<<计算机网络安全的理论与实践>>

图书基本信息

书名：<<计算机网络安全的理论与实践>>

13位ISBN编号：9787040317985

10位ISBN编号：7040317982

出版时间：2011-6

出版时间：高等教育出版社

作者：王杰

页数：367

内容概要

本书第2版是在第1版和英文版的基础上修订和补充而成的。
在保持第1版结构的指导思想下，增加了若干新内容，包括彩虹表及其在字典攻击中的应用、rc4序列密码安全性讨论、中国余数定理及其在证明rsa算法正确性的应用、漩涡散列函数、无线网状网安全问题以及第二代万维网技术的一些安全问题等。
第2版还充实了第1版中部分章节的内容，如电子邮件安全协议、无线局域网安全协议以及无线个人网安全协议等。

第2版附有大量精心设计的习题，帮助读者掌握书中的内容，训练实际动手能力。
有些习题还引申了书中的内容，可作为课程设计及研究课题。
为了满足读者自学和教师教学的需求，第2版还给出了部分练习的详细解答，包括流程框图、加密算法及程序的源代码等。

作者简介

作者：（美国）王杰

<<计算机网络安全的理论与实践>>

书籍目录

章节摘录

版权页：插图：为便于实际应用，加密算法应公之于众，不公开的加密算法在极少数情况下曾被使用过，比如，在第二次世界大战中的太平洋战场，美国海军陆战队就曾使用过一个极偏僻的印第安人部落纳瓦霍人的语言作为密码算法，这个密码系统从使用开始到二战结束从未被日军识破，然而，加密算法不公开便无法设立工业化标准，也不利于研讨算法的安全性，所以，在现代通信应用中加密算法本身是不保密的，保密的只是加密算法所用的密钥，要求一把密钥能使用多次而不会威胁到加密算法的安全，除此之外，好的加密算法还应满足下列要求，1，运算简便快捷算法所执行的运算必须在计算机硬件和软件上容易实现，而且只需使用很少的计算资源就能完成，通常要求加密算法的时间复杂性和空间复杂性均为输入长度的小系数线性函数，这样做的目的是保证加密算法的执行不会影响系统的正常运行。
比如，为使加密和解密运算简便快捷，通常使用排斥加、置换、替换、循环位移和有限域的加法和乘法等简单运算，置换和替换运算都将某个二元字符串替换成另一个二元字符串，置换运算是一对一的，即不同的二元字符串不能被相同的二元字符串所取代，而替换运算则可以是多对一，2，抵御统计分析加密算法必须彻底打乱明文的统计结构，使任何统计分析的方法都难以破译密文，为保证这一点，要求加密算法必须同时具有扩散性和混淆性。
扩散性是指明文中的每一位二元数字都对密文中的多个二元数字有直接影响，也就是说，密文中的每一位二元数字都由明文中多个二元数字共同决定。
混淆性是指密钥中的每一位二元数字对密文中的多个二元数字有直接影响，也就是说，密文中的每一位二元数字都由密钥中多个二元数字共同决定。
扩散性和混淆性有时也统称为雪崩效应，它指的是在明文或密钥中哪怕只修改一位数字也会引起密文中多位数字的改变，就像轻微震动便能引起雪山崩塌一样。
产生扩散性最常用的方法是对明文段执行某些特定的运算，如替换运算，并对新产生的二元字符串如法重复数次，产生混淆性最常用的方法是从密钥生成若干子密钥，将明文段用一个子密钥执行某些特定的运算，如排斥加运算，并对新产生的二元字符串如法重复数次，将这两种方法按一定的方式结合起来使用便可望获得同时满足扩散性和混淆性的加密算法。

编辑推荐

《计算机网络安全的理论与实践(第2版)》是信息安全系列丛书之一。

<<计算机网络安全的理论与实践>>

版权说明