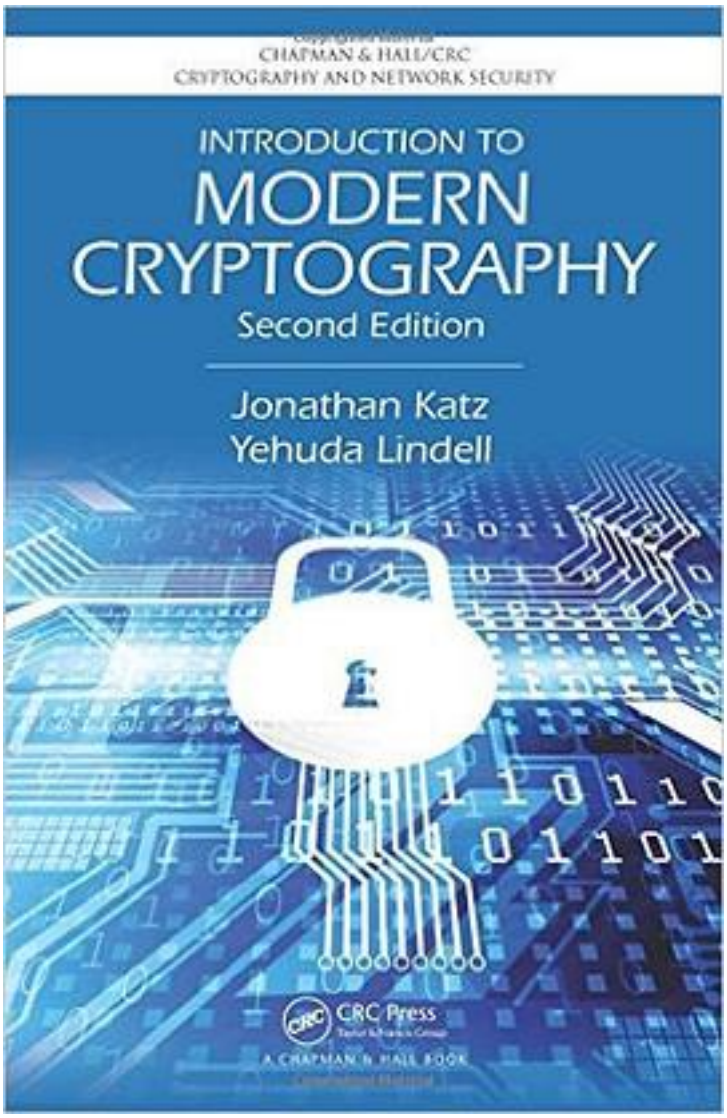
Introduction to Modern Cryptography, Second Edition



Introduction to Modern Cryptography, Second Edition_下载链接1_

著者:Jonathan Katz

出版者:Chapman and Hall/CRC

出版时间:2014-12-18

装帧:Hardcover

isbn:9781466570269

作者介绍:

About the Author

Jonathan Katz is a professor of computer science at the University of Maryland, and director of the Maryland Cybersecurity Center. He has published over 100 articles on cryptography, and serves as an editor of the Journal of Cryptology, the premier journal of the field. Prof. Katz has been invited to give introductory lectures on cryptography for audiences in academia, industry, and government, as well as an on-line cryptography course through Coursera.

Yehuda Lindell is a professor of computer science at Bar-Ilan University. He has published more than 90 articles on cryptography and four books, and has considerable industry experience in deploying cryptographic schemes. Professor Lindell lectures widely in both academic and industry venues on both theoretical and applied cryptography, and has been recognized with two prestigious grants from the European Research Council.

目录:

标签

密码学

计算机

专业参考书

课程

计算机科学

英文原版

评论

除了没有题解之外没啥缺点了

重大的改进：增加了Hash及其应用一章；重点改写了PKE，增加了KEM的内容等；数字签名一章的改写也很多；第一版第六章也重新了。

作为intro很不错，但错误很多。私钥那边看得比较仔细，例如书上说EAV security的IND定义和semantic定义是等价的，reference给的是Micali的paper。但其实书上那两个定义是否等价好像还是open的。那篇paper里semantic的定义要更强（根本问题是不知道P和BPP的关系）。类似的毛病还有sp resistance推owf的条件没给全（应该要求定义域和值域之间有一个super polynomial的gap，单compress是不够的）。这样的错误其实不少。公钥那边没有细抠，只因各种函数带key不带key，集合是所有串还是一个群，函数是映射还是PPT还是family都太乱了，抠起来太麻烦。总之虽然很疵，但是够用。稍微再难一点点可能会更好。

Introduction to Modern Cryptography, Second Edition_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, Second Edition_下载链接1_