<<密码理论与技术>>

图书基本信息

书名：<<密码理论与技术>>

13位ISBN编号：9787564901172

10位ISBN编号：7564901179

出版时间：2010-4

出版时间：河南大学出版社

作者：王天芹

页数：144

<<密码理论与技术>>

内容概要

《密码理论与技术》是在编者为硕士研究生讲授密码学选修课讲义的基础上编写而成的.主要内容包括密码学的基本概念及在信息安全中的地位和作用；私钥密码体制及一些有代表性的密码算法；公钥密码体制及与公钥有关的若干算法；Hash函数与数字签名；密钥管理和秘密共享；身份认证协议；零知识证明技术；密码协议和算法在网络安全中的应用.《密码理论与技术》适用于高等院校计算机或通信专业的本科生或研究生，也可供信息安全领域的科技人员参考。

<<密码理论与技术>>

书籍目录

章节摘录

公钥的分配方法有以下几种： 公开发布：用户将自己的公钥发送到公开的区域.（这种方法的最大缺陷是公钥信息容易被伪造）。

公钥动态目录表：由某个公钥管理机构建立和维护一个公用的公钥动态目录表，每个用户都可靠地知道管理机构的公钥.公钥分配模式如图5.2.3所示. （1）A向公钥管理机构发送一个带时间戳的请求，请求得到B的公钥； （2）管理机构为A的请求发出应答，应答中包含A的原始请求信息和B的公钥； （3）A用B的公钥加密A的身份和一个一次性随机数N1后发给B； （5）B用与A同样的方法从公钥管理机构得到A的公钥； （6）B用A的公钥加密N1和另一个一次性随机数N2后发给A； （7）A用B的公钥加密N：后发给B. 由于每一个用户都需要与管理机构通信才能获得其他用户的公钥，因而公钥管理机构可能成为系统的瓶颈，并且公钥目录表也容易成为攻击对象. 公钥证书：由证书管理机构CA为用户建立和维护公钥证书，其中包含有用户的公钥、用户的身份、时间戳等信息，并由CA用自己的私钥签名.这是分配公钥的一种常用的安全有效的方法，后面将详细讨论。

5.3密钥协商 密钥协商是一个协议，通过通信双方或多方在公开信道上相互交换信息进而共同建立一个秘密密钥.在密钥协商方案中，秘密密钥是通信双方所提供的信息的函数值.下面介绍两个具体的协议。

版权说明