

图书基本信息

书名：<<移动通信系统认证协议与密码技术>>

13位ISBN编号：9787115143501

10位ISBN编号：7115143501

出版时间：2007-3

出版时间：人民邮电

作者：李方伟

页数：211

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## 内容概要

《现代移动通信技术丛书：移动通信系统认证协议与密码技术》以作者的科研成果为基础，系统地研究了移动通信系统认证协议与密码技术。

全书分为四大部分（共11章）：第一部分（第1~4章）介绍了移动通信认证协议和密码技术的理论基础，主要包括数论知识、对称和非对称密钥体制、身份认证与密钥协商机制等内容；第二部分（第5~6章）介绍了移动通信系统中的安全问题，主要包括安全威胁和安全技术，并针对GSM等系统进行了详细的分析；第三部分（第7~10章）研究第三代移动通信系统中的安全问题，主要包括安全体系结构、系统接入链路和网络域的安全技术以及2G与3G互操作与切换时的安全保证等内容；第四部分（第11章）研究公钥密码体制在移动通信系统中的应用。

本书能够为从事移动通信网络认证协议设计、密码算法研究的工程技术人员集中了解和研究这方面工作提供有益的帮助，也可以作为大专院校相关专业本科生和研究生了解移动通信网络安全方面知识的参考教材和参考资料。

书籍目录

第1章 数论基础1.1 加密系统中常用的数论知识1.2 复杂性理论简介第2章 对称密码体制2.1 对称密码体制的模型2.2 流密码2.3 分组密码2.4 数据加密标准 ( DES ) 2.5 Rijndael密码体制2.6 KASUMI分组密码第3章 非对称密码体制3.1 非对称密码体制的基本原理3.2 RSA密码体制3.3 ElGamal密码体制3.4 椭圆曲线密码体制第4章 身份证与密钥协商4.1 认证与认证系统4.2 杂凑函数4.3 数字签名4.4 身份认证4.5 密钥协商4.6 认证与密钥协商4.7 Kerberos认证系统第5章 移动通信网中的安全概述5.1 移动通信系统的概述5.2 移动通信网中的安全威胁5.3 移动通信中的安全业务5.4 移动通信系统中的安全技术第6章 移动通信系统中的安全实现6.1 GSM的安全实现6.2 GPRS的安全实现6.3 CDMA的安全实现第7章 第三代移动通信系统的安全特性7.1 第二代移动通信系统中存在的安全缺陷7.2 第三代移动通信系统的安全原则7.3 第三代移动通信的安全结构7.4 第三代移动通信的数据类型7.5 第三代移动通信的安全威胁7.6 第三代移动通信系统的安全要求7.7 第三代移动通信系统的安全特性第8章 第三代移动通信系统的网络访问安全实现8.1 移动用户的身份保密技术.....第9章 第三代移动通信系统的网络域安全实现第10章 UMTS与GSM间互操作与切换时的安全实现第11章 公钥密码体制在移动通信网络中的应用参考文献

编辑推荐

《现代移动通信技术丛书：移动通信系统认证协议与密码技术》以作者的科研成果为基础，系统地研究了移动通信系统认证协议与密码技术。

全书分为四大部分：第一部分介绍了移动通信认证协议和密码技术的理论基础；第二部分介绍了移动通信系统中的安全问题；第三部分研究第三代移动通信系统中的安全问题；第四部分研究公钥密码体制在移动通信系统中的应用。

本书能够为从事移动通信网络认证协议设计、密码算法研究的工程技术人员集中了解和研究这方面工作提供有益的帮助，也可以作为大专院校相关专业本科生和研究生了解移动通信网络安全方面知识的参考教材和参考资料。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>