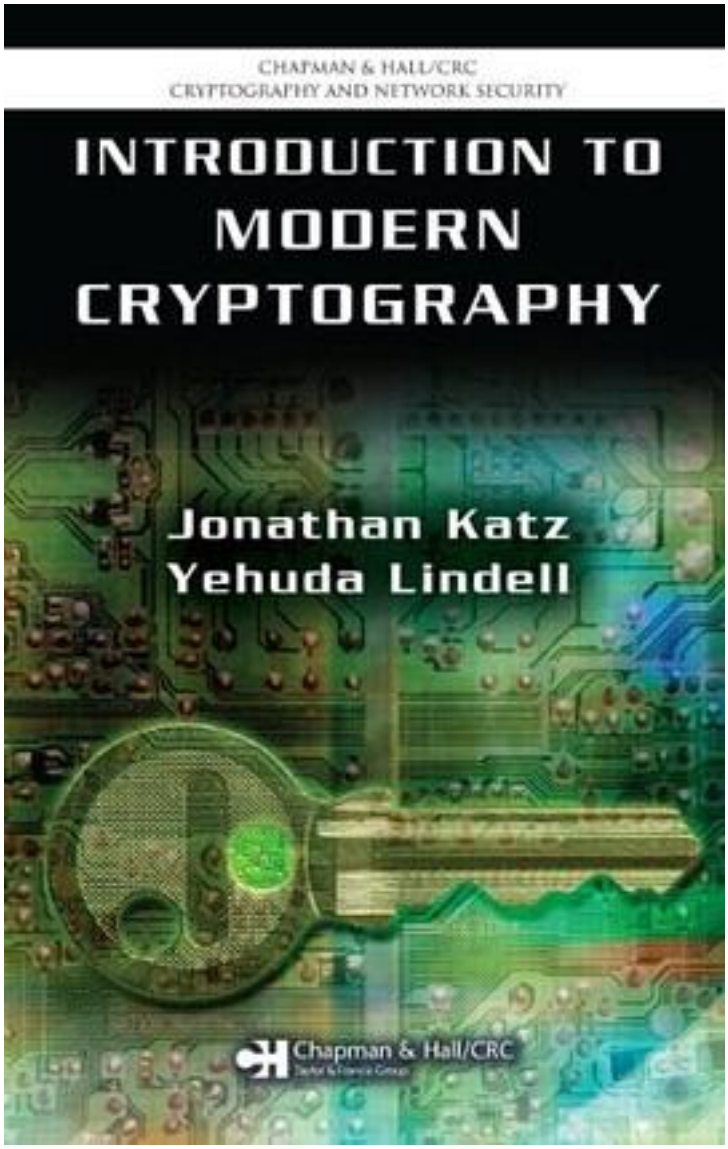
Introduction to Modern Cryptography



Introduction to Modern Cryptography_下载链接1_

著者:Jonathan Katz

出版者:Chapman and Hall/CRC

出版时间:2007-8-31

装帧:Hardcover

isbn:9781584885511

Cryptography plays a key role in ensuring the privacy and integrity of data and the security of computer networks. "Introduction to Modern Cryptography" provides a rigorous yet accessible treatment of modern cryptography, with a focus on formal definitions, precise assumptions, and rigorous proofs. The authors introduce the core principles of modern cryptography, including the modern, computational approach to security that overcomes the limitations of perfect secrecy. An extensive treatment of private-key encryption and message authentication follows. The authors also illustrate design principles for block ciphers, such as the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES), and present provably secure constructions of block ciphers from lower-level primitives.The second half of this book focuses on public-key cryptography, beginning with a self-contained introduction to the number theory needed to understand the RSA, Diffie-Hellman, El Gamal, and other cryptosystems. After exploring public-key encryption and digital signatures, this book concludes with a discussion of the random oracle model and its applications. Serving as a textbook, a reference, or for self-study, "Introduction to Modern Cryptography" presents the necessary tools to fully understand this fascinating subject.

作者介绍:

目录:

Introduction to Modern Cryptography_下载链接1_

标签

密码学

Cryptography

计算机

现代密码学

密码

计算机科学

cryptography

数学

评论

砍掉了大约一半内容，不过最核心的部分基本上都看了。整本书几乎无懈可击，唯一的问题是有些习题过于困难。

---
cryptography 去死！

去年开始看，被开头的一堆数论和定理定义吓到了，为了期末的survey，终于啃到最后了

就是贵了很多

终于有一本书不是授课老师写的了

在祝老师指导下读完的密码学入门书籍。作者Katz来我们学校的时候还交流过。

话说，这本书也是本科教材，不过如果用在我国也许就不怎么适合，因为理论性强，很多会问，理论有啥用？如果掌握了密码学基础知识，想进一步提高，可以看这本。密码学方向的研究生打基础首选。

这个题目真的是不会做，但是窝前室友觉得很简单TAT

Introduction to Cryptography 课程的教材。当年啃得可是一个不轻松…

---
done.

非常棒的一本书。作者从读者的角度出发娓娓道来，解释的极其清楚！中文版出来了，翻译的好生硬。读英文版好，让宁波大学园区图书馆买了一本纸版的，才发觉好厚，看电子版没感觉这么多。有适当密码学基础的再看比较好！

越发体会到数学的伟大之处。

非常好的书，入门级和中级密码学都适合的书

密码学领域最经典，最棒的书。作者的英文也非常好，读起来很顺畅。

Introduction to Modern Cryptography_下载链接1_

书评

如果Stinson的《密码学理论与实践》可以作为密码学的入门教材，Goldreich的《密码学基础》可以作为高级密码学理论研究的敲门砖，这本书就担当起了承上启下的作用，以严谨而不失易懂的文笔，清晰地将密码学中各个原语和他们依赖的安全基础假设完整的结合在一起，让每一个密码学...

很少有书能够把理论密码学的那些事儿系统的讲清楚，而且还能够给出详细的推导和说明。Bellare的那份讲义虽然非常好，但是厚度上还略差一些。

到目前为止，还不能把课后习题都做出来。而不论是网络，还是通过其他方式，都拿不到习题集。这对于自学巩固没太多好处。
到目前为止，还不能把课后习题都做出来。而不论是网络，还是通过其他方式，都拿不到习题集。这对于自学巩固没太多好处。

Introduction to Modern Cryptography_下载链接1_