

信息安全专业

一、培养目标

培养学生成为适应我国经济建设实际需要，德、智、体全面发展，具有宽厚、扎实的数理基础和电子技术、通信技术、计算机技术基础，掌握信息安全的基本理论、基本知识、基本技能及综合应用方法，具有较强的信息安全系统分析与设计、安全防护、安全策略制订、操作管理、综合集成、工程设计和技术开发能力，了解信息安全的新发展，熟练掌握英语，能够顺利地阅读本专业的英文文献，受到严格的科学思维训练和全面的素质教育的专门人才。

毕业生适宜到科研和教育部门从事科学研究和教学工作，也可以到企事业、技术和管理部门从事应用开发工作，可继续攻读本学科及相关学科的硕士学位。

二、学制、授予学位及毕业基本要求

学制 4 年。实行学分制，学生按专业教学计划修满 160 学分，通过毕业论文答辩，并且符合学校有关本科学位授予规定者，授予工学学士学位。

课程设置的分类及学分比例如下表：

类 别	学 分	比 例
通 修 课	76	47.5%
学科群基础课	34	21.25%
专 业 课	42	26.25%
毕 业 论 文	8	5.00%
合 计	160	

三、修读课程

要求修读的课程分为四个层次，每个层次的课程设置及结构如下：

1、通修课：（76 学分）

参照学校关于通修课的课程要求。其中计算机类课程和电子类课程以本专业要求为准；并要求修读以下物理类课程：

力学与热学（4 学分）、电磁学（4 学分）、光学与原子物理（4 学分）、大学物理-基础实验（1.5 学分）、大学物理-综合实验（1.5 学分）、大学物理-现代技术实验（1.5 学分）；

2、学科群基础课：（34 学分）

MA02*（数学类课程）：（8 学分）

复变函数 (A) (3 学分)、概率论与数理统计 (3 学分)、随机过程 (2 学分);

ES02* (电子类课程): (11.5 学分)

电路基本理论 (3 学分)、电路基本理论实验 (0.5 学分)、线性电子线路(A) (4 学分)、
线性电子线路实验 (0.5 学分)、数字逻辑电路 (3 学分)、数字逻辑电路实验 (0.5 学分);

CS02* (计算机类课程): (12.5 学分)

数据结构及其算法 (4 学分)、微机原理与系统(A) (5 学分)、计算机网络 (3.5 学分);

IN* (信息类课程): (2 学分)

信息论基础 (2 学分);

3、专业课: (43 学分)

专业必修课程: (33.5 学分)

IN* (信息类课程): (7.5 学分)

信号与系统 (4 学分)、操作系统 (3.5 学分);

CS* (计算机类课程): (7 学分)

算法基础 (3.5 学分)、编译原理和技术 (3.5 学分);

MA* (数学类课程): (3 学分)

计算数论 (3 学分);

IS53* (信息安全类课程): (16 学分)

离散数学 I (3 学分)、离散数学 II (3 学分)、信息安全综合设计与实践 (1 学分)、
密码学导论 (3 学分)、计算机安全 (3 学分)、网络安全协议 (3 学分);

专业选修课程: (选 \geq 8.5 学分, 共 37.5 学分)

PI02* (机械类课程): (2 学分)

机械制图(非机类) (2 学分);

CS* (计算机类课程): (14.5 学分)

代数结构 (3 学分)、数据库基础 (2.5 学分)、软件工程 (2.5 学分)、面向对象程序
设计语言 (2.5 学分)、计算机组成原理(3)、计算机组成原理实验(1);

CN* (控制类课程): (2.5 学分)

模式识别导论 (2.5 学分);

IN* (信息类课程): (14.5 学分)

数字信号处理 (3 学分)、现代通信原理 (3.5 学分)、数字图象处理导论 (3 学分)、
无线通信原理及应用 (3 学分)、多媒体技术 (2.5 学分);

