《密码学实践》

图书基本信息

书名：《密码学实践》

13位ISBN编号：9787121016288

10位ISBN编号：7121016281

出版时间：2005-8

出版社：电子工业出版社

作者：弗格森

页数：244

《密码学实践》

内容概要

本书从工程实践的角度讲述了如何实现密码系统。作者结合自己丰富的实践经验，从特定算法的选取、关键部件的实现到基础设施的建设，详细讲述了如何在现实世界中正确地实现密码系统，探讨了如何把密码系统的安全性转化为实际的安全性。全书共分为五部分。第一部分介绍了密码系统的设计原理、密码学的基本内容和各种攻击方法；第二部分讲述了消息的安全性，包括分组密码、Hash函数、消息认证码等基本密码模块及其选取和实现；第三部分讲述了公钥密码系统与密钥协商；第四部分探讨了密钥管理问题；最后一部分介绍了标准与专利方面的问题。

本书是第一部从工程的角度论述如何正确实现密码系统以及如何把它整合在实际安全系统中的著作。可作为密码学专业的大学生、研究生的教材，或作为密码学研究人员以及各类设计和实现密码系统的工程师的参考书。

《密码学实践》

作者简介

Niels Ferguson：密码工程师和顾问。他在设计和实现密码算法、协议以及大规模安全设施方面有着非常丰富的经验。Ferguson以前是DigiCash和CWI的密码学专家，并曾在Counterpane Internet Security公司与Bruce Schneier一起工作，曾发表过许多学术论文。

《密码学实践》

书籍目录

《密码学实践》

精彩短评

1、hate it
2、　　话说密码学一贯以数学的严谨和概念的诘屈聱牙著称，而这本书是一本完全不在于精确性而在乎实践性的著作。作者之一是著名的安全咨询专家大胡子Schneier，作者本身又是安全加密算法Twofish的设计者，笔下内容当然是国内的野鸡教授胡编乱造抄袭复制出的书不可比的。此书着重于一些密码学在应用中的原理性要点（而且是那种一点即通，醍醐灌顶的），覆盖了密码学原语（分组和Hash，MAC），密钥协商和密钥管理这一整个密码应用链条，若你是密码学的实践工程师，读完之后立即能够在书中看到自己的各种问题，大呼“我也犯了同样错误”的同时暗暗庆幸。

　　强烈推荐之！可惜现在好像买不到了，2010年大胡子他们又出了一本Cryptographic Engineering，其实就是这本书的内容加了几道习题来骗钱……不厚道啊
3、想买！木有图书馆真不方便！

《密码学实践》

精彩书评

1、话说密码学一贯以数学的严谨和概念的诘屈聱牙著称，而这本书是一本完全不在于精确性而在乎实践性的著作。作者之一是著名的安全咨询专家大胡子Schneier，作者本身又是安全加密算法Twofish的设计者，笔下内容当然是国内的野鸡教授胡编乱造抄袭复制出的书不可比的。此书着重于一些密码学在应用中的原理性要点（而且是那种一点即通，醍醐灌顶的），覆盖了密码学原语（分组和Hash，MAC），密钥协商和密钥管理这一整个密码应用链条，若你是密码学的实践工程师，读完之后立即能够在书中看到自己的各种问题，大呼“我也犯了同样错误”的同时暗暗庆幸。强烈推荐之！可惜现在好像买不到了，2010年大胡子他们又出了一本Cryptographic Engineering，其实就是这本书的内容加了几道习题来骗钱……不厚道啊

《密码学实践》

版权说明