高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材

信息安全工程人才培养规范

（卓越工程师计划）

张仕斌　吴春旺　编著

西安电子科技大学出版社
http://www.xduph.com

高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材

信息安全工程人才培养规范

（卓越工程师计划）

张仕斌　吴春旺　编著

西安电子科技大学出版社

内容简介

本书共8章，主要包括信息安全专业的学科基础，信息安全专业卓越工程师培养目标及培养标准，信息安全专业的知识能力体系及培养标准实现矩阵，信息安全专业卓越工程师培养计划课程体系的设置、信息安全专业卓越工程师企业学习阶段的培养方案、信息安全专业卓越工程师培养计划的质量保障体系、信息安全专业卓越工程师培养规范制定的主要参考指标以及信息安全专业知识导论等内容。

本书初步建立起了一整套完善的信息安全专业卓越工程师培养计划体系，可作为标准性文件，规范、指导信息安全专业卓越工程师的培养。

本书既可以作为高等院校信息安全专业师生和教育管理人员的用书，也可以供其他高等院校、信息安全相关行业、企事业单位参考。

图书在版编目(CIP)数据

信息安全工程人才培养规范/张仕斌，吴春旺编著. —西安：西安电子科技大学出版社，2015.11
高等学校电子信息类“十三五”规划教材
ISBN 978-7-5606-3897-3

Ⅰ.①信… Ⅱ.①张… ②吴… Ⅲ.①信息安全—人才培养—高等学校—教材 Ⅳ.①TP309

中国版本图书馆CIP数据核字(2015)第256230号

策划编辑 李惠萍
责任编辑 王文秀 李惠萍
出版发行 西安电子科技大学出版社(西安市太白南路2号)
电 话 (029)88242885 88201467 邮 编 710071
网 址 www.xduph.com 电子邮箱 xdupfxb001@163.com
经 销 新华书店
印刷单位 陕西天意印务有限责任公司
版 次 2015年11月第1版 2015年11月第1次印刷
开 本 787毫米×1092毫米 1/16 印 张 11.375
字 数 259千字
印 数 1～3000册
定 价 20.00元
ISBN 978-7-5606-3897-3/TP

XDUP 4189001-1

*****如有印装问题可调换*****

序

进入21世纪以来，信息技术迅速改变着人们传统的生产和生活方式，社会的信息化已经成为当今世界发展不可逆转的趋势和潮流。信息作为一种重要的战略资源，与物资、能源、人力一起已被视为现代社会生产力的主要因素。目前，世界各国围绕着信息获取、利用和控制的国际竞争日趋激烈，使得网络与信息安全问题成为一个世纪性、全球性的课题。党的十八大报告明确指出，要“高度关注海洋、太空、网络空间安全”。党的十八届三中全会决定设立国家安全委员会，成立中央网络安全和信息化领导小组，并把网络与信息安全列入了国家发展的最高战略方向之一。这为包含网络空间安全在内的非传统安全领域问题的有效治理提供了重要的体制机制保障，是我国国家安全体制机制的一个重大创新性举措，彰显了我国政府治国理政的战略新思维和“大安全观”。

人才资源是确保我国网络与信息安全第一位的资源，信息安全人才培养是国家信息安全保障体系建设的基础和必备条件。随着我国信息化和信息安全产业的快速发展，社会对信息安全人才的需求不断增加。2015年6月11日，国务院学位委员会和教育部联合发出“学位[2015]11号”通知，决定在“工学”门类下增设“网络空间安全”一级学科，代码为“0839”，授予工学学位。这是国家推进专业化教育，在信息安全领域掌握自主权、抢占先机的重要举措。