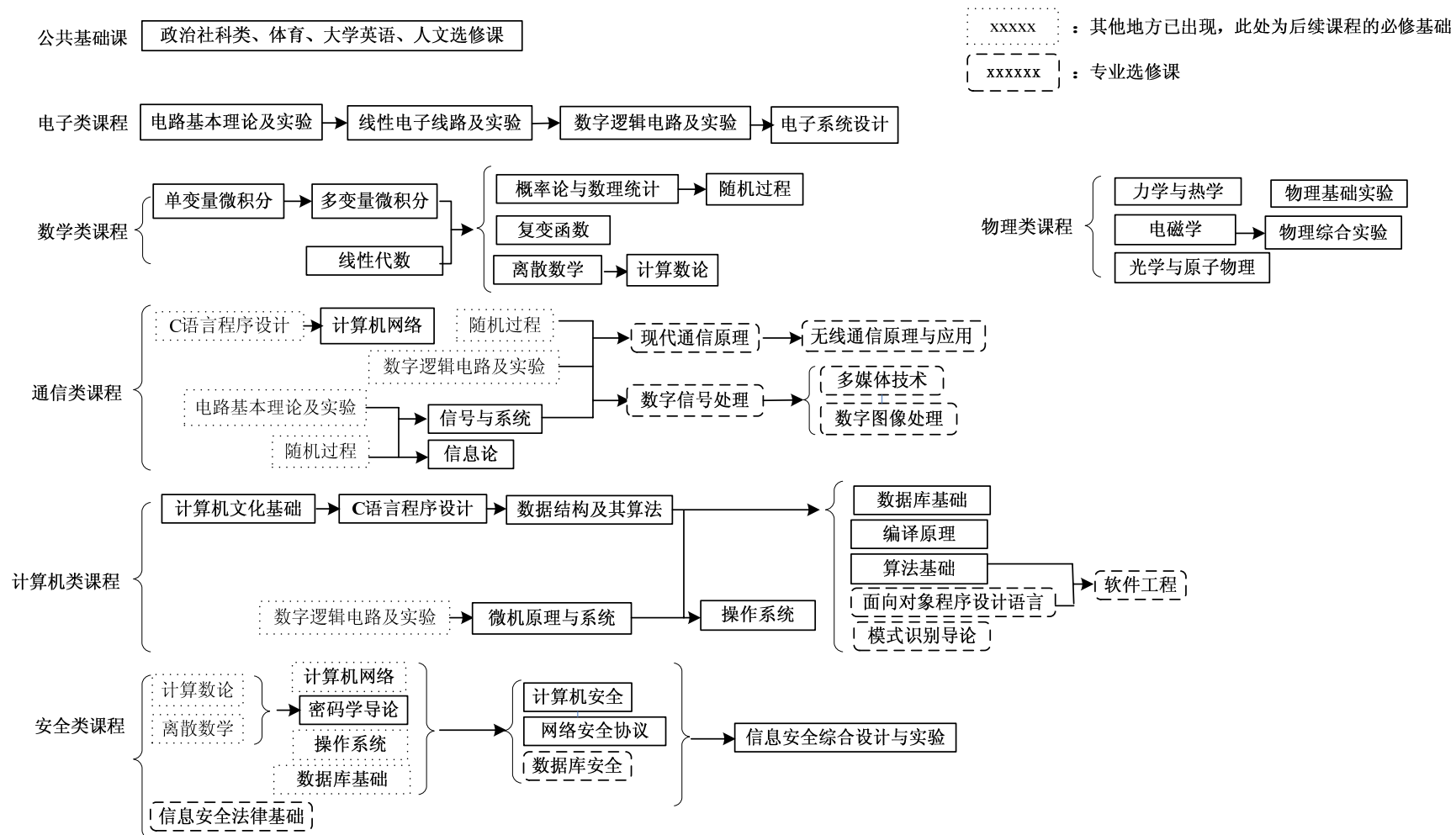
IS531* (信息安全类课程): (4 学分)

信息安全法律基础 (2 学分)、数据库安全 (2 学分);

