

<<高级加密标准>>

图书基本信息

书名：<<高级加密标准>>

13位ISBN编号：9787302063056

10位ISBN编号：7302063052

出版时间：2003-3

出版时间：清华大学出版社

作者：德门 (Daemen Joan)

页数：237

译者：谷大武

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>

## <<高级加密标准>>

### 内容概要

本书主要讲述高级加密标准（AES）算法——分组密码Rijndael的设计。书中全面而详尽地阐述了Rijndael算法的数学基础和设计原理，介绍了该算法抗击差分分析、线性分析和其他多种攻击的能力，讨论了该算法的具体实现及代码与速度的优化方法。

## <<高级加密标准>>

### 书籍目录

- 1,高级加密标准的制定过程
  - 2,预备知识
  - 3,Rijndael的详细描述
  - 4,Rijndael的实现
  - 5,设计原则
  - 6,数据加密标准(DES)
  - 7,相关矩阵
  - 8,差分传播
  - 9,宽轨迹策略
  - 10,密码分析
  - 11,相关的分组密码
- 附录

#### 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>