建国以来，我国高等工科院校一直是培养各类高级应用型专门人才的主力。培养网络与信息安全高级应用型专门人才也是高等院校责无旁贷的责任。目前，许多高等院校和科研院所已经开办了信息安全专业或开设了相关课程。作为国家首批61所“卓越工程师教育培养计划”试点院校之一，成都信息工程大学以《国家中长期教育改革和发展规划纲要(2010—2020年)》、《国家中长期人才发展规划纲要(2010—2020年)》、《卓越工程师教育培养计划通用标准》为指导，以专业建设和工程技术为主线，始终贯彻“面向工业界、面向未来、面向世界”的工程教育理念，按照“育人为本、崇尚应

用”、“一切为了学生”的教学教育理念和“夯实基础、强化实践、注重创新、突出特色”的人才培养思路，遵循“行业指导、校企合作、分类实施、形式多样”的原则，实施了一系列教育教学改革。令人欣喜的是，该校信息安全工程学院与西安电子科技大学出版社近期联合组织了一系列网络与信息安全专业教育教学改革的研讨活动，共同研讨培养应用型高级网络与信息安全工程技术人才的教育教学方法和课程体系，并在总结近年来该校信息安全专业实施“卓越工程师教育培养计划”教育教学改革成果和经验的基础上，组织编写了“应用型高级网络与信息安全工程技术人才培养系列教材”。本套教材总结了该校信息安全专业教育教学改革成果和经验，相关课程有配套的课程过程化考核系统，是培养应用型网络与信息安全工程技术人才的一套比较完整、实用的教材，相信可以对我国高等院校网络与信息安全专业的建设起到很好的促进作用。该套教材为中国电子教育学会高教分会推荐教材。

信息安全是相对的，信息安全领域的对抗永无止境。国家对信息安全人才的需求是长期的、旺盛的。衷心希望本套教材在培养我国合格的应用型网络与信息安全工程技术人才的过程中取得成功并不断完善，为我国信息安全事业做出自己的贡献。

高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材
名誉主编（中国密码学会常务理事）

何大可

二〇一五年九月

中国电子教育学会高教分会推荐

高等学校电子信息类“十三五”规划教材

应用型网络与信息安全工程技术人才培养系列教材

编审专家委员会名单

名誉主任：何大可（中国密码学会常务理事）

主　　任：张仕斌（成都信息工程大学信息安全学院副院长、教授）

副 主 任：李　飞（成都信息工程大学信息安全学院院长、教授）

何明星（西华大学计算机与软件工程学院院长、教授）

苗　放（成都大学计算机学院院长、教授）

赵　刚（西南石油大学计算机学院院长、教授）

李成大（成都工业学院教务处处长、教授）

宋文强（重庆邮电大学移通学院计算机科学系主任、教授）

梁金明（四川理工学院计算机学院副院长、教授）

易　勇（四川大学锦江学院计算机学院副院长、成都大学计算机学院教授）

杨瑞良（成都东软学院计算机科学与技术系主任、教授）

编审专家委员：（排名不分先后）

范太华　叶安胜　黄晓芳　黎建文　张　洪　张　蕾　贾　浩

赵　攀　陈　雁　韩　斌　李享梅　曾令明　何林波　盛志伟

林宏刚　王海春　索　望　吴春旺　韩桂华　赵　军　陈　丁

秦　智　王中科　林春蔷　张金全　王祖俪　蔺　冰　王　敏

万武南　甘　刚　王　燚　闫丽丽　昌　燕　黄源源　张仕斌

李　飞　王海春　何明星　苗　放　李成大　宋文强　梁金明

万国根　易　勇　杨瑞良

前　言

21世纪，信息科学技术与产业空前繁荣，信息技术的广泛应用促进了全球资源的优化配置和发展模式的创新，互联网对各国政治、经济、社会和文化的影响愈加深远。信息作为一种重要的战略资源，已与物资、能源、人力一起被列为现代社会生产力的重要因素。目前，世界各国围绕着信息获取、利用和控制的国际竞争日趋激烈，网络与信息安全面临的形势日益严峻。当前，特别是随着经济社会和信息化进程的全面加快，网络与信息系统的基础性、全面性作用日益增强，网络与信息安全已成为国家安全的重要组成部分。党的十八大明确指出要“高度关注海洋、太空、网络空间安全”。因此，加快国家信息安全保障体系建设，确保我国的信息安全，已经成为我国发展的最高战略方向之一。人才资源是确保我国信息安全第一位的资源，信息安全人才培养是国家信息安全保障体系建设的基础和必备条件。

