普通高等教育“十五”国家级规划教材

信息安全概论

牛少彰摇主编

北京邮电大学出版社
·北京·

信息安全专业系列教材
编摇委摇会

总摇摇序

办好信息安全本科专业的第一要素是拥有高质量的教材。由于各方面的原因，我国开办信息安全本科专业的历史很短，刚刚起步，但是，当前以各种形式开办信息安全本科专业的高等院校却非常多，学生总数也相当可观，而且其中大部分学生已经学完基础课程，即将进入专业课的学习阶段。

与信息安全本科专业招生的火爆场面形成鲜明对比的是，到目前为止，我国还没有一套自己的信息安全本科专业系列教材。为了保证信息安全本科专业学生的培养质量，[illegible]年，北京市教委以“精品教材立项”的形式委托我们北京邮电大学信息安全中心负责编写《现代密码学基础》、《信息安全概论》、《网络安全》、《信息隐藏与数字水印》、《入侵检测》、《计算机病毒原理及防治》等 远本教材，随后，教育部又将此套系列教材列入了“普通高等教育‘十五’国家级教材规划”。由此可见，此套教材的编写确实受到了各级教育主管部门的高度重视。

北京邮电大学信息安全中心是一专门从事信息安全的教学、科研和成果转化的重点实验室。该实验室已经培养出了我国第一位密码学博士，而且在“信息安全”和“密码学”两个专业领域内健全了博士后、博士、硕士和本科的培养教育体系，已经培养出了数以百计的信息安全研究生。

在接受了北京市教委和教育部的编写信息安全本科系列教材的任务之后，我们立即组织了最强的师资队伍投入到教材的编写工作之中。经过两年多的不懈努力，数易其稿，反复研讨，按照教育目标和大学生基本素质培养的要求，本着推进理工融合及学科交叉的思想，经过优化课程体系和精选课程内容，我们终于完成了信息安全本科专业系列教材的第一批教材（共 远本）。现在我们正在着手规划信息安全本科专业的第二批教材，它们的暂定名分别是《安全操作系统》、《安全数据库》、《安全访问控制》、《安全检测与监控》、《数字证书与管理》、《安全备份与灾难恢复》、《安全隔离技术》、《安全服务技

术》、《安全系统工程》、《安全规范与标准》等。我们诚意邀请国内所有高等院校的权威安全专家加入第二批教材的编写工作（有意者请与我们直接联系。地址：北京邮电大学信息安全中心，邮箱）。我们希望这套信息安全本科专业系列教材最终完成之后能够基本满足国内各类高校信息安全本科专业的普遍需求。

虽然我们的目标是编写一套适合信息安全专业本科生使用的精品教材，但是，由于水平有限，时间仓促，且信息安全本科专业刚刚开始，我们还没有足够的实践机会，不足之处和错误在所难免，恳请读者和同行专家多提意见，以便我们再版时充分修改，不断完善。

衷心感谢北京邮电大学胡正名教授对本套教材的大力支持，感谢北京邮电大学信息安全中心二百余位成员的支持与配合。本套教材也是国家自然科学基金项目（）和国家“”项目（）资助的成果，在此一并表示感谢。

杨义先 教授、博士生导师、全国政协委员
于北京邮电大学信息安全中心

内 容 简 介

随着信息社会的到来，人们在享受信息资源所带来的巨大的利益的同时，也面临着信息安全的严峻考验。本书全面介绍了信息安全的基本概念、原理和知识体系，主要内容包括信息保密技术、信息认证技术、密钥管理技术、访问控制技术、数据库安全、网络安全技术、信息安全标准和信息安全管理等内容。

本书内容全面，既有信息安全的理论知识，又有信息安全的实用技术。文字流畅，表述严谨，并包括信息安全方面的一些最新成果。本书可作为高等院校信息安全相关专业的本科生、研究生的教材或参考书，也可供从事信息处理、通信保密及与信息安全有关的科研人员、工程技术人员和技术管理人员参考。

