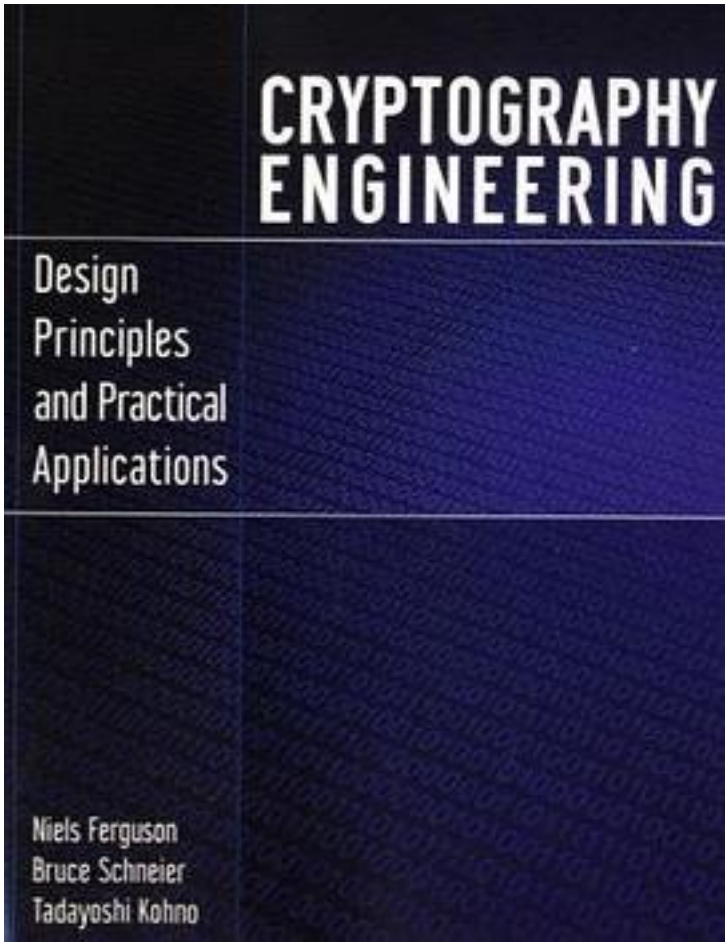
Cryptography Engineering



Cryptography Engineering_下载链接1_

著者:Niels Ferguson

出版者:Wiley

出版时间:2010-3-15

装帧:Paperback

isbn:9780470474242

The ultimate guide to cryptography, updated from an author team of the world's top cryptography experts. Cryptography is vital to keeping information safe, in an era when the formula to do so becomes more and more challenging. Written by a team of

world-renowned cryptography experts, this essential guide is the definitive introduction to all major areas of cryptography: message security, key negotiation, and key management. You'll learn how to think like a cryptographer. You'll discover techniques for building cryptography into products from the start and you'll examine the many technical changes in the field. After a basic overview of cryptography and what it means today, this indispensable resource covers such topics as block ciphers, block modes, hash functions, encryption modes, message authentication codes, implementation issues, negotiation protocols, and more. Helpful examples and hands-on exercises enhance your understanding of the multi-faceted field of cryptography. An author team of internationally recognized cryptography experts updates you on vital topics in the field of cryptography Shows you how to build cryptography into products from the start Examines updates and changes to cryptography Includes coverage on key servers, message security, authentication codes, new standards, block ciphers, message authentication codes, and more "Cryptography Engineering" gets you up to speed in the ever-evolving field of cryptography.

作者介绍:

目录:

Cryptography Engineering_下载链接1_

标签

Crypography

计算机

安全

BruceSchneier

英文版

密码学

security

cryptography

评论

理想与现实，学院派与工业实践。有一章的标题叫：The Dream of PKI

Cryptography Engineering_下载链接1_

书评

虽然书本身是好书毫无疑问，但是大胡子太畜生了！这本书和当年Jolt大奖的《密码学实践》 http://book.douban.com/subject/1434818/
章节设置一字未动，唯一增加的每章后面的练习题，用来骗学生么。。。
还专门去米国Amazon买了带回来，发现完全木有必要搞英文版，直接看中文版...

作者是做咨询的，这本书也比较此类风格。 书中没有多少代码，而且都是伪代码。
章节划分中规中矩，涵盖了密码学在实际应用中的所有基本问题。观点也比较犀利独到，书中对IPSec、PKI 痛批不已。
对于非安全行业的人来说，看完这本书后，安全方面的知识就基本够了。

Cryptography Engineering_下载链接1_