一直以来，党中央、国务院都十分重视信息安全学科和专业的建设以及人才培养工作。2003年，国家信息化领导小组颁布的27号文件明确提出，我国要加强信息安全保障工作，必须有一批高素质的信息安全管理和技术人才，要加强信息安全学科和专业的建设，加快信息安全人才的培养；2005年，教育部发布7号文件指出发展和建设我国信息安全保障体系，人才培养是必备基础和先决条件，并对我国信息安全学科和专业的建设提出了明确要求；2007年，教育部决定成立高等学校信息安全专业教学指导委员会，负责对我国高等学校信息安全专业的建设进行指导；2012年，国发23号文件大力支持信息安全学科师资队伍、专业院系、学科体系和重点实验室的建设，对高等院校信息安全学科与专业的建设给予政策支持；2014年2月27日，习近平总书记在网络安全与信息化领导小组成立大会上指出，加强网络信息安全人才队伍建设，要把造就世界水平的科学家、网络科技领军人才、卓越工程师、高水平创新团队作为国家的战略任务来抓，切实把人才资源汇聚起来，建设一支政治强、业务精、作风好的强大队伍；2015年6月，为实施国家安全战略，加快网络空间安全高层次人才培养，国务院学位委员会、教育部决定在“工学”门类下增设“网络空间安全”一级学科。

自2010年6月23日教育部正式启动“卓越工程师教育培养计划”以来，随着工程教育理念研究的深入和各高等院校“卓越工程师教育培养计划”试点专业工作的展开，“卓越工程师教育培养计划”有了更加明确的方向。作为国家首批61所“卓越工程师教育培养计划”试点高等院校，成都信息工程大学信息安全工学院根据《国家中长期教育改革和

发展规划纲要（2010—2020年）》、《国家中长期人才发展规划纲要（2010—2020年）》、《卓越工程师教育培养计划通用标准》的要求，结合近几年来我校信息安全专业实施“卓越工程师教育培养计划”的成果和经验，对原有我校信息安全专业卓越工程师人才培养方案进行了修订和完善，制定出了信息安全专业卓越工程师人才培养规范，即本规范，有力地推动了我校信息安全专业“卓越工程师教育培养计划”的实施。

在本规范的编写过程中，我们牢牢把握信息安全理论与技术及信息安全应用行业飞速发展的时代背景，始终贯彻“面向工业界、面向未来、面向世界”的工程教育理念，按照“育人为本、崇尚应用”、“一切为了学生”的教育教学理念和“夯实基础、强化实践、注重创新、突出特色”的人才培养思路，遵循“行业指导、校企合作、分类实施、形式多样”的原则，以实际工程为背景，以社会需求为导向，以工程技术为主线，着力提高信息安全专业学生的创新意识、工程素质和工程实践能力。

我们在遵循信息安全专业技术人才培养规律的基础上，对信息安全行业、企事业单位进行了大量走访，广泛听取了信息安全行业、企事业单位的意见，建立了一整套完善的信息安全专业卓越工程师培养计划体系，既可以作为高校信息安全专业卓越工程师培养的标准性文件，也可以供高等院校信息安全相关专业、行业、企事业单位参考。

在本规范的编写过程中，编者参考了国内外一些书籍及互联网上公布的相关资料，所参考的资料已尽量在参考文献中列出，但由于网上资料数量众多且杂乱，所以可能无法把所有文献的出处一一注明。在此对这些参考文献的作者表示衷心的感谢。编者写作过程中参考的这些资料，其原文版权属于原编者，特此声明。

