# 《电子商务的安全技术》

## 图书基本信息

书名：《电子商务的安全技术》

13位ISBN编号：9787508432007

10位ISBN编号：7508432002

出版时间：2005-9

出版社：中国水利水电出版社

作者：劳帼龄

页数：292

# 《电子商务的安全技术》

## 前言

电子商务从20世纪90年代中期诞生以来，已经走过了十年的发展历程。十年来，安全问题始终是影响其发展的一个瓶颈。这在中国互联网络信息中心所作的历次调查和发布的《中国互联网络调查统计报告》中可见一斑，历次调查，安全问题一直是电子商务用户特别关注的主题。可以这么说，电子商务安全是电子商务顺利发展的一个关键，也是一个难点。电子商务作为一种全新的业务和服务方式，为全球客户提供了丰富的商务信息、简捷的交易过程和低廉的交易成本。但是电子商务在给人们带来方便的同时，也把人们引进了安全陷阱。电子商务是利用计算机通过网络来实现的。

# 《电子商务的安全技术》

## 内容概要

电子商务的安全技术，ISBN：9787508432007，作者：劳帼龄主编

# 《电子商务的安全技术》

## 书籍目录

# 《电子商务的安全技术》

## 章节摘录

2.2 分组加密与高级加密标准密码体制从原理上可分为两大类，即单钥体制（One—key System）和公钥体制（TWO.key System）。单钥体制的加密密钥和解密密钥相同，也称对称加密体制。本节所介绍分组密码是一种重要的对称加密体制，它是将明文按一定的位长分组，输出也是固定长度的密文。它的优点十分突出，应用非常广泛。本节在详细介绍了密码体制以及对称加密模式后，将介绍分组密码加密算法中最具典型意义的数据加密标准DES和高级加密标准AES。2.2.1 密码体制的分类密码是实现秘密通信的主要手段，是隐蔽语言、文字、图像的特殊符号。凡是用特殊符号按照通信双方约定的方法把电文的原型隐蔽起来，不为第三者所识别的通信方式称为密码通信。在计算机通信中，采用密码技术将信息隐蔽起来，再将隐蔽后的信息传输出去，使信息在传输过程中即使被窃取或截获，窃取者也不能了解信息的内容，从而保证信息传输的安全。密码体制是指密钥空间与相应的加密运算结构，同时还包括了明文和密文的结构特征。密码体制一般可分为传统密码和现代密码，传统密码包括换位密码、代替密码、转轮机密码等，现代密码又包括序列密码、分组密码、公钥密码、量子密码体制等，现代密码已经广泛应用于军事、商业经济、网络间的通信、电子商务、电子政务等领域。从不同的角度根据不同的标准，可以把密码分成若干类。1.按密钥方式划分（1）对称式密码。收发双方使用相同密钥的密码，叫做对称式密码。传统的密码都属此类，现代密码中的分组码和序列密码也属于这一类。（2）非对称式密码。收发双方使用不同密钥的密码，叫做非对称式密码。如现代密码中的公开密钥密码就属此类。2.按应用技术或历史发展阶段划分（1）手工密码。以手工完成加密作业，或者以简单器具辅助操作的密码，叫做手工密码。第一次世界大战前的密码主要是这种作业形式。（2）机械密码。以机械密码机或电动密码机来完成加解密作业的密码，叫做机械密码。这种密码从第一次世界大战出现到第二次世界大战中得到普遍应用。（3）电子机内乱密码。通过电子电路，以严格的程序进行逻辑运算，以少量制乱元素生产大量的加密乱数，因为其制乱是在加解密过程中完成的而不需预先制作，所以称为电子机内乱密码。从20世纪50年代末期出现到70年代广泛应用。（4）计算机密码。是以计算机编程进行算法加密为特点，适用于计算机数据保护和网络通信等广泛用途的密码。从20世纪70年代出现到现在广泛应用。

# 《电子商务的安全技术》

## 编辑推荐

《注册电子商务工程师(CEBE)认证培训教材·电子商务的安全技术》可作为注册电子商务工程师(CEBE)认证考试的教材，也可以作为电子商务专业的概论性课程教材，或作为计算机专业、信息管理与信息系统专业有关电子商务课程的教材，还可供一般工程技术人员、工商管理人员和社会大众，系统了解和学习电子商务的有关知识。

# 《电子商务的安全技术》

## 版权说明