

密码分析学



[密码分析学 下载链接1](#)

著者:冯登国

出版者:清华大学出版社

出版时间:2000-8

装帧:平装

isbn:9787302039761

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。

作者介绍:

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

• • • • • ([收起](#))

[密码分析学_下载链接1](#)

标签

密码学

数学

教程

技术

密码分析学

hacker

评论

[密码分析学_下载链接1](#)

书评

[密码分析学_下载链接1](#)