本规范获得了成都信息工程大学教改项目（NO. Z2015002）的资助，以及四川省卓越工程师培养计划项目的支持。

本规范由张仕斌教授和吴春旺老师负责编写，其中吴春旺老师参与第5章的编写，其余章节由张仕斌教授编写，全书由张仕斌教授统稿。

本规范的编写得到了成都信息工程大学、西安电子科技大学出版社和相关高等院校的大力支持与热情帮助，在此一并致以诚挚的谢意。由于时间仓促，疏漏之处在所难免，恳请读者对本规范提出宝贵意见，以便作进一步完善。

编　者

二〇一五年八月于成都

目　录

第1章　信息安全专业的学科基础

1.1　信息安全学科的内涵

目前，学术界关于信息安全学科的定义和内涵，仍未有统一的说法，许多学者根据自己的理解和研究给出了不同的解释。尽管这些解释不尽相同，但是其核心内容是相同的。

传统的信息安全强调信息(数据)本身的安全属性，认为信息安全是指对信息的机密性、完整性和可用性进行保护，即面向数据的安全。但是信息论告诉我们，信息不能脱离它的载体而孤立存在。因此，我们不能脱离信息系统而孤立地谈论信息安全。通常说，每当我们谈论信息安全时也总是不可避免地要谈论信息系统的安全，这正是因为若信息系统的安全受到危害，则必然会危害到存在于信息系统中的信息的安全。因此，我们还应当从信息系统的角度来全面考虑信息安全的内涵。信息系统安全主要包括设备安全、数据安全、内容安全和行为安全四个方面，其中数据安全是传统的信息安全。

1. 设备安全

信息系统设备(包括硬件设备和软件设备)的安全是信息系统安全的首要问题，主要包括以下三个方面：

(1) 设备的稳定性(Stability)：设备在一定时间内不出故障的概率；

(2) 设备的可靠性(Reliability)：设备在一个给定的时间内能正常执行任务的概率；

(3) 设备的可用性(Availability)：设备随时可以正常使用的概率。

2. 数据安全

数据安全是指采取措施确保数据免受未授权的泄露、篡改和毁坏，主要包括以下三个方面：

(1) 数据的保密性(Secrecy)：使信息不泄露给未授权者的特性；

(2) 数据的完整性(Integrity)：保护信息真实、完整和未被修改的特性；

(3) 数据的可用性(Availability)：已授权实体一旦需要就可访问和使用信息的特性。

3. 内容安全

内容安全是信息安全在政治、法律、道德层次上的要求，主要包括以下三个方面：

(1) 信息内容在政治上是健康的；

(2) 信息内容符合国家的法律法规；

(3) 信息内容符合中华民族优良的道德规范。

4. 行为安全

在信息系统中许多数据是程序，程序是要进行某种处理的，处理的过程称为行为。程

序在静态存储时就是一种数据，因此数据安全是静态安全。而程序在运行时（也就是动态时）表现为一系列的行为。因此，除了要确保静态的数据安全外，还需要确保动态的行为安全。行为安全是考察主体行为的过程和结果是否会危害信息安全，或者是否能够确保信息安全。从行为安全的角度来分析和确保信息安全，符合哲学上实践是检验真理唯一标准的基本原理。行为安全主要包括以下三个方面的内容。

（1）行为的保密性：行为的过程和结果不能危害数据的保密性，必要时行为的过程和结果也应是保密的；

（2）行为的完整性：行为的过程和结果不能危害数据的完整性，行为的过程和结果是预期的；

（3）行为的可控性：当行为的过程出现偏离预期时，能够发现、控制或纠正。

由以上分析可知，要确保信息系统的安全，就必须确保信息系统的设备安全、数据安全、内容安全和行为安全。信息系统的硬件系统安全和操作系统安全是信息系统安全的基础，密码和网络安全等技术是信息系统安全的关键技术。确保信息系统安全是一个系统工程，只有从信息系统的硬件和软件的底层做起，从整体上采取措施，才能比较有效地确保信息系统的安全。[注：为了表述简单，在不会产生歧义时可以直接将信息系统安全简称为信息安全。]

