第一图书网, tushu007.com

<<计算机安全与保密>>

图书基本信息

书名：<<计算机安全与保密>>

13位ISBN编号：9787302293873

10位ISBN编号：7302293872

出版时间：2013-2

出版时间：李辉 清华大学出版社 (2013-02出版)

作者：李辉

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

第一图书网, tushu007.com

<<计算机安全与保密>>

内容概要

《21世纪高等学校信息安全专业规划教材:计算机安全与保密》共分为10章。
第1章介绍一些常见的古典密码系统算法；第2章介绍包括DES、AES在内的对称密码系统和国内教材很少提及的加密与解密模式；第3～5章介绍公钥密码系统，其中，第3章的公钥密码系统基于大数因式分解问题，第4章的公钥密码系统基于离散对数问题，第5章的一些公钥密码系统则基于其他的完全NP问题；第6章介绍数字签名的原理；第7章介绍Hash函数以及基于Hash函数和对称密码算法的消息验证码技术；第8章介绍密钥管理和PKI技术；第9章以专题的形式介绍目前计算机安全应用领域的一些主流技术，包括口令安全、VPN等；第10章基于Java平台介绍密码学及安全的编程框架和技术。
以上各章中，第1～7章偏重理论与原理；第8章和第9章偏重于应用；第10章偏重于编程。

第一图书网, tushu007.com

<<计算机安全与保密>>

书籍目录

第一图书网, tushu007.com

章节摘录

版权页： 插图： （4）防陷害攻击：包括群管理员在内的任何人都不能以其他群成员的名义产生有效的群签名。
（5）不关联性：在不打开签名的情况下，确定两个不同的签名是否为同一个群成员所签在计算上是不可行的。
（6）抗联合攻击：即使一些群成员串通起来，也不能产生一个有效的不被跟踪的群签名。
一个群签名方案往往包括以下5个关键算法。
（1）创建（Setup）算法：通常是通过概率算法产生群公钥和群管理员的私钥。
（2）加入（Join）算法：一个用户和群管理员之间使用户成为群成员的协议。
执行该协议可产生群成员的私钥和成员证书。
（3）签名（Sign）算法：输入是要签名的消息和一个群成员的私钥，输出是该消息的签名。
（4）验证（Verify）算法：输入是消息的签名和群公钥后，输出的结果是签名是否有效。
（5）打开（Open）算法：给定一个签名和群管理员的私钥，确定签名人的具体身份。
最经典的群签名方案莫过于CS97方案。
1997年Camenisch发表了论文Efficientand generalized group signature，文中首次提出了知识签名的概念，并依据这种新思路给出了一个实用的群签名方案。
由于引入了知识签名的方法，研究者们发现群签名验证的目的被明确，签名者必须在验证中应用知识签名清晰地证明自己拥有的有效身份，才能防止任何非授权者伪造签名。
由于篇幅限制，本书没有系统地介绍知识签名的相关原理，CS97方案在此也一并略过，感兴趣的读者可查阅相关文献。
2.盲签名 早在1982年Chaum就提出了旨签名的概念。
Chaum给出一个例子：当文件装在信封中时，任何人都不能读它，签这个文件就是在信封里放一张复写纸，当签名者签这个信封时，他的签名便透过复写纸签到了文件上。
可以把盲签名的需求更明确地表达如下：（1）消息的内容对签名者是盲的；（2）即使签名者保存签过的文件，也不能确定出所签文件的真实内容。
针对以上需求，通常盲签名的实施包括以下几个步骤：（1）在将原始信息发送给签名者前，首先要对原始信息进行盲化；（2）签名者对盲化后的信息进行签名并返还给接收者；（3）接收者得到签名后，先进行去盲化，然后得到签名者关于原始信息的正确签名。
盲数字签名的基本原理是实用两个公钥密码算法，第一个公钥密码算法用于隐蔽信息，可称为盲变换。
第二个公钥密码算法用于签名。
下面以RSA盲签名为例进行说明。

第一图书网, tushu007.com

编辑推荐

《21世纪高等学校信息安全专业规划教材:计算机安全与保密》覆盖较多的知识点，可以作为高等院校计算机系教材，同时，书中提供大量的数据实例，也可以作为教师、科研人员以及兴趣爱好者的参考书。
《21世纪高等学校信息安全专业规划教材:计算机安全与保密》内容编排要合理。
既能使同学们在计算机安全方面提高素养和能力，又能使没有太多基础的同学保持浓厚兴趣并积极参与实践。
重视方法和思路胜过具体知识和手段。
陆续有一些方案被破解或认为不那么安全，但解决安全问题的思路不会有大的变化。
理论与实践并重。

第一图书网, tushu007.com

<<计算机安全与保密>>

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