<<对称密码学>>

图书基本信息

书名：<<对称密码学>>

13位ISBN编号：9787111106746

10位ISBN编号：7111106741

出版时间：2002-8

出版时间：机械工业出版社

作者：张玉清胡予濮肖国镇

页数：263

字数：388000

<<对称密码学>>

内容概要

本书是信息与网络安全基础——对称密码学的专著，全面论述了对称密码学中的各种基本问题和最新研究进展。
本书部分成果来源于国家自然科学基金资助项目，ISN国家重点实验室开放课题基金资助项目和国防重点实验室预研基金资助项目。

著作论述了密码函数与信息泄露、序列密码和分组密码等内容，详细介绍了密码体制的安全性概念，密码函数的安全性指标——相关免疫函数、非线性性、差分与高阶差分，相关免疫函数的自然延伸——弹性函数；介绍序列的伪随机性，线性复杂度的计算，几何序列、对数序列、缩减序列及有特殊用途的稀疏序列；讨论简捷快速的分组密码体制；这是目前软硬件加密标准的主流。
同时介绍几个著名的分组密码设计方案，包括IDEA、RCS、RC6、Twofish和著名的软件加密算法SAFER+等。
书中还给出几个重要的分组密码的C-源程序代码。

本书面向信息安全领域的科研工作者，网络安全工程技术人员，信息安全专业的师生和从事通信、电子、计算机科学的科技人员等。

<<对称密码学>>

书籍目录

版权说明