本专业主干课程: 计算数论、离散数学、算法基础、密码学导论、操作系统、编译原
理和技术、信息安全综合设计与实践、计算机安全、网络安全协议。

四、主要课程关系结构图

信息安全专业主要基础课程和专业课程相互关系结构图



五、指导性学习计划表

信息安全专业四年制指导性学习计划

一 年 级									
秋					春				
新课号	老课号	课程名称	学时	学分	新课号	老课号	课程名称	学时	学分
PS01004	104008	思想道德修养与法律基础	60	3	PS01003	104007	马克思主义基本原理	60	3
PS01002	104006	中国近现代史纲要	40	2	FL01002	018502	综合英语二级	80	4
PS01006	104018	综合英语一级	80	4	PE012**	103B01	基础体育选项	40	1
PS01007	104027	单变量微积分	120	6	PH01001	022153	力学与热学	80	4
FL01001	018501	线性代数	40	4	PH01701	022162	大学物理一基础实验	60	1.5
PE011**	103A01	计算机文化基础	10/20	1	MA01002	001513	多变量微积分	120	6
CS01001	210505	C 语言程序设计	40/30	2.5	ES02001	210045	电路基本理论	60	3
MA01001	001512	基础体育	40	1	ES02701	210046	电路基本理论实验	30	0.5
PS01001	无	形势与政策（讲座）		1	CS33001	210043	代数结构	60	3
PI02004	009004	机械制图（非机类）	40	2			文化素质类课程		8
小 计		(10) 门课		25.5	小 计		(9) 门课		23
二 年 级									
秋					春				
新课号	老课号	课程名称	学时	学分	新课号	老课号	课程名称	学时	学分
MA02505	001505	复变函数（A）	60	3	PH01003	022155	光学与原子物理	80	4
PS01005	104009	重要思想概论	80/80	6	MA02504	017080	概率论与数理统计	60	3
FL01003	018503	综合英语三级	80	4	PE013**	103D01	体育选项（2）	40	1
PH01002	022154	电磁学	80	4	PH01703	022143	大学物理一现代技术实验	60	1.5
PH01702	022142	大学物理一综合实验	60	1.5	ES02003	023003	数字逻辑电路	60	3
PE013**	103C01	体育选项（1）	40	1	ES02703	023004	数字逻辑电路实验	30	0.5

二 年 级									
秋					春				
新课号	老课号	课程名称	学时	学分	新课号	老课号	课程名称	学时	学分
ES02002	210062	线性电子线路(A)	80	4	ES02702	210053	线性电子线路实验	30	0.5
CS02001	011142	数据结构及其算法	60/40	4	MA03015	001120	计算数论	60	3
IS53006	210024	离散数学 I	60	3	IN13001	006105	信号与系统	80	4
IS53101	210005	信息安全法律基础	40	2	IS53007	210025	离散数学 II	60	3
		文化素质类课程			CS33009	011146	算法基础	60/30	3.5
							文化素质类课程		
小 计		(9+2*) 门课		29.5	小 计		(10+2*) 门课		27
三 年 级									
秋					春				
新课号	老课号	课程名称	学时	学分	新课号	老课号	课程名称	学时	学分
MA02510	017084	随机过程	40	2	IN33102	210026	信息论基础	40	2
CS02003	210060	计算机网络	60/20	3.5	IS53003	210002	操作系统	60/20	3.5
CS02002	023215	微机原理与系统 (A)	80/40	5	CS33011	210027	编译原理和技术	60/30	3.5
IS53004	210004	密码学导论	60	3	IN04201	210602	网络安全协议	40	3
CS33102	011095	面向对象程序设计语言	40/30	2.5	IN13005	006170	现代通信原理	60/20	3.5
IN13003	006011	数字信号处理	60	3	IS53106	210028	数据库安全	40	2
CS33007	011013	计算机组成原理	60	3	CS33012	011128	软件工程	40/20	2.5
CS33701	011138	计算机组成原理实验	40	1	IN13101	006183	数字图象处理导论	60	3
CS43001	023229	数据库基础	40/20	2.5					
		文化素质类课程					文化素质类课程		
小 计		(5+5*) 门课		13.5	小 计		(4+5*) 门课		12

六、课程简介

课 号: CS02003

课程名称 (中文): 计算机网络

课程名称 (英文): Computer Networks

学 时: 60/20

学 分: 3.5

开课学期: 春

预修课程: 计算机原理或 CS02002 微机原理与系统、CS01002C 语言程序设计

适用对象和学科方向: 信息科学与技术学院各学科

主要内容: 在 21 世纪的今天, 人类社会进入了全面的信息时代, 网络已经成了信息社会不可或缺的基础设施。本课程是信息科学技术学院各个学科本科生学习和应用计算机网络的重要入门课程。通过本课程的学习, 可以理解、掌握计算机网络的基本原理、技术和主要协议, 能够为进一步学习、研究和应用计算机网络打下坚实的基础。本课程的目标是让学生比较系统地了解与掌握有关计算机网络的基本概念、理论知识和基本应用, 并了解计算机网络的最新发展和最新技术, 以适应信息社会的需求。通过教学和课程实验, 使学生掌握基本网络理论、网络分层结构和协议、TCP/IP 协议基本原理、因特网的各种应用, 学会熟练使用计算机网络, 为今后利用计算机网络资源、从事本学科进一步的学习和研究打下良好基础。

