<<计算机安全与密码学>>

图书基本信息

书名：<<计算机安全与密码学>>

13位ISBN编号：9787121120268

10位ISBN编号：7121120267

出版时间：2010-11

出版时间：康海姆(Alan G.Konheim)、张焕国、唐明、 王后珍 电子工业出版社 (2010-11出版)

作者：(美) 康海涛 著
唐明

页数：436

前言

21世纪是信息的时代，信息已成为重要的战略资源。
信息的获取、存储、处理和信息的安全保障能力已成为一个国家综合国力的重要组成部分。
如果信息系统的安全受到危害，将会危及国家安全，引起社会混乱，从而造成重大损失。
因此，确保信息系统的安全已成为世人关注的社会问题，并成为信息科学技术领域中的研究热点。
在信息安全科学技术的发展与应用过程中，信息安全已经发展成为一个独立的学科门类。
信息安全学是研究信息获取、信息存储、信息传输及信息处理领域的安全威胁与安全保障问题的一门新兴学科。
密码学和以计算机安全为代表的信息系统安全，是信息安全学科的重要组成部分。
发展我国信息安全事业，人才培养是关键，而人才培养的基础是教育。
目前，在我国已有70多所高等学校建立了信息安全专业。
无论是计算机安全，还是密码学，都是信息安全专业的重要学习内容。
除了高校之外，如何有效地提高我国广大计算机用户的信息安全意识及对信息安全风险的基本防护能力，已经成为我国信息安全事业中的一个十分迫切的问题。
信息安全人才培养以及信息安全意识和风险防护能力的提高，都需要实施相应的教育，因此都需要教材。
为此，我们组织翻译出版了本书。
本书的作者.Alan G. Konheim是一位著名的密码专家。
他在1960年完成研究生学业后，便到IBM ThomasJ. Watson研究中心成为专职研究人员，并且在其中的数学研究部门工作了22年，主要从事数学在计算机科学中的应用研究。
从20世纪60年代中期，他开始担任数学科学的密码研究计划的负责人，并领导进行了数据加密标准（DES）的评估工作。
1982年，他离开IBM Thomas J.Watson研究中心，到加利福尼亚大学圣，巴巴拉分校计算机科学系担任教授。
在那里他讲授“汇编语言”、“性能评估”和“计算机网络与密码学”等课程，于2005年退休。
1981年他曾经出版《密码学初步》一书，后来又拍成电影。
他还先后在美国国家安全局和美国国防部分析研究所的通信研究分部工作过，并担任过美国国家安全局的技术顾问。

<<计算机安全与密码学>>

内容概要

《计算机安全与密码学》系统地介绍了密码学和计算机安全的基本原理及应用技术。
全书的内容可划分为以下四个部分。
第一部分介绍古典密码。
第二部分探讨第二次世界大战时期的密码。
第三部分分析现代密码，主要介绍了数据加密标准（DES）、高级数据加密标准（AES）、公钥密码的原理及大整数因子分解和离散对数问题、背包公钥密码、RSA公钥密码、椭圆曲线公钥密码（ECC）等。
第四部分描述密码技术的应用，主要介绍了数字签名与认证、密钥交换、操作系统口令、电子商务保护、ATM卡和智能卡等。
为便于教学，书中给出了大量例子，并配有许多习题，参考资料可以从网站得到。
《计算机安全与密码学》内容全面，讲述深入浅出，理论结合实际，适合课堂教学和自学，是一本难得的好书。
《计算机安全与密码学》可作为研究生和高年级本科生的教材，也可供从事信息安全、计算机、通信、电子工程及电子商务等领域的科技人员参考。

作者简介

作者：（美国）康海姆（Alan G.Konheim） 译者：唐明 王后珍 韩海清 等 合著者：张焕国康海姆(Konheim A.G.)，在1960年毕业后，我成为IBM的Thomas J.Watson研究中心（位于纽约的约克敦）的一名研究员。
在IBM数学科学部的22年中，我研究数学在计算机问题中的应用。
20世纪60年代中期开始，我成为数学加密项目的负责人；特别是针对DES算法的评价。
由于向往和我妻子Carol一同度过美丽的时光，我于1982年离开了IBM的实验室，转而接受了UCSB（加州大学圣巴巴拉分校）的教授职位。
在UCSB的24年里，我教授汇编语言、计算机网络和密码学。
我拓展了CMPSC 178（密码学导论），并且在UCSB开讲此课程21次，在以色列理工大学（位于以色列的海法）、拉特罗布大学（位于澳大利亚的墨尔本）和夏威夷大学（位于火奴鲁鲁）开讲此课程3次。
为了追求懒散的生活，我于2005年7月1日从UCSB退休。
由Wiley＆Sons Inc.于1981年出版的《密码学导论》，可能被拍成了电影。
1984年我在国家安全局度过了一个夏天。
接下来的三个夏天都在国防分析研究所（位于新泽西的普林斯顿）从事通信分析的研究。
1997～1999年间我成为国家安全局的顾问。

<<计算机安全与密码学>>

书籍目录

章节摘录

插图：

编辑推荐

《计算机安全与密码学》：国外计算机科学教材系列

版权说明