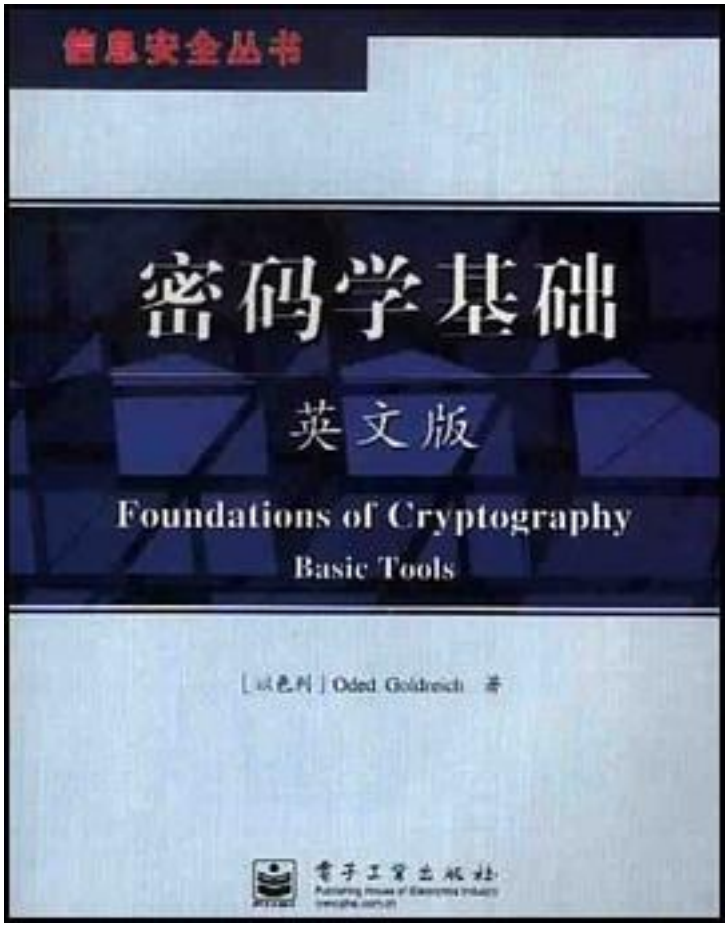
密码学基础



密码学基础_下载链接1_

著者:Goldreich

出版者:电子工业出版社

出版时间:2003-1

装帧:简装本

isbn:9787505381780

密码学涉及解决通信保密问题的计算系统的概念、定义及构造。密码系统的设计必须基于坚实的基础。本书对这一基本问题给出了系统而严格的论述：用已有工具来定义密码的目标并解决新的密码学问题。全书集中讨论了基本的数学工具：计算困难性、伪随机性以及零知识证明等。本书的重点是澄清基本概念及证明密码学问题解决方法的可行性

。而不侧重于对特殊方法的描述。

作者介绍:

目录:

密码学基础_下载链接1_

标签

密码学

密码

数学

计算机科学

经典

教材

科学

专业参考书

评论

这本书不打五分肯定不行，密码学经典的经典。Goldreich大牛啊。。。能看完至少能硕士毕业，读透了博士离毕业也不远了

密码学基础_下载链接1_

书评

Goldreich是交互证明系统的创始人之一，很好的写的，而且他偏重于概念性的讲述，把这些概念的关系讲的很清楚。 关于 入门 这两个字的意思
，我想解释一下，因为已经不能改题目了，所以有误导性，如果你没有密码学的基础的话，一定不能用这本书，我的入门的意思是如果你想研究密...

密码学基础_下载链接1_