摇图书在版编目（悦陨孕）数据

摇信息安全概论 辕牛少彰主编援—北京：北京邮电大学出版社，圆园园源
摇陨杂月晕 苑鄄缘远猿缘鄄园愿园远鄄园

摇Ⅰ援信…摇Ⅱ援牛…摇Ⅲ援信息系统－安全技术－概论摇Ⅳ援栽孕猿园怨

摇中国版本图书馆 悦陨孕 数据核字（圆园园源）第 园圆源缘远缘号

书　　名：信息安全概论
主　　编：牛少彰
责任编辑：王守平
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 员园号（员园园愿苑远）
电话传真：园员园鄄远圆圆愿圆员怨猿（发行部）　园员园鄄远圆圆愿猿缘苑愿（传真）
电子信箱：贼赠凿曾泽＠遭怎责贼援藻凿怎援糟灶
经　　销：各地新华书店
印　　刷：北京源海印刷厂印刷
开　　本：苑愿苑 皂皂×员园怨圆 皂皂　员／员远
印　　张：员远援缘
字　　数：猿猿源千字
印　　数：员—缘园园园册
版　　次：圆园园源年 源月第 员版摇圆园园源年 源月第 员次印刷

陨杂月晕 苑鄄缘远猿缘鄄园愿园远鄄园／栽孕·苑愿猿　　定摇价：圆远援园园元

·如有印装质量问题，请与北京邮电大学出版社发行部联系·

前摇摇言

随着信息社会的到来，人们在享受信息资源所带来的巨大的利益的同时，也面临着信息安全的严峻考验。信息安全已经成为世界性的现实问题，信息安全问题已威胁到国家的政治、经济、军事、文化、意识形态等领域，同时，信息安全问题也是人们能否保护自己个人隐私的关键。信息安全是社会稳定安全的必要前提条件。本书全面介绍了信息安全的基本概念、原理和知识体系，主要内容包括信息保密技术、信息认证技术、访问控制技术、密钥管理技术、数据库安全、网络安全技术、信息安全标准和信息安全管理等内容。

本书内容全面，既有信息安全的理论知识，又有信息安全的实用技术，并包括信息安全方面的一些最新成果。本书可作为高等院校信息安全相关专业的本科生、研究生的教材或参考书，也可供从事信息处理、通信保密及与信息安全有关的科研人员、工程技术人员和技术管理人员参考。本书的教学时数约为 猿源学时，每章后面均有小结并配有习题。

在本书编写的过程中，赵义斌参加了第 圆章和第 猿章初稿的编写，李志虎参加了第 苑章的编写，刘歆编写了第 怨章，郭春碌参加了第 远章的编写，翟军华参加了第 愿章的编写，张晓芬、邓雁城、郭延龄、谢正程参加了书稿的讨论。此外，刘歆还在本书的整理和校对方面做了许多工作。

在本书的编写过程中，还得到了很多老师同学的关心和帮助。北京邮电大学出版社为本书的出版付出了大量的工作，借此表示衷心感谢。

限于编者水平有限，书中难免有疏漏和错误之处，恳请读者批评指正。

作摇者

圆园园源年 猿月

员

目摇摇录

第猿章摇信息认证技术

猿

源

第 愿章摇信息安全标准

第 怨章摇信息安全的管理

第 员章摇绪摇论

随着现代通信技术迅速的发展和普及，特别是随着通信与计算机相结合而诞生的计算机互联网络全面进入千家万户，信息的应用与共享日益广泛，且更为深入。世界范围的信息革命激发了人类历史上最活跃的生产力，人类开始从主要依赖物质和能源的社会步入物质、能源和信息三位一体的社会。各种信息系统已成为国家基础设施，支撑着电子政务、电子商务、电子金融、科学研究、网络教育、能源、通信、交通和社会保障等方方面面，信息成为人类社会必需的重要资源。

与此同时信息的安全问题也日渐突出，情况也越来越复杂。从大的方面来说，信息安全问题已威胁到国家的政治、经济、军事、文化、意识形态等领域，因此很早就有人提出了“信息战”的概念并将信息武器列为继原子武器、生物武器、化学武器之后的第四大武器；从小的方面来说，信息安全问题也涉及到人们能否保护个人隐私。

信息安全已成为社会稳定安全的必要前提条件。

信息安全，即关注信息本身的安全，以防止偶然的或未授权者对信息的恶意泄露、修改和破坏，从而导致信息的不可靠或无法处理等问题，能使人类在最大限度地利用信息的同时而不招致损失或使损失最小。

员援员摇信息的定义、性质和分类

在人类社会的早期，人们对信息的认识比较肤浅而模糊，对信息的含义没有明确的定义。到了圆园世纪特别是中期以后，随着科学技术的发展，特别是信息科学技术的发展，对人类社会产生了深刻的影响，迫使人们开始探讨信息的准确含义。

