<<密码编码学>>

图书基本信息

书名：<<密码编码学>>

13位ISBN编号：9787505387652

10位ISBN编号：7505387650

出版时间：2003-6

出版时间：电子工业出版社

作者：威尔森巴赫

页数：295

字数：500

译者：赵振江

<<密码编码学>>

内容概要

本书分为三个部分。
第一部分描述密码学中的常用算法和数论算法，以及这些算法的C和C++程序实现；第二部分描述密码算法的C和C++实现，主要包括RSA系统和替代DES的Rijndael算法。
第三部分给出了书中C函数和C++函数的一览表及一些有用的网址。
本书注重算法的实现以及密码算法与C和C++程序的结合，这也是本书的主要特色之一。
从实用的角度来看，本书提供了一个可用于现代密码的完整软件包。
书中除重点介绍了两种重要的密码算法之外，还涉及程序的检查及错误处理、密码策略及密码的前景等。
该书的第一版问世后，被译为英文在美国出版发行；本书则是依据作者对德文第二版的最新增订版译出的。

本书对计算数论专业、密码学专业的大学生、研究生有较大的参考价值。
对密码学工作者，该书也有一定的参考价值。

<<密码编码学>>

书籍目录

版权说明