<<密码学导引>>

图书基本信息

书名：<<密码学导引>>

13位ISBN编号：9787302160144

10位ISBN编号：7302160147

出版时间：2007-10

出版时间：清华大学

作者：何德全 编

页数：310

<<密码学导引>>

内容概要

《密码学导引：原理与应用》主要从两个方面介绍密码学的知识：第一部分介绍了经典密码学中的对称密码体制、非对称密码体制及相关的密码协议，重点讨论了模代数学和以模代数学为基础的非对称密码。
第二部分从Shannon经典的信息论工作出发，分析了概率算法和单向函数的安全性，并给出了基本的安全性定义。
在此基础上，对公钥加密和签名方案的可证明安全性做了详细的分析。
另外，在附录中，《密码学导引：原理与应用》还完整地介绍了密码学中需要用到的代数数论和概率信息论的基础知识。

《密码学导引：原理与应用》可作为信息安全领域的大学生与研究生的相关课程的教材，也可作为密码学和信息安全领域的研究人员的参考书。

<<密码学导引>>

书籍目录

版权说明