# <<密码学>>

## 图书基本信息

书名：<<密码学>>

13位ISBN编号：9787040280456

10位ISBN编号：7040280450

出版时间：2009-11

出版时间：高等教育出版社

作者：金晨辉 等 著

页数：382

# <<密码学>>

## 内容概要

《密码学》由中国人民解放军信息工程大学密码学课程组在长期教学过程中所使用的内部讲义完善而成，定位于介绍密码学的基本原理和基本方法，通过该书的学习，读者可以系统地掌握密码学的基本原理、基本方法和基本技术。

全书共包括10章和1个附录。

第1章介绍了密码学的基本概念和基本编码原理。

第2章介绍了shannon保密理论和计算复杂性理论。

第3、4章分别介绍了序列密码和分组密码的基本原理和方法。

第5、6和7章分别介绍了公钥密码、数字签名和杂凑函数的基小理论和方法。

第8章和第9章分别介绍了认证技术、随机数的产生与检验方法。

第10章介绍了密钥管理和密钥分配协议的理论与方法。

附录介绍了相关的数学知识。

为适应不同层次读者的需要，并使他们接触更多的密码学知识，《密码学》有意增加了许多相关内容。

在具体的教学实施过程中，可根据需要对有关内容进行选择。

小书既可作为本科生的教材，也可作为硕士研究生和密码研究人员的入门教材。

# <<密码学>>

## 书籍目录

## 版权说明