<<信息存储安全理论与应用>>

图书基本信息

书名：<<信息存储安全理论与应用>>

13位ISBN编号：9787118081220

10位ISBN编号：7118081221

出版时间：2012-9

出版时间：国防工业出版社

作者：张青凤

页数：228

字数：263000

<<信息存储安全理论与应用>>

内容概要

《信息存储安全理论与应用》以信息存储安全的角度为着眼点，围绕信息存储安全涉及到的加密技术、身份认证技术、访问控制技术、pki技术、智能卡技术、数字签名技术、身份认证技术、信息隐藏技术、密钥管理技术、云存储技术来展开论述，为了更好地理解和应用这些相关技术，在介绍其相关基本理论的基础上，重点介绍了加密技术、身份认证技术、访问控制技术等核心技术的应用，并配备了来源于实际项目开发中的应用实例对其深入的进行讲解。

《信息存储安全理论与应用》共分为两部分：第一部分为基础篇，共7章，主要介绍信息存储所涉及到的主要技术，第二部分为应用篇，共6章，侧重介绍源于项目开发中基于信息存储技术的应用实例。

《信息存储安全理论与应用》的一大亮点是对当前信息安全中最前沿的云计算和云存储相关问题做了比较系统的介绍和探讨。

《信息存储安全理论与应用》适合于信息安全相关专业学生、从事网络安全产品开发的技术人员、企事业单位网络工作人员以及信息安全领域的爱好者阅读。

<<信息存储安全理论与应用>>

书籍目录

章节摘录

版权页： 插图： 2.5 密码学新方向 密码学把信息安全核心算法作为研究目标，其研究内容也是不断发展变化的。
现代的加密技术就是适应了网络安全的需要而产生的，它为电子商务活动提供了安全保障，目前一些很实用的密码新技术逐渐为人们所用。
1.密码专用芯片集成 密码技术是信息安全的核心技术，目前已经渗透到大部分安全产品之中，正向芯片化方向发展。
在芯片设计制造方面，目前微电子水平已经发展到0.1微米工艺以下，芯片设计的水平很高。
我国在密码专用芯片领域的研究起步落后于国外，近年来我国集成电路产业技术的创新和自我开发能力得到了提高，微电子工业得到了发展，从而推动了密码专用芯片的发展。
加快密码专用芯片的研制将会推动我国信息安全系统的完善。
2.量子加密技术方面 量子技术在密码学上的应用分为两类：一是利用量子计算机对传统密码体制的分析；二是利用单光子的测不准原理在光纤一级实现密钥管理和信息加密，即量子密码学。
量子计算机是一种传统意义上的超大规模并行计算系统，利用量子计算机可以在几秒钟内分解RSA的公钥。
随着网络的发展，全光网络将是今后网络连接的发展方向，利用量子技术可以实现传统的密码体制，在光纤一级完成密钥交换和信息加密。
如果攻击者企图接收并检测发送方的信息，则将造成量子状态的改变，这种改变对攻击者而言是不可恢复的，而对收发方则可很容易地检测出信息是否受到攻击。
目前量子加密技术仍然处于研究阶段，其量子密钥分配QKD在光纤上的有效距离还达不到远距离光纤通信的要求。
3.信息隐藏技术方面 数字水印技术与信息安全、信息隐藏、数据加密等均有密切的关系，是多媒体信息安全研究领域的一个热点。
该技术通过在原始数据中嵌入秘密信息（水印）来证实该数据的所有权，被嵌入的水印可以是一段文字、标识、序列号等，它与原始数据紧密结合并隐藏其中，即使经历破坏源数据使用价值的操作也能保存下来。
4.智能卡技术及生物测量方面 智能卡及生物测量学在密码学方面的应用也十分广泛。
生物测量学是指借助个人身体特征来对个人进行认证的广泛技术，包括指纹鉴定、虹膜和视网膜扫描、声音或面部识别、手形测量等。
生物测量学系统的优势在于其识别标志是独一无二的且总是存在的。
这些系统同智能卡系统一起正在得到日益广泛的使用，经常可以用其替代基于密码的认证，或同传统密码系统一起使用。
5.可证明安全性 可证明安全性是指一个密码算法的安全性可以通过归约的方法去证明。
所谓的归约是把一个公认的难解问题转化为密码算法的破译问题，即证明安全性是假定攻击者能够成功，则可以在逻辑上推出这些攻击信息可以使得攻击者或者系统的使用者能够解决一个公认的数学难题。
这种思想使密码算法的安全性论证比以往的方法更加科学、更加可信，因此成为密码学研究的一个热点问题。
6.基于身份的密码技术 利用用户的部分身份信息可以直接推导出其公开密钥的思想，早在1984年Shamir就提出来了。
对于普通公钥密码来说，证书权威机构是在用户生成自己的公私密钥对之后，对用户身份和公钥进行捆绑，并公开这种捆绑关系。
对于基于身份的公钥密码来说，与证书权威机构对应的可信第三方，在用户的密钥对生成过程已经参与，公开密钥可以选择以用户的部分身份信息形成的函数值。
此时用户与其公钥的捆绑关系不是通过数字签名，而是通过可信第三方对密码参数的可信、统一（而不是单独对每个用户的公钥）公开得到保障。

可以看出来，在多级交叉通信的情况下，对于身份的密码的使用比普通公钥密码的使用减少了一个签名及验证层次，从而受到业界的关注。

编辑推荐

《信息存储安全理论与应用》的一大亮点是对当前信息安全中最前沿的云计算和云存储相关问题做了比较系统的介绍和探讨。
《信息存储安全理论与应用》适合于信息安全相关专业学生、从事网络安全产品开发的技术人员、企事业单位网络工作人员以及信息安全领域的爱好者阅读。

<<信息存储安全理论与应用>>

版权说明