<<应用密码学基础>>

图书基本信息

书名：<<应用密码学基础>>

13位ISBN编号：9787307073210

10位ISBN编号：7307073218

出版时间：2009-11

出版时间：武汉大学出版社

作者：李益发，赵亚群，张习勇，张铎 编著

页数：312

<<应用密码学基础>>

内容概要

本书简要介绍了密码学基础理论和基本技术，内容分为三个部分：基础的密码算法、基本的应用技术和必要的数学基础知识。
密码算法部分包括：对称分组密码算法、非对称密码算法、散列算法和数字签名算法；基本应用技术包括：密钥管理的基本技术、基本认证技术和在防伪识别中的简单应用技术；数学基础知识部分包括：初等数论、代数学基础、有限域和椭圆曲线基础、计算复杂性理论基础。
　本书不同于其他密码学教材之处有二：一是包含了较多的密钥管理和认证技术，二是包含了密码学在自动识别中的保密和防伪应用。
本书可供自动识别技术专业的专科生、本科生作为密码学的教材使用，也可供计算机专业的专科生和本科生作为了解密码学的参考资料。

<<应用密码学基础>>

书籍目录

章节摘录

一个密钥只加密一个明文（称为一次一密），且所有密钥都是等概率的。
这里，p、c、K分别表示明文空间、密文空间和密钥空间。
当然，完善保密只是理论上的安全性，实际上很难实现。
而即使是理论上安全的密码系统，实际上也可能很脆弱，因为实际应用中还要求密钥能够安全传递。
比如“一次一密”系统，就要求在收发双方间传递大量密钥，增加了密钥管理的难度，甚至会使密钥管理系统变得十分脆弱，从而使整个密码系统不安全。
因此，密码系统不能单纯地追求理论上的安全。
由于实际的密码分析者所拥有的资源（资金、设备、时间等）总是有限的，因此人们更关心的是，如何构造一个超过敌手实际攻击能力的密码系统。
如果一个密码系统虽然不是完善保密的，但攻击该系统所要付出的努力远远超过攻击者实际拥有的能力，则称该密码系统是实际安全的。
可是，如何评估攻击者的能力呢？
由于破译密码本质上是计算，因此，目前普遍的做法是用计算能力来衡量。
而计算能力取决于两个主要方面：一个是拥有的计算资源，一个是算法的有效性。
对密码系统来说，如果在充分估计攻击者的计算能力的前提下，破译它所需要的计算量仍远远超出了攻击者所能付出的计算量，就认为它是实际安全的。
实际安全性也称为计算安全性。
1.1.3 密码学的概念　　早期的密码学分为密码编码学和密码分析学两大分支。
密码编码学研究如何保护消息的机密性，主要内容是各种加、解密算法；而密码分析学则研究在不知道密钥的前提下如何破译密文，主要内容是各种分析方法。
不过古代的密码还不能称为密码学，只能称为密码术。
密码真正成为一个学科，还是近代的事。

<<应用密码学基础>>

版权说明