<<数字内容安全原理与应用>>

图书基本信息

书名：<<数字内容安全原理与应用>>

13位ISBN编号：9787302284291

10位ISBN编号：7302284296

出版时间：2012-7

出版时间：清华大学出版社

作者：彭飞　等编著

页数：280

字数：435000

<<数字内容安全原理与应用>>

内容概要

《数字内容安全原理与应用》全面介绍了数字内容安全技术的起源、研究发展和应用。
全书共分为10章，内容包括绪论、信息加密技术、消息认证与数字签名、信息隐藏与数字水印、数字取证技术、文本内容安全、数字图像内容安全、数字音频内容安全、数字视频内容安全和数据库安全。

《数字内容安全原理与应用》适合作为信息安全专业本科高年级学生以及研究生的专业课教材，也可供从事信息安全专业技术人员阅读参考。

本书由彭飞负责编写。

<<数字内容安全原理与应用>>

书籍目录

章节摘录

版权页： 插图： 1.强力攻击法 强力攻击可用于任何分组密码，目攻击的复杂度仅依赖于分组长度和密钥长度。
严格地讲，攻击所需的时间复杂度依赖于分组密码的工作效率，其工作效率包括加解密速度、密钥扩展速度、存储空间等。
2.差分密码分析 差分密码分析是迄今为止已知最有效的攻击迭代密码的方法之一，它利用高概率特征或差分恢复密钥。
其基本思想为：通过分析明文对的差值对密文对的差值的影响来恢复某些密钥比特。
简单地，随机选取具有固定差分的一对明文，只要它们符合特定的差分条件，甚至可以不必知道它们的值。
然后，按照不同的概率，将输出密文中的差分分配给不同的密钥。
随着对密文对的分析越来越多，将使最可能的一个密钥显现出来，这样就得到了正确的密钥。
差分密码分析最初是针对DES加密提出的一种攻击方法，可用于6轮以上的DES加密。
8轮DES需要214个选择明文，10轮和14轮DES分别需要224和239个选择明文才能破解。
虽然差分密码分析未能破解16轮的DES加密，但用它破解轮数较低的DES还是很成功的。
例如，在个人计算机上几分钟就可以破解8轮DES。
差分密码分析除了用来攻击DES外，也可以被用来攻击其他的密码体制。
3.线性密码分析 线性密码分析本质上是一种已知明文攻击法，是对DES加密方法进行破译的主要方法。
这种方法用221个已知明克可以破译8轮DES，用247个明文可以破译16轮DES。
在某些情况下，这种方法可用于唯密文攻击。
其基本思想是：通过寻找一个给定密码算法的有效的线性近似表达式来破译密码系统。
由于每个密码系统均为非线性系统，因此只能寻找线性近似表达式。
如果分别将明文的一些位、密文的一些位进行异或运算，然后再将这两个结果进行异或运算，这两个结果的运算结果是一个位，这一位与密钥的一些位进行异或运算的结果相同。
这一位就是概率为P的线性近似值，在P不等于1/2前提下，就可以使用该偏差，用得到的明文及相对应的密文便可猜测密钥的位值。
得到的明文数据越多，猜测密钥的位置越可靠。
概率P越大，用同样数据量分析的成功率就越高。

<<数字内容安全原理与应用>>

编辑推荐

《高等院校信息技术规划教材:数字内容安全原理与应用》具有理论与应用相结合，详细介绍了当前数字内容安全的基本理论与应用技术；内容全面，包含了主流数字载体类型（文本，图像音频视频，数据库等）的安全技术；实例丰富，阐述理论知识的同时结合实例进行介绍清晰易懂；技术新颖，涵盖了当前数字内容安全领域的最新研究成果的特点，适合作为信息安全专业本科高年级学生以及研究生的专业课教材，也可供从事信息安全专业技术人员阅读参考。

<<数字内容安全原理与应用>>

版权说明