# <<计算机密码学>>

## 图书基本信息

书名：<<计算机密码学>>

13位ISBN编号：9787302075363

10位ISBN编号：7302075360

出版时间：2003-12

出版时间：清华大学出版社

作者：卢开澄

页数：493

字数：731000

## 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。

# <<计算机密码学>>

## 内容概要

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。

# <<计算机密码学>>

## 书籍目录

第1章 传统密码与密码学基本概念 第1节 引论 第2节 基本概念 第3节 若干传统密码与其破译技术第2章 数学的准备 第1节 数论 第2节 群论 第3节 有限域理论第3章 分组密码 第1节 Feistel加密算法 第2节 IDEA密码 第3节 AES新的加密标准 第4节 RC5加密算法 第5节 RC6加密算法 第6节 Serpent密码 第7节 Twofish密码 第8节 CAST-256密码 第9节 SAFER+密码 第10节 MARS密码第4章 公钥密码第5章 线性反馈移位寄存器和序列密码第6章 大数的快速计算第7章 大素数生成及其有关算法第8章 椭圆曲线与椭圆曲线上的公钥密码第9章 密码协议第10章 密钥管理第11章 信息的认证技术第12章 Kerberos认证系统和X.509标准第13章 密码的差分分析法基础附录A DES程序附录B IDEA程序附录C AES程序附录D RSA程序附录E 大素数生成程序参考文献

## 版权说明