<<现代密码学>>

图书基本信息

书名：<<现代密码学>>

13位ISBN编号：9787030236357

10位ISBN编号：7030236351

出版时间：2009-2

出版时间：科学出版社

作者：李顺东，王道顺 著

页数：273

前言

战争年代保密通信对于战争的胜负起着十分关键的作用。
第二次世界大战中，美军正是凭借破译日本的高级密码“紫密”，击毙了日本海军大将山本五十六，扭转了美军在太平洋战场上的被动局面。
同样在欧洲战场上也因为盟军破译了法西斯德国的恩尼格马密码而掌握了欧洲战场的主导权。
有军事科学研究者和历史学家说：没有恩尼格马密码的破译，欧洲战场上的第二次世界大战至少还要再持续2年，还要再付出2000万人生命的代价。
第二次世界大战中两个密码的破译已成为众所皆知的密码攻防战中的范例。
保密通信不仅在军事等领域发挥着独特作用，而且对当今的社会发展也日渐重要。
网络信息安全问题是随着网络的发展而产生和发展的。
最初设计互联网的目的是为使用者提供一种弹性、快速的通信方式。
初期互联网的使用者都是一些知识层次较高，具有一定身份的人群。
因为网络信息有限，网络用户比较单一，使用目的也比较单纯，所以最初的网络并不存在明显的安全问题。
20世纪90年代，由于商业的进入与应用的推动，互联网获得了迅猛的发展，现在网络已经无处不在、无时不在、无孔不入，人类产生了严重的互联网依赖，信息处理依靠计算机，信息通信依靠互联网，各行各业都严重依赖互联网。
网络中的内容越来越丰富，网络中信息的价值也越来越大。
网络用户变得异常复杂，不法之徒可能出于经济的目的、政治的目的、个人的目的等利用网络中的各种漏洞对网络实施攻击，达到自己不可告人的目的，并且造成网络瘫痪、丧失机密、丢失数据、服务质量下降等网络安全事故，造成国家、机构、组织、个人等严重的经济、政治、社会及组织形象等方面的损失。
敌对国家可能通过瘫痪一个国家的通信指挥系统、经济系统，攻破保密通信系统而达到战胜、控制一个国家的目的。
因此网络安全不仅仅是一个技术问题，更是一个经济、政治问题。
是否能保证网络信息安全足以影响一个国家的国家安全、经济发展、社会稳定。
因此信息保障能力已经成为国家综合国力的重要组成部分，成为未来国际竞争、企业竞争的杀手锏，是国家的头等大事。
没有信息安全就没有真正意义上的政治安全，就没有稳固的经济安全和军事安全，就没有完整意义上的国家安全。
包括网络安全在内的信息安全问题，成为世界各国所面临的共同难题。

<<现代密码学>>

内容概要

本书是一本现代密码学的入门书，书中系统地讲解了现代密码学研究所需要的预备知识、基础理论与研究中使用的理论工具、证明方法、协议构造方法，以及现代密码学研究的若干前沿领域。
全书分10章，内容包括预备知识、理论计算机科学基础、数论与代数基础、传统密码学协议的设计与分析、单向散列函数与随机性、公开密钥算法与数字签名、数字承诺、零知识证明与不经意传输、多方保密计算、量子密码学等。
本书可作为数学、计算机科学与技术、信息安全、通信等专业科研人员的参考书，也可供相关的教师、研究生参考。

<<现代密码学>>

书籍目录

版权说明