综上所述，这里给出大家比较公认的信息安全学科内涵的定义：信息安全学科是研究信息获取、信息存储、信息传输和信息处理领域中信息安全保障问题的一门新兴学科。

1.2 信息安全学科的主要研究方向及内容

信息安全学科是交叉融合了计算机、电子、通信、数学、物理、生物、法律、管理及教育等学科，并发展演绎而形成的一门综合性学科。信息安全学科与这些学科既有紧密的联系，又有本质的不同，目前它已形成了自己的内涵、理论、技术和应用，并服务于信息社会，是一门独立的学科。信息安全学科属于工学，但考虑到现阶段我国的信息安全专业发展的实际情况，允许不同的学校给信息安全专业的毕业生授予工学、理学或管理学学位。

当前，信息安全学科的主要研究方向包括密码学、网络安全、信息系统安全、信息内容安全和信息对抗。但随着信息安全科学与技术的发展和应用，信息安全学科一定还会产生新的研究方向，其研究内容也将不断丰富。下面简要介绍密码学、网络安全、信息系统安全、信息内容安全和信息对抗这五个研究方向的主要研究内容。

1. 密码学

密码学由密码编码学、密码分析学和密钥密码学组成。其中，密码编码学主要研究对信息进行编码以实现信息隐蔽；密码分析学主要研究通过密文获取对应的明文信息；密钥密码学主要以密钥管理作为研究对象，研究内容包括密钥的产生、分配、存储、保护、销毁等环节。密码学研究密码理论、密码算法、密码协议、密码技术、密码应用和密钥管理等，具体内容包括对称密码、公钥密码、Hash 函数、密码协议、新型密码（如量子密码、生物密码等）、密码应用和密钥管理等。

2. 网络安全

网络安全的基本思想是在网络的各个层次和范围内采取防护措施，以便能对各种网络

安全威胁进行检测和发现，并采取相应的响应措施，确保网络环境中信息的安全。其中，防护、检测和响应都需要基于一定的安全策略和安全机制。网络安全的研究包括网络安全威胁、网络安全理论、网络安全技术和网络安全应用等，具体内容有：网络安全威胁、通信安全、协议安全、网络防护、入侵检测、入侵响应和可信网络等。

3. 信息系统安全

信息系统是提供服务的各种软硬件系统，用户通过信息系统得到信息的服务。在实际应用中，有的信息系统规模小，但许多信息系统是复杂庞大的(如操作系统、数据库系统、电子商务系统、电子政务系统等)。信息系统是信息的载体，它应当确保存在于其中的信息的安全。信息系统安全的特点是从系统的整体上考虑信息安全威胁并采取防护措施，其主要的研究内容包括信息系统的安全威胁、信息系统的设备安全、信息系统的硬件系统安全、信息系统的软件系统安全、访问控制、可信计算、信息系统安全测评认证、信息系统安全等级保护和应用信息系统安全。

4. 信息内容安全

信息内容安全是信息安全在政治、法律、道德层次上的要求。所谓信息内容是安全的，其实就是要求信息内容在政治上是健康的，在法律上是符合国家法律法规的，在道德上是符合中华民族优良的道德规范的。

1995 年，西方七国信息会议上就提出了“数字内容产业（Digital Content Industry）”的概念。在中国,“数字内容产业”的定义为基于数字化、网络化，利用信息资源创意、制作、开发、分销、交易产品和服务的产业。很显然，数字内容产业需要信息内容安全来保障。如果不能确保信息内容的安全，将不能确保数字内容产业的健康发展和壮大。

