<<电子商务安全技术>>

图书基本信息

书名：<<电子商务安全技术>>

13位ISBN编号：9787302303862

10位ISBN编号：730230386X

出版时间：2013-2

出版时间：熊平、朱平、陆安生、 张爱菊 清华大学出版社 (2013-02出版)

<<电子商务安全技术>>

内容概要

《21世纪高等学校电子商务专业规划教材:电子商务安全技术(第2版)》共包括10章。
第1章介绍电子商务安全的基本概念、电子商务安全系统的体系结构及相关技术的介绍；第2章对密码技术及常用算法进行了介绍；第3章是认证技术，介绍了身份认证和消息认证，并对常用的认证技术进行了阐述；第4章对称密码体制和非对称密码体制中的密钥管理技术，Diffie—Hellman密钥交换协议等进行了介绍；第5章介绍计算机网络安全技术，包括防火墙、虚拟专用网、计算机病毒和入侵检测技术等；第6章介绍了公钥基础设施；第7章介绍了电子支付基本概念、我国和国外的支付系统，电子支付方式和网络银行等；第8章介绍安全套接层协议，包括认证算法、协议实现和协议安全性分析等；第9章介绍电子商务安全协议——SET协议，并和SSL协议进行了对比分析；第10章是移动电子商务安全，在这章介绍了我国的无线网络、常用的无线网络协议，移动电子商务存在的安全隐患以及目前移动电子商务中常用的安全解决方法。

<<电子商务安全技术>>

书籍目录

章节摘录

版权页： 插图： 如果一个密码系统的加密密钥和解密密钥相同，或者虽然不相同，但由其中的任意一个密钥可以很容易地推导出另外一个，则所采用的就是对称密钥密码体制。
如A5、SEAL、DES、IDEA、RC5、AES等都是对称密码体制的加密算法。
反之，如果一个密码系统的加密和解密分别用两个不同的密钥实现，并且由加密密钥推导出解密密钥在计算上是困难的，则该系统所采用的就是非对称密码体制。
采用非对称密码体制的每个用户都有一对选定的密钥，其中一个是可以公开的，称为公钥，一个由用户自己秘密保存，称为私钥。
RSA、E1Gamal、椭圆曲线密码等都是非对称密码体制的典型代表。
对称密码体制用复杂的非线性交换来实现；非对称密钥密码体制一般使用某个数学上的难题来实现。一般来说，后者的安全程度与现实的计算能力具有密切的关系，非对称密码体制适应于开放性的使用环境，密钥管理问题相对简单，可以方便、安全地实现数字签名和验证。
（3）根据密码算法对明文信息的加密方式，可分为流密码和分组密码。
流密码逐位地加密明文消息字符（如二进制数），本书中介绍的A5、SEAL即为流密码算法；分组密码将明文消息分组（每个分组含有多个字符），逐组地进行加密，本书所介绍的DES、IDES、RC5、AES等即为分组密码算法。
（4）按照加密变换是否可逆，又可将密码算法分为单向函数密码以及人们通常所指的双向变换密码。
单向函数是一类特殊的密码体制，其性质是可以容易地把明文转换成密文，但再把密文转换成原来的明文却是困难的（有时甚至是不可能的）。
单向函数只适用于某种特殊的、不需要解密的场合（如密钥管理和信息完整性鉴别技术）。
典型的单向函数包括MD4、MD5、SHA—1等。
另外，关于密码体制的分类，还有一些其他的方法，例如按照在加密过程中是否注入了客观随机因素可以分为确定型密码体制和概率密码体制等。
我们最经常使用的分类方法是第二种。
2.3密码分析 密码分析主要研究如何分析和破译密码。
对于一个密码体制，如果能够根据密文确定明文或密钥，或者能够根据明文和相应的密文确定密钥，则我们说这个密码体制是可破译的；否则，称其为不可破译的。
密钥空间中不同密钥的个数称为密码体制的密钥量，它是衡量密码体制安全性的一个重要指标。
一个密码系统的实际安全性牵涉到两方面的因素。
1.所使用的密码算法的保密强度 密码算法的保密强度取决于密码设计的水平、破译技术的水平以及攻击者对于加密系统知识了解的程度。
密码系统所使用的密码算法的保密强度提供了该系统安全性的技术保证。

<<电子商务安全技术>>

编辑推荐

《21世纪高等学校电子商务专业规划教材:电子商务安全技术(第2版)》可作为电子商务、信息管理、计算机、国际贸易类专业本科生和研究生的教材，也可作为相关领域高级管理人员的培训教材或参考用书。

版权说明