<<应用密码学手册>>

图书基本信息

书名：<<应用密码学手册>>

13位ISBN编号：9787121013393

10位ISBN编号：7121013398

出版时间：2005-6

出版时间：电子工业出版社

作者：Menezes

页数：711

字数：1164000

译者：胡磊

<<应用密码学手册>>

内容概要

本书是目前最优秀的密码学书籍之一。
全书包含15章，内容覆盖了近20年来密码学发展的所有主要成就。
除了通常密码学书籍都会讲到的对称密码、杂凑涵数、公钥密码和签名、身份识别和密钥建立协议等内容外，本书首先提供了密码学的概貌，中间有三章专门讲述了公钥密码学的数学基础，最后两章给出了密码实现技巧和专利、标准等细节。
这些内容对研究者和工程师们都是十分有用的。
全书提供了丰富的密码学技术细节，包括200多个算法和协议、200多幅图表、1000多个定义、事实、实例、注释和评论。
书末列举了1200多篇关于密码学的主要文献，并在各章中对其做了简要评述。
本书组织完美，表述清晰，适合密码学、计算机、通信、数学等领域折师生、专家和工程师们参考或作为教材使用。

作者简介

Alfred U．Menezes于1992年获得加拿大滑铁卢大学博士学位，现任滑铁卢大学教授，在椭圆曲线密码方面有很高的造诣。
Paul C．van Oorschot于1988年获得计算机科学博士学位，现任加拿大Carleton大学计算机科学学院教授，也是加拿大网络与软件安全研究主席，在密码学和网络安全方面具有深厚的学术功底。
Scott丸Vanstone于1974年获得博士学位，是加拿大滑铁卢大学教授，曾任杂志Designs，Codes and Cryptography的主编，滑铁卢大学数据加密研究组的主任。
他还是著名的Certicom信息安全公司的创始人。

<<应用密码学手册>>

书籍目录

<<应用密码学手册>>

编辑推荐

本书是目前最优秀的密码学书籍之一。
全书提供了丰富的密码学技术细节，十分适合研究人员和工程师们学习。
本书的三位作者均是国际著名的密码学家和活跃的密码学研究者。
Alfred J.Menezes于1992年获得加拿大滑铁卢大学博士学位，现任滑铁卢大学教授，在椭圆曲线密码方面有很高的造诣。
Paul C.van Oorschot于1988年获得计算机科学博士学位，现任加拿大Carleton大学计算机科学学院教授，也是加拿大网络与软件安全研究主席，在密码学和网络安全方面具有深厚的学术功底。
Scott A.Vanstone于1974年获得博士学位，是加拿大滑铁卢大学教授，曾任杂志Designs,Codes and Cryptography的主编，滑铁卢大学数据加密研究组的主任。
他还是著名的Certicom信息安全公司的创始人。

版权说明