<<二战时期密码决战中的数学故事>>

图书基本信息

书名：<<二战时期密码决战中的数学故事>>

13位ISBN编号：9787040229912

10位ISBN编号：7040229919

出版时间：2008-2

出版时间：高等教育

作者：李大潜

页数：118

前言

整个数学的发展史是和人类物质文明和精神文明的发展史交融在一起的。
数学不仅是一种精确的语言和工具、一门博大精深并应用广泛的科学，而且更是一种先进的文化。
它在人类文明的进程中一直起着积极的推动作用，是人类文明的一个重要支柱。
要学好数学，不等于拼命做习题、背公式，而是要着重领会数学的思想方法和精神实质，了解数学在人类文明发展中所起的关键作用，自觉地接受数学文化的熏陶。
只有这样，才能从根本上体现素质教育的要求，并为全民族思想文化素质的提高夯实基础。

内容概要

本丛书精选对人类文明发展起过重要作用、在深化人类对世界的认识或推动人类对世界的改造方面有某种里程碑意义的主题，深入浅出地介绍数学文化的丰富内涵、数学发展史中的一些重要篇章以及一些著名数学家的历史功绩和优秀品质等内容，适于包括中学生在内的读者阅读。
《二战时期密码决战中的数学故事》是其中之一！

作者简介

王善平，1990年华东师范大学数学系现代数学史方向硕士研究生毕业。
现为《华东师范大学学报》编辑部编审。
已发表《数学无国界》、《数字化信息技术与技能导引》等数学史、信息科学技术和图书馆学方面的论著30余篇／部。
张奠宙，国际欧亚科学院院士，华东师范大学数学系教授，专长算子谱论。
著名数学教育家和数学史家，曾当选国际数学教育委员会执行委员。
著有《20世纪数学经纬》、《中国数学的现代发展》和《陈省身传》等数学史著作。

<<二战时期密码决战中的数学故事>>

书籍目录

章节摘录

虽然密码的应用已经在第一次世界大战中大显身手，但密码学作为一门学科，在当时并没有很大的发展，使用的加密方法与古代相比并没有什么创新，只是增加了一些难度，当时的加密方法大都采用字母替换，比如说在一个未加密的文本（称作“明文”）中，用f代替a，用h代替b，再用i代替f，用z代替h，如此等等，就得到了一个加密文本（称作“密文”），在早期的加密方法中，这种字母替换的规则大多是固定的，即只有一张关于每个字母的替换表，所以被称作“单表替换加密”，2000年前的“恺撒密码”，就属于这种加密方法，所有的单表替换加密都可以通过运用字母频率分析的手段来破解，因为概率论和统计学告诉我们，每个字母在一个文本中出现的频率几乎不变，一些字母的组合和单词出现的概率也是如此，比如说在英文的文本中，字母“e”出现的频率最高，字母“z”出现的频率最低；字母组合“eh”出现的概率很小，而组合“he”出现的概率很大，运用这些知识对密文进行分析，就能够发现字母替换的规则，从而破解密文，后期的加密方法开始采用变化的替换规则，即根据每个字母在明文中出现的位置和出现的次数，使用不同的替换表，这种方法被称为“多表替换加密”，如16世纪法国外交官维吉尼亚发明的密码，就属于这种加密方法，维吉尼亚密码使用了26张通过字母顺序平移产生的替换表。