

<<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

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>

## <<密码理论与技术>>

### 内容概要

《密码理论与技术》是在编者对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。

## &lt;&lt;密码理论与技术&gt;&gt;

## 书籍目录

第1章 概论1.1 密码学的产生与发展1.2 密码学的基本概念1.3 密码学的理论基础小结第2章 私钥密码体制2.1 分组密码设计原则2.2 高级加密标准AES2.3 AES的工作模式2.4 国际数据加密算法IDEA小结第3章 公钥密码体制3.1 RSA密码体制3.2 ElGamal密码体制3.3 椭圆曲线密码体制小结第4章 数字签名4.1 数字签名基础4.2 安全Hash函数4.3 基于因子分解问题的数字签名4.4 基于离散对数问题的数字签名4.5 代理签名4.6 群签名4.7 代理群签名4.8 盲签名4.9 签密小结第5章 密钥管理5.1 概述5.2 密钥分配5.3 密钥协商5.4 密钥保护5.5 公钥基础设施 (PKI) 小结第6章 身份认证6.1 口令认证6.2 挑战-应答身份认证6.3 零知识身份认证6.4 Kerberos (K) 认证6.5 X.509认证小结第7章 秘密共享技术7.1 门限方案7.2 访问结构7.3 单调电路构造法7.4 完善秘密共享方案7.5 信息率7.6 Brickell向量空间构造法7.7 分解构造法小结第8章 伪随机数生成8.1 引言8.2 PRBG的安全性8.3 Blum-Blum-Shub生成器8.4 概率加密小结第9章 零知识证明9.1 交互证明系统9.2 完善零知识证明9.3 比特托管9.4 计算零知识证明小结第10章 安全协议10.1 IPSec10.2 传输层安全协议SSL小结第11章 应用安全11.1 Email安全11.2 电子商务安全小结参考文献

## 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N2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。

<<密码理论与技术>>

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>