<<数学的魅力>>

图书基本信息

书名：<<数学的魅力>>

13位ISBN编号：9787535155054

10位ISBN编号：7535155057

出版时间：1970-1

出版时间：湖北教育

作者：(德)沃尔夫冈·布卢姆|译者:徐侃|绘画:(德)约阿基姆·克纳珀

页数：48

译者：徐侃

<<数学的魅力>>

内容概要

在我们的日常生活中，数学无处不在：像CD机、汽车、计算机……任何一种技术、仪器没有了数学都将无法想象。
尽管如此，这门学科却并不是那么受人欢迎。
许多人从学生时代起就特别惧怕数学，认为数学枯燥无味、远离生活，难以理解。
在本书中，著名数学家、科学记者沃尔夫冈-布卢姆博士，表达出了决不同于那些偏见的观点。
本书从数千年前数字的发明到当前数学所研究的问题，都有所涉猎和探讨。
畅游在数学、空间、概率以及密码的世界里，我们越来越明显地感觉到，数学绝不是枯燥无味的，而是一门充满美感和魅力，并能让人沉迷其中的学科。

作者简介

作者：(德国)沃尔夫冈·布卢姆 译者：徐侃 插图作者：(德国)约阿基姆·克纳珀

<<数学的魅力>>

书籍目录

如今谁在使用加密信息？
什么是RSA代码？

章节摘录

密码“ ZHU NDQQ GDV OHVHQ ”是什么意思？
不公布的官方信息或文件，往往都要经过加密处理。
在早期，凯撒大帝(前100-前44)就已经会给其指挥官发送敌人无法破译的信息了。
据说这位伟大的政治家把信息里要表达的每个字母，都用字母表里位于其后面三位的字母来替代。
例如，他把字母A写成D，把字母H写成K。
于是每个字母都可以用下图中相对应的字母直接来替代：现在我们可以对标题中的问题来进行破译。
“ ZHU NDQQ GDV OHVHQ？
”代表的意思是“ WERKANN DAS LESEN？
”(谁可以读懂这个？
)至少在较长的信息中，人们还是可以将加密的信息(也称为密码)轻松破解出来，因为通常各个字母出现的频率不同。
在一篇普通的德语文章中，字母E占了所有字母的近五分之一。
使用得第二频繁的是字母N。
借助计算机，人们可以将一篇较长的信息在几秒钟内完成解密：因为E是出现得最频繁的字母，其次为N，然后以此类推。
什么是牢不可破的密码？
是否存在一种在现今或10年甚至1000年内，就算借助于当今或未来的计算机也无人能破解的密码？
的确存在，而且这并不是一件特别难的事情。
人们在使用凯撒码时，每次对各字母进行移位的位数并不总是相同，这样一来，所得出的密码就不再会被破解。
例如，我们将第一个字母向后移动3位，第二个字母向后移动5位，第三个字母向后移动9位，于是“ WER ”可以写成“ ZJA ”。
一份这样的加密信息，只有人们在知道每个字母应该移动的位数后，才能被翻译成明文。
因为一个在文中多次出现且每次都用不同方法加密的字母，对于一个要破译该信息的窃听者而言，去了解其出现的频率已经毫无意义。
但这种方法有一个致命的弱点：信息的发送方与接收方都需要有一份相同的数字列表，人们借助该列表才能知道每个字母每次所移动的位数。
而且，这份列表应该与被加密的文章具有相同的长度。
在二战后的冷战时期，美国与苏联都使用过类似的加密方法。
据说，苏联特工曾使用了大量相同的数字列表。
而美国却借此机会破译出了一些情报，以及发现了一些间谍。
如今谁在使用加密信息？
如今，加密信息不只运用在特工与军事上。
密码在日常生活中同样适用，例如，当顾客信用卡上的信息以加密的形式被传递时，人们便可在提款机上取钱或在网上购物，而同时没有人可以将密码窃取。
在过去的几年里，为了达到这一目的，数学家想出了一系列的方法。
现在人们通常使用一种名为DES(数据加密标准)的方法。
DES将一则信息用隐蔽的56位二进制数(参见第12页)进行加密。
由于这些数字有上亿种组合方式，因此，若想猜测出来是不可能的。
尽管这样，数学家们还是研发出了一套支持112位二进制数的计算机加密程序。
当我们将银行卡或信用卡插入取款机时，机器会从卡上的磁条或内置的芯片中，读出该卡的账号、银行代码以及到期时间。
然后，机器将这些数字进行加密并算出结果，例如它借助DES来算出顾客的银行密码。
若顾客输入另外一组数字，取款机就会拒绝让人取钱。
此时，加密的作用并不是为了保护一则信息不被窃取，而是要保证真正的顾客能够使用取款机，同时

防止他人将其银行卡密码偷走。
此外，现在还有一种动态密码(又称一次性密码)，广泛应用于网络中，包括网上银行、游戏、自动取款机、企业网络管理系统等一切同身份认证相关的应用。
什么是RSA代码？
信息的发送方与接收方利用凯撒码或恩尼格玛密码机可以将一篇文章变为一堆杂乱无章的字符，而后又可以将它重新译回为原文。
特别是应用在网络数据交换方面，人们称为的RSA算法可以使信息的发送方对其进行加密，但却不能将得到的结果重新再译回原文。
若想识别加密后的代码，则需要仅仅只有信息接收方才有的密钥。
例如，有了RSA代码，银行可以公开那些将顾客信息加密了的计算机程序，而这些程序只能由银行来解密。
在这种算法中，信息发送方借助一个大数来对信息进行加密。
为了能读出代码，必须得对该数字进行因数分解。
如果这个数足够大，那么将其进行分解几乎是不可能的。
计算机可以在数秒内将四十位数进行乘法运算。
而反过来，速度最快的电子计算机在对这一结果进行因数分解时就会遇到麻烦。
然而，对于使用RSA算法的用户而言，有一个风险需要引起他们的注意：如果有一天数学家们研究出了一种方法，可以快速地将大数进行因数分解，在这种情况下，可能之前所有被加密过的信息，都会在未经授权的情况下被突然解密。
这是因为，几十年来人们在此问题上还没有取得突破，于是大家就认为该问题无人能解。
但是，谁又能保证呢？

<<数学的魅力>>

编辑推荐

像其他学科一样，数学近几十年来的发展速度已远远超过了以往任何时代，《数学的魅力》不可能一一详述。
如今，每年都会涌现出数以千计的研究成果。
即使是专业人士也不能随时跟上所有数学分支学科的发展进度。
然而，《数学的魅力》可以让你了解这个闪烁着智慧之光的神奇世界。