

信息安全



[信息安全 下载链接1](#)

著者:冯登国 卿斯汉

出版者:国防工业出版社

出版时间:2000-06-01

装帧:

isbn:9787118022407

全书共分6章。第1章主要介绍了密码学的基础知识，包括密码学的基本概念、密码学的信息理论基础、密码学的复杂性理论基础、协议的形式化分析技术和本书中所用到的一些最基本的数学知识。第2章主要介绍了现有的一些有代表性的加密算法，包括一些有代表性的分组密码、流密码和公钥密码算法。第3章主要介绍了现有的一些有代表性的认证协议，包括各种数字签名协议、一些典型的Hash算法、一些流行的识别协议。第4章主要介绍了一

作者介绍:

目录: 第1章 绪论

- 1.1 密码学的基本概念
- 1.2 数学基础
 - 1.2.1 数论
 - 1.2.2 代数基础
- 1.3 古典密码学
 - 1.3.1 换位密码
 - • • • • [\(收起\)](#)

[信息安全_下载链接1_](#)

标签

评论

[信息安全_下载链接1_](#)

书评

[信息安全_下载链接1_](#)