<<信息安全数学基础>>

图书基本信息

书名：<<信息安全数学基础>>

13位ISBN编号：9787302084471

10位ISBN编号：7302084475

出版时间：2004-6

出版时间：清华大学出版社

作者：陈恭亮

页数：211

字数：340000

<<信息安全数学基础>>

内容概要

本书系统地介绍了信息安全所涉及的数论、代数和椭圆曲线论等数学理论，特别是对在信息安全工程实践中所涉及的数学知识做了较详细的讲述；此外，本书还介绍了在信息安全研究和应用中所产生的一些新的数学成果。

本书可作为信息安全专业、通信专业、信息专业、计算机专业的本科生和研究生的教科书，也可以供从事信息安全工作的科研人员参考。

<<信息安全数学基础>>

书籍目录

媒体关注与评论

书评本色特色： 详细介绍了信息安全，特别是公钥密码系统所涉及的数论、代数和椭圆曲线论等数学理论。

对欧几里得除法、模同余、欧拉定理、中国剩余定理、二次同余、原根、有限群、有限域、椭圆曲线做了较详细的讲述。

不仅能使读者从数学方面了解密码系统的安全性，而且可帮助读者运用所学知识去构建安全有效的密码系统。

<<信息安全数学基础>>

编辑推荐

本色特色：　　详细介绍了信息安全，特别是公钥密码系统所涉及的数论、代数和椭圆曲线论等数学理论。

对欧几里得除法、模同余、欧拉定理、中国剩余定理、二次同余、原根、有限群、有限域、椭圆曲线做了较详细的讲述。

不仅能使读者从数学方面了解密码系统的安全性，而且可帮助读者运用所学知识去构建安全有效的密码系统。

<<信息安全数学基础>>

版权说明