员援员援员摇信息的概念

员怨圆愿年，哈特莱（砸援灾援蕴援匀葬则贼造藻赠）在《贝尔系统技术杂志》（月杂栽允）上发表了一篇题为“信息传输”的论文。在这篇论文中，他把信息理解为选择通信符号的方式，且用选择的自由度来计量这种信息的大小。哈特莱认为，任何通信系统的发信端总有一个字母表

（或符号表），发信者所发出的信息，就是他在通信符号表中选择符号的具体方式。假设这个符号表中一共有 n 个不同的符号，发送信息选定的符号序列包含 m 个符号，则从这个符号表中共有 n^m 种不同的选择方式，因而可以形成 n^m 个长度为 m 的序列。因此，就可以把发信者产生信息的过程看成是从 n^m 个不同的序列中选定一个特定序列的过程，或者说是排除其它序列的过程。

哈特莱的这种理解在一定程度上解释了通信工程中的一些信息问题，但也存在一些严重的局限性。主要表现在：一方面，他所定义的信息不涉及内容和价值，只考虑选择的方式，也没有考虑到信息的统计性质；另一方面，将信息理解为选择的方式，就必须有一个选择的主题作为限制条件。这些缺点使它的适用范围受到很大的限制。

[illegible]年，美国数学家仙农（[illegible]）在《贝尔系统技术杂志》上发表了一篇题为“通信的数学理论”的论文，在对信息的认识方面取得了重大突破，堪称信息论的创始人。这篇论文以概率论为基础，深刻阐述了通信工程的一系列基本理论问题，给出了计算信源信息量和信道容量的方法和一般公式，得到了著名的编码三大定理，为现代通信技术的发展奠定了理论基础。

仙农指出，通信系统所处理的信息在本质上都是随机的，可以用统计方法进行处理。仙农在进行信息的定量计算的时候，明确地把信息量定义为随机不定性程度的减少，这就表明了他对信息的理解是：信息是用来减少随机不定性的东西。

虽然仙农的信息概念比以往的认识有了巨大的进步，但仍存在局限性，这一概念同样没有包含信息的内容和价值，只考虑了随机型的不定性，没有从根本上回答“信息是什么”的问题。

[illegible]年，就在仙农创立信息论的同时，维纳（[illegible]）出版了专著《控制论：动物和机器中的通信与控制问题》，创建了控制论。后来人们常常将信息论、控制论和系统论合称为“三论”，或统称为“系统科学”或“信息科学”。

维纳从控制论的角度出发，认为“信息是人们在适应外部世界，并且这种适应反作用于外部世界的过程中，同外部世界进行互相交换的内容的名称”。维纳关于信息的定义包含了信息的内容与价值，从动态的角度揭示了信息的功能与范围，但也有局限性。由于人们在与外部世界的相互作用过程中，同时也存在着物质与能量的交换，维纳关于信息的定义没有将信息与物质、能量区别开来。

[illegible]年，意大利学者朗高（[illegible]）在《信息论：新的趋势与未决问题》一书的序言中认为“信息是反映事物的形式、关系和差别的东西，它包含在事物的差异之中，而不在事物本身”。当然，“有差异就是信息”的观点是正确的，但是反过来说“没有差异就没有信息”就不够确切。所以，“信息就是差异”的定义也有其局限性。

据不完全统计，有关信息的定义有[illegible]多种，它们都从不同的侧面、不同的层次揭示了信息的特征与性质，但同时也都有这样或那样的局限性。

员怨愿愿年，我国信息论专家钟义信教授在《信息科学原理》一书中把信息定义为：事物运动的状态和状态变化的方式。并通过引入约束条件推导了信息的概念体系，对信息进行了完整和准确的描述。信息的这个定义具有最大的普遍性，不仅涵盖所有其他的信息定义，而且通过引入约束条件还能转化为所有其他的信息定义。

为了进一步加深对信息概念的理解，下面讨论一些与信息概念关系特别密切、但又很容易混淆的相关概念。

- 信息不同于消息，消息是信息的外壳，信息则是消息的内核，也可以说：消息是信息的笼统概念，信息则是消息的精确概念；
- 信息不同于信号，信号是信息的载体，信息则是信号所载荷的内容；
- 信息不同于数据，数据是记录信息的一种形式，同样的信息也可以用文字或图像来表述。当然，在计算机里，所有的多媒体文件都是用数据表示的，计算机和网络上信息的传递都是以数据的形式进行，此时信息等同于数据；
- 信息不同于情报，情报通常是指秘密的、专门的、新颖的一类信息，可以说所有的情报都是信息，但不能说所有的信息都是情报；
- 信息也不同于知识，知识是由信息抽象出来的产物，是一种具有普遍的和概括性的信息，是信息的一个特殊的子集，也就是说：知识就是信息，但并非所有的信息都是知识。