目前，学术界关于信息内容安全还没有统一的认识。广义的信息内容安全既包括信息内容在政治、法律和道德方面的要求，还包括信息内容的保密、知识产权保护、隐私保护等方面，其主要研究内容包括信息内容安全的威胁、信息内容的获取、信息内容的分析与识别、信息内容的管理和控制、信息隐藏、隐私保护、信息内容安全管理和信息内容安全的法律保障。

5. 信息对抗

随着计算机网络的迅速发展和广泛应用，信息领域的对抗从电子对抗发展到信息对抗。信息对抗就是为削弱、破坏对方电子信息设备和信息的使用效能，保障己方电子信息设备和信息正常发挥效能而采取的综合技术措施，其实质是斗争双方利用电磁波和信息来争夺电磁频谱和信息的有效使用及控制权。

信息对抗研究信息对抗的理论、信息对抗技术和应用，具体内容包括通信对抗、雷达对抗、光电对抗和计算机网络对抗。

1.3　信息安全学科的理论和方法论基础

信息安全学科是交叉融合了计算机、电子、通信、数学、物理、生物、法律、管理及教育等学科发展而来的，其理论基础和方法论基础与这些学科紧密相关，在学科的形成和发展过程中又丰富和发展了这些理论和方法论，从而形成了自己特有的学科理论和方法论。

1.3.1 信息安全学科的理论基础

信息安全学科的理论基础主要涉及数学、计算理论、信息论、控制论和系统论等。

1. 数学

数学是一切自然科学的理论基础，当然也是信息安全学科的理论基础。

1）密码算法的数学理论基础

现代密码算法可以分为两类：基于数学的密码算法和基于非数学的密码算法。

对于基于数学的密码算法，从本质上来讲，一个密码算法就是一个数学函数（设计一个密码算法就是设计一个数学函数），而该密码算法的破解就是求解该数学难题。因此，数学理论是密码学的理论基础是显而易见的。作为密码学理论基础的数学分支主要有代数、数论、概率统计和组合数学等。

基于非数学的密码算法（如量子密码算法和DNA密码算法等）目前还处于发展阶段，尚不能在实际中应用。现已广泛应用的密码算法仍然是基于数学的密码算法。

2）网络协议的数学理论基础

协议是网络的核心，因此协议安全是网络安全的核心，作为协议安全理论基础之一的数学主要有逻辑学等。逻辑学是研究抽象思维的形式结构及其规律的科学，其本质是寻找事物的相对关系，并用已知推断未知。

3）信息安全的基础理论之一——博弈论

信息安全领域的斗争本质上都是攻防双方之间的斗争，因此博弈论便成为信息安全的基础理论之一。

一般来说，人们称具有对抗或竞争性质的行为为博弈行为。在博弈行为中，参加对抗或竞争的各方各自具有不同的目标或利益，并力图选取对自己最有利的或最合理的方案。作为现代数学的一个分支，博弈论（game theory）是研究博弈行为的数学理论与方法，它考虑对抗中的个体的预测行为和实际行为，并研究它们的优化策略。其实，博弈论研究的就是博弈行为中对抗各方是否存在最合理的行为方案，以及如何找到这个合理方案。

博弈论的思想古已有之，我国古代的《孙子兵法》不仅是一部军事著作，而且是最早的一部博弈论专著。目前，博弈论已经在经济、军事、体育和商业等领域中得到了广泛应用。信息安全领域的斗争无一不具有对抗性或竞争性，如网络攻防技术、密码的加密与破译技术、病毒的制毒与杀毒技术、信息隐藏与攻击技术、信息对抗技术等。

由于信息安全领域的斗争，本质上都是人与人之间的对抗性的斗争，因此博弈论便成为信息安全的基础理论之一。博弈论考虑对抗各方的预期行为和实际行为，并研究其优化策略。遵循博弈论的指导原则，会使我们在信息安全的斗争中避免被动，掌握主动，立于不败之地。

