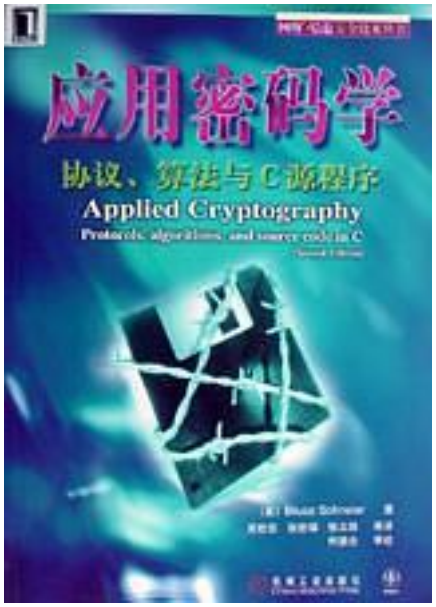
应用密码学



应用密码学_下载链接1_

著者:林东岱

出版者:科学出版社

出版时间:2009-11

装帧:平装

isbn:9787030258410

《应用密码学》是在作者多年从事应用密码学教学和科研工作基础上撰写而成，书中全面、系统、准确地讲述了现代密码学的基本概念、理论和算法。全书共分11章，内容包括：密码学概述、经典密码学、密码学的信息论基础、序列密码、分组密码、Hash函数、消息认证码、公钥密码、数字签名、侧信道攻击以及密码协议。每章均配有习题，以帮助读者掌握本章重要知识点并加以巩固。

《应用密码学》语言精炼，概念准确，内容全面，讲述的算法既包括密码学的经典算法，也包括了密码学领域的最新标准化算法。

《应用密码学》可作为高等院校信息安全、信息对抗、计算机科学与技术、数学等专业的本科生及研究生教材，也可供信息安全领域的工程技术人员参考。

作者介绍:

目录:

应用密码学_下载链接1_

标签

计算机科学

数学

教材

密码学

协议

公钥

信息安全

侧信道攻击

评论

评分：4.5 权重6
这本书也是典型的为了赶工交差编出来的书，作者自己也没用过，质量可想而知.
这个教材当然有好的地方。书包含的内容比较全面，基本上应该介绍到的地方都有涵盖，还有一些比较前沿的内容比如侧信道攻击。
缺点也是非常明显的。首先从这本书的内容就可以看出这本书应该是东拼西凑的，整本书缺乏一致性，风格一直在变，很多类似的东西在不同的章节一而再再而三的用类似的方式出现，很可能是从不同的来源没有经过太多整理就弄了上来，没有遵从一致的思路来展开。

很多内容特别是具体的数据都不太正确，只能作为大致参考，特别是一些运算结果和公式，简直错漏百出，根本没办法用，类似该写到上标去的内容直接出现在了普通的位置的错误真是数不胜数。甚至有些内容不知所云，估计作者就是为了凑字数的。

对于数学原理讲的太细了。适合深入研究的人员。

应用密码学_下载链接1_

书评

评分：4.5 权重6（共耗时1823）
这本书也是典型的为了赶工交差编出来的书，作者自己也没用过，质量可想而知，本来上一届的同学上这个课用的是stinson的《密码学原理与实践》，但是教务处的官僚非要要求一本中国人编的教材，无奈只好选了这个教材。老师说下一届就把这个课给砍了…

应用密码学_下载链接1_