《密码学导引》

图书基本信息

书名：《密码学导引》

13位ISBN编号：9787030072955

10位ISBN编号：7030072952

出版时间：2001-10-01

出版社：科学出版社

作者：冯登国,裴定一

《密码学导引》

内容概要

全书包括十一章和一个附录，系统地介绍了现代密码学的基本理论和技术，主要内容包括密码学的基本概念、倍息理论基础、复杂性理论基础，流密码，分组密码的设计原则、工作模式和一些有代表性的分组密码算法及攻击分组密码的一些典型方法，公钥密码算法，各种数字签名方案和各种签名的应用环境，Hash函数的分类、攻击方法和一些有代表性的Hash算法，时戳技术，大量的身份识别协议和基于身份的密码方案，一些赛钥管理技术，电

《密码学导引》

书籍目录

《密码学导引》

精彩短评

1、冯登国先生这本书。。哎。。怎么说呢。。一看就知道是从各处抄的。。符号表示太没有体系了，第一次看书这么吃力。。哎。。不过最终考试还挺好~
2、比较难
3、其实学数学，语言，哲学的时候，能够读几本计算机的书，是在是一种福气，因为里面的思维实现了可视化，其实可视并不仅仅是图像，还有可能是文字。。破解密码的本身的数学形式就是寻找从未知空间到已知空间的函数，所以一定是寻找算子，而算子可能是一本85年出版的圣经，可能是一本字典，可能是某天股市的记号，或者是天气预报，或者是一个物理公式

《密码学导引》

版权说明