<<信息安全概论>>

图书基本信息

书名：<<信息安全概论>>

13位ISBN编号：9787030289698

10位ISBN编号：7030289692

出版时间：2010-9

出版时间：科学出版社

作者：唐晓波

页数：480

前言

信息资源管理（infornlation resource management，IRM）是20世纪70年代末兴起的一个新领域。
30多年来，IRM已发展成为影响最广、作用最大的管理领域之一，是一门受到广泛关注的富有生命力的新兴学科。
IRM对经济社会可持续发展和提高国家、区域、组织乃至个人的核心竞争力来说，都具有基础性的意义和独特的价值。
在国际范围内，受信息技术进步的推动和经济社会管理需求的牵引.IRM理论研究和职业实践发展迅速，并呈现出一些明显的特征：①广泛融合了信息科学、经济学、管理学、计算机科学、图书情报学等多学科的理论方法，形成以“信息资源”为管理对象的一个新学科，在管理学知识地图中确立了自己的地位。
②研究范式的形成和变化。
IRM的记录管理学派、信息系统学派、信息管理学派各自发展，以及管理理念、理论和技术方法的交叉融合，形成了IRM的集成管理学派。
集成管理学派以信息系统学派的继承和发展为主线，吸收了记录管理学派的内容管理和信息管理学派的社会研究视角，形成了IRM强调“管理”和“技术”，并在国家、组织、个人层面支持决策和各自目标实现的新的研究范式①。
③研究热点的变化。
当前IRM研究在国家、组织、个人层面上表现出新的研究热点，如国家层面的国家信息战略、国家信息主权与信息安全、信息政策与法规、支持危机管理的信息技术等；组织层面的信息系统理论，信息技术（系统）的绩效、价值与应用，IT投资，知识管理，电子商务，电子政务，IT部门与IT员工，虚拟组织，IRM技术等。

<<信息安全概论>>

内容概要

本书是《现代信息资源管理丛书》之一。
　本书系统介绍信息安全的理论知识、信息安全的技术以及信息安全方面的一些最新成果。
全书共分为10章，内容包括绪论、信息密码技术、信息认证技术、密钥管理技术、访问控制技术、操作系统安全和数据库安全、网络安全技术、应用安全机制、信息安全标准和信息安全的管理。
　本书可供信息管理与信息系统专业、信息资源管理专业、电子商务专业以及信息技术类专业本科生、研究生学习参考，也可供从事信息处理、通信保密及与信息安全工作的有关科研人员、工程技术人员和技术管理人员参考。

<<信息安全概论>>

作者简介

邱均平，武汉大学信息管理学院杠教育科学学院教授、博士生导师。
华中师范大学特聘教授。
我国著名情报学家和评价管理专家、文献计量学的主要奠基人之一。
享受国务院政府特殊津贴专家、湖北省有突出贡献的中青年专家。
现任湖北省人文社会科学重点研究基地__武汉大学中国科学评价研究中心主任、《评价与管理》杂志主编、《图书情报知识》杂志副主编；兼任教育部高等教育教学评估专家，教育部CSsCI指导委员会委员和中国管理科学研究院、南京理工大学等8个单位的研究员、教授或博士生导师，中国索引学会副理事长，中国科学学与科技政策研究会等4个全国性学会的常务理事及《情报学报》、《高教发展与评估》等14种杂志的编委。
一直从事“情报、计量、评价、管理”领域的教学和研究工作，特别在文献计量学、科学计量学与网络计量学、信息管理与知识管理、科学评价与大学评价等方面有精深研究。
指导和培养研究生100余名，其学生中不少已成为学术骨干或学科带头人；主持并完成国家和省部级课题28项，获国家社科基金重点项目优秀成果和湖北省社会科学优秀成果省级一等奖（2项）等55项各类学术奖励，特别是近几年来研发的“中国大学及学科专业评价系统”被省级鉴定为“国内领先”成果；出版著作40部，代表作有《文献计量学》、《信息计量学》、《知识管理学》、《大学评价与科研评价》、《中国大学及学科专业评价报告》、《中国学术期刊评价报告》等，其中《文献计量学》首次构建了理论、方法、应用相结合的内容体系，是本学科的奠基之作；《信息计量学》被选为教育部“面向21世纪课程教材”、《知识管理学》被、平为“普通高等教育‘十一五’国家级规划教材”；在国内外重要期刊如Scientometrios.《情报学报》、《中国图书馆学报》等上发表论文376篇，其中有60余篇获奖或被SC／、SSC／、《新华文摘》、《人大报刊复印资料》全文转载或收录。
据权威机构统计和发布，其学术影响力在“图书馆、情报与档案管理”学科领域名列第一，并被收入国际著名的英国剑桥、美国国际《世界名人录》等十多种大型辞书中。
唐晓波，教授，博士生导师。
现任武汉大学信息管理学院信息管理科学系主任；兼任国际信息系统协会中国分会理事、湖北省信息学会常务理事、武汉市系统工程学会理事。
1983年毕业于武汉水利电力大学电子技术专业获工学学士学位，1990年毕业于武汉水利电力大学计算机科学与技术专业获工学硕士学位，2007年毕业于武汉大学管理科学与工程专业获管理学博士学位。
主要从事管理信息系统、信息管理与知识管理、信息资源集成与利用、JT项目管理等领域的教学和研究工作。
近年来，发表学术论文50余篇，其中部分论文被SCI、EI、ISTP和ISSHP收录；出版学术专著4部。
主持教育部人文社会科学重点基地重大项目、教育部人文社会科学规划项目和横向项目近201页，参加多项国家自然科学基金重点项目、教育部重大攻关项目的研究工作。

<<信息安全概论>>

书籍目录

章节摘录

插图：2.4.6分组密码的分析方式密码是用来对明文提供保护，防止明文泄露的。
而密码分析人员的任务是在某种意义下破译密码。
如果密码分析者能确定该密码正在使用的密钥，则他就可以像合法用户一样阅读所有的消息，则称该密码是完全可破译的；如果密码分析者仅能从所窃获的密文恢复明文，但他却不能发现密钥，则称该密码是部分可破译的。
根据攻击者掌握的信息，可将分组密码的攻击分为以下4类：1）唯密文攻击：攻击者除了截获的密文外，没有其他可利用的信息。
2）已知明文攻击：攻击者仅知道当前密钥下的一些明密文对。
3）选择明文攻击：攻击者能获得当前密钥下的一些特定的明文所对应的密文。
4）选择密文攻击：攻击者能获得当前密钥下的一些特定的密文所对应的明文。
显然，在上述的4类攻击中，选择明文攻击是密码分析者可能发动的最强打力的攻击，但是在许多场合这种攻击是不现实的。
一种攻击的复杂度可以分为两部分，即数据复杂度和处理复杂度。
数据复杂度是实施该攻击所需输入的数据量；处理复杂度是处理这些数据所需的计算量。
对某一攻击通常是以这两个方面的其中之一为主要因素，来刻画攻击复杂度。
例如：穷举攻击所需的数据量和计算量相比微不足道，因此穷举攻击的复杂度实际就是考虑处理复杂度；差分密码分析是一种选择明文攻击，其复杂度主要是由该攻击所需的明密文对的数量来确定，而实施该攻击所需的计算量相对来说要小的多。
下面是几种常见的攻击方法。

<<信息安全概论>>

编辑推荐

《信息安全概论》：现代信息资源管理丛书

版权说明