2. 计算理论

信息安全学科的许多问题都是计算安全问题，因此计算理论也是信息安全学科的理论基础，其中包括可计算性理论和计算复杂性理论等。

1）可计算性理论

可计算性理论（computability theory）是研究计算的可行性和函数算法的数学理论，又称算法理论。它通过建立计算的数学模型，精确区分哪些是可计算的，哪些是不可计算

的；对于判定问题，可计算性理论研究哪些问题是可判定问题，哪些问题是不可判定问题。它是算法设计与分析的基础，也是计算机科学的理论基础。

可计算性理论的重要课题之一，就是将算法这一直观概念精确化。算法概念精确化的途径很多，其中之一是通过定义抽象计算机，把算法看做抽象计算机的程序。通常把那些存在算法计算其值的函数叫做可计算函数。因此，可计算函数的精确定义为能够在抽象计算机上编出程序计算其值的函数，这样就可以讨论哪些函数是可计算的，哪些函数是不可计算的。

众所周知，授权是信息系统访问控制的核心，若要使信息系统是安全的，首先其授权系统必须安全。可计算性理论告诉我们，一般意义上，对于给定的授权系统是否安全这一问题是不可判定问题，但是一些“受限”的授权系统的安全问题又是可判定问题。由此可知，一般操作系统的安全问题是一个不可判定问题，而具体的操作系统的安全问题却是可判定问题。例如，著名的“停机问题”是不可判断问题，而具体程序的停机问题是可判定的。一般计算机病毒的检测是不可判定问题，而具体软件的计算机病毒检测是可判定问题，这就说明了可计算理论是信息系统安全的理论之一。

2）计算复杂性理论

计算复杂性理论（Computational Complexity Theory）是使用数学方法对计算中所需的各种资源的耗费作定量的分析，并研究各类问题之间在计算复杂程度上的相互关系和基本性质的理论，是算法分析的理论基础。

计算复杂性理论是计算理论在可计算理论之后的又一个重要发展。可计算理论研究区分哪些是可计算的，哪些是不可计算的，但是这里的可计算是理论上的可计算，或原则上的可计算，即研究问题的重心在于不管需要多少资源，问题能否解决。而计算复杂性理论则进一步研究现实的可计算性，如研究计算一个问题类需要的资源，如时间（时间复杂度越小，说明该算法效率越高，则该算法越有价值）和空间（一般来说，空间复杂度越小，算法越好），以及如何尽可能地节省这些资源；研究哪些问题是现实可计算的，哪些问题虽然是理论可计算的，但因计算复杂性太大而实际上是无法计算的。

实际上，破译密码算法就是求解一个数学难题，如果这个难题是理论不可计算的，则这个密码算法就是理论上安全的；如果这个难题虽然是理论可计算的，但是由于计算复杂性太大而实际上不可计算，则这个密码算法就是实际安全的，或计算上安全的。“一次一密”密码算法是理论上安全的密码算法，其余的密码算法都只是计算上安全的密码算法。根据计算复杂性理论的研究，NPC 问题是最难计算的一类问题。公钥密码算法的构造往往基于一个 NPC 问题，以使公钥密码算法在计算上是安全的。例如，McEliece 密码算法基于纠错码的一般译码是一个 NPC 问题；背包密码算法基于求解一般背包问题是 NPC 问题；MQ 密码算法基于多变量二次非线性方程组的求解问题是 NPC 问题等，这些都说明计算复杂性理论是密码学的理论基础之一。

3. 信息论、控制论和系统论

信息论是香农为解决现代通信问题而创立的，控制论是维纳在解决自动控制技术问题中建立的，系统论是为了解决现代化大科学工程项目的组织管理问题而诞生的。起初，信息论、控制论和系统论都是独立的科学理论，但由于它们之间具有紧密的联系，因而在后来的应用和发展中相互作用、相互渗透，出现了趋向综合、统一，形成统一学科的趋势。