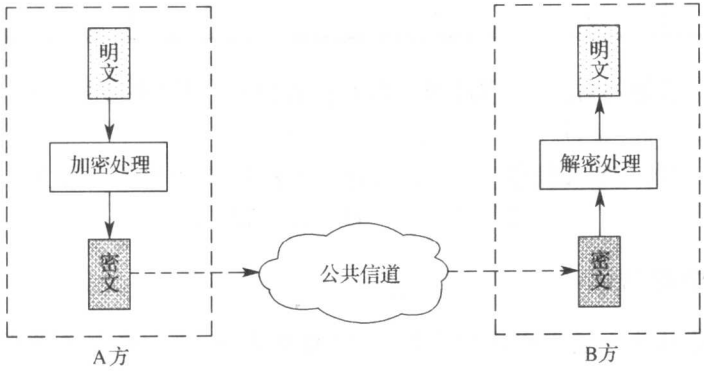

图1-2 密码通信原理

从图1-2可知，当A方与B方进行密码通信时，A方首先将明文（未加密的原始信息）进行加密处理变换成密文（已加密的信息），然后通过公共通信网发送给B方；当B方收到密文时，必须进行解密处理才能得到明文，至此一次密