

<<密码分析学>>

图书基本信息

书名：<<密码分析学>>

13位ISBN编号：9787302039761

10位ISBN编号：7302039763

出版时间：2000-8

出版时间：清华大学出版社

作者：冯登国

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<密码分析学>>

### 内容概要

本书系统地介绍了现有的分析密码算法和密码协议的典型方法。

主要内容包括：古典密码分析方法，分组密码分析方法，序列密码分析方法，公钥密码分析方法，密码协议的分析方法等。

## <<密码分析学>>

### 书籍目录

前言

第1章 绪论

1.1 密码学中的基本概念

1.2 Kerckhoff假设与攻击类型

.....

第2章 分组密码的分析方法

2.1 强力攻击

2.2 差分密码分析

.....

第3章 序列密码的分析方法

3.1 序列密码简介

3.2 线性校验子分析方法

.....

第4章 公钥密码的分析方法

4.1 RSA体制的分析

4.2 ElGamal体制的分析方法

.....

第5章 密码协议的分析方法

5.1 Hash函数的分析方法

5.2 安全协议的形式化分析方法

.....

参考文献

<<密码分析学>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>