综上所述，一般意义上的信息定义为：信息是事物运动的状态和状态变化的方式。如果引入必要的约束条件，则可形成信息的概念体系。信息有许多独特的性质与功能，它是可以测度的，正因为如此，才导致信息论的出现。

员摇摇信息的特征

信息有许多重要的特征。最基本的特征为：

信息来源于物质，又不是物质本身：它从物质的运动中产生出来，又可以脱离源物质而寄生于媒体之中，相对独立地存在。信息是“事物运动的状态和状态变化方式”，但“事物运动的状态和状态变化方式”并不是物质本身，信息不等于物质。

信息也来源于精神世界。既然信息是事物运动的状态与状态变化方式，那么精神领域的事物运动（思维的过程）当然可以成为信息的一个来源。同客观物体所产生的信息一样，精神领域的信息也具有相对独立性，可以被记录并加以保存。

信息与能量息息相关，传输信息或处理信息总需要一定的能量来支持，而控制和利用能量需要信息来引导。但是信息与能量又有本质的区别，即信息是事物运动的状态和状态变化的方式，能量是事物做功的本领，提供的是动力。

信息是具体的并可以被人（生物、机器等）所感知、提取、识别，可以被传递、储存、变换、处理、显示、检索、复制和共享。

正是由于信息可以脱离源物质而载荷于媒体物质，可以被无限制地进行复制和传播，

因此信息可为众多用户所共享。

员遥遥遥遥信息的性质

信息具有下面一些重要的性质。

(员) 普遍性:信息是事物运动的状态和状态变化的方式,因此,只要有事物的存在,只要事物在不断地运动,就会有它们运动的状态和状态变化的方式,也就存在着信息,所以信息是普遍存在的,即信息具有普遍性。

(圆) 无限性:在整个宇宙时空中,信息是无限的,即使是在有限的空间中,信息也是无限的。由于一切事物运动的状态和方式都是信息,而事物是无限多样的,事物的发展变化更是无限的,因而信息是无限的。

(猿) 相对性:对于同一个事物,不同的观察者所能获得的信息量可能不同。

(源) 传递性:信息可以在时间上或在空间中从一点传递到另一点。

(缘) 变换性:信息是可变换的,它可以用不同载体以不同的方法来载荷。

(远) 有序性:信息可以用来消除系统的不定性,增加系统的有序性。获得了信息,就可以消除认识主体对于事物运动状态和状态变化方式的不定性。信息的这一性质对人类具有特别重要的价值。

(苑) 动态性:信息具有动态性质,一切信息都随时间而变化,因此,信息是有时效的。由于事物本身在不断发展变化,因而信息也会随之变化。脱离了母体的信息因为不再能够反映母体的新的运动状态和状态变化方式而使其效用降低,以至完全失去效用,这就是信息的时效性。所以人们在获得信息之后,不能就此满足,要不断补充和更新。

(愿) 转化性:在一定的条件下,信息可以转化为物质、能量。

上面的这些性质是信息的主要性质。了解信息的性质,一方面有助于对信息概念的进一步理解,另一方面也有助于人们更有效地掌握和利用信息,一旦被人们有效而正确地利用时,就可能在同样的条件下创造更多的物质财富和能量。

员遥遥遥遥信息的功能

信息的基本功能在于维持和强化世界的有序性,可以说,缺少物质的世界是空虚的世界,缺少能量的世界是死寂的世界,缺少信息的世界是混乱的世界。信息的社会功能则表现在维系社会的生存,促进人类文明的进步和人类自身的发展。

信息具有许多有用的功能,主要表现在以下几个方面:

- 信息是一切生物进化的导向资源。生物生存于自然环境之中,而外部自然环境经常发生变化,如果生物不能得到这些变化的信息,生物就不能及时采取必要的措施来适应环境的变化,就可能被变化了环境所淘汰。

- 信息是知识的来源。知识是人类长期实践的结晶,知识一方面是人们认识世界的结果,另一方面又是人们改造世界的方法,信息具有知识的秉性,可以通过一定的归纳算