主要讲授: 本课程系统地介绍计算机网络的基本原理和关键技术。首先, 简单介绍计算机网络的基本概念、发展历史、分类等。然后, 重点介绍计算机网络的层次体系结构, 使学生初步了解计算机网络的工作流程。接着, 围绕计算机网络的层次体系结构, 详细介绍各层的主要功能、实现这些功能的关键技术、以及典型协议实例, 依次为物理层、数据链路层、介质访问控制子层、网络层、传输层、应用层和网络安全。在介绍各层基本原理及关键技术时, 结合了因特网、移动通信等近年来迅速发展的网络技术。

具体讲授内容包括: 计算机网络的定义, 计算机网络的应用, 网络参考模型, 数据通信的理论基础, 物理层协议, 数据链路层设计问题, 差错检测和纠正, 基本数据链路协议, 滑动窗口协议, 局域网的多路访问协议, 局域网和 IEEE 802 标准, 网桥规范, 网络层的路由选择算法, 拥塞控制算法, 网络互联, 因特网上的网络层, 传输层协议的要素, 一个简单的传输协议, 因特网传输协议 (TCP 和 UDP), 域名系统, SNMP 简单网络管理协议, 电子邮件, 万维网 (WWW), 网络安全和数据加密等。

课 号: CS43001

课程名称 (中文): 数据库基础

课程名称 (英文): Introduction to Database Systems

学 时: 40/20

学 分: 2.5

开课学期: 秋

预修课程: 计算机原理, CS01002C 语言程序设计, CS02001 数据结构及其算法

适用对象和学科方向: 信息科学与技术学院各学科

主要内容: 本课程介绍数据库的基本原理、数据库技术的特点、数据库系统的组成与结构, 着重阐述当前广泛使用的关系数据库的基本概念、数据语言 SQL, 在此基础上进一步介绍关系数据库的规范化原理和关系数据库系统的设计方法。

主要讲授: 数据库的基本概念 (数据模型, 数据库系统结构, 数据库管理系统), 关系数据库 (关系数据结构, 关系的完整性, 关系代数, 关系演算, 关系数据库管理系统),

关系数据库标准语言 SQL (SQL 概述, 数据定义, 查询, 数据更新, 视图, 数据控制, 嵌入式 SQL), 关系数据库设计理论 (数据依赖, 范式, 关系模式的规范化), 数据库保护 (安全性, 完整性, 并发控制, 恢复, 数据库复制和数据库镜像), 数据库设计 (数据库设计的步骤, 需求分析, 概念结构设计, 逻辑结构设计, 数据库物理设计, 数据库实施, 数据库运行与维护), 数据库管理系统和数据库技术新进展。

课 号: IS53003

课程名称 (中文): 操作系统

课程名称 (英文): Operating System

学 时: 60/20

学 分: 3.5

开课学期: 春

预修课程: 微型计算机原理, CS01002C 语言程序设计, CS02001 数据结构及其算法

适用对象和学科方向: 信息科学与技术学院各学科

主要内容: 介绍现代操作系统的基本概念、系统结构和基本原理; 例如, 多道程序的并发运行, 进程之间的同步与互斥 (包括线程之间的同步与互斥), 假脱机 I/O 技术, 操作系统的特性与性能, 现代主要的操作系统 (如 Unix 和 Windows 2000) 的系统结构。并且系统地阐述操作系统的进程管理、进程之间的同步与通信、作业管理、存储管理、设备管理和文件管理的概念和技术、使用的数据结构和算法; 结合 Unix 和 Windows 2000 操作系统, 系统地介绍现代操作系统引入的新概念和技术。

主要讲授: 操作系统的基本概念, 多道程序的并发运行, 进程/线程调度与管理, 进程之间的同步与互斥, 并能用类 Pascal 或类 C 语言和阻塞等待信号量编程实现几个传统的进程之间的同步与互斥的程序模型, 进程通信, 死锁。进程与线程的管理、调度, 作业管理与调度, 分区存储管理、分页和分段存储管理和虚拟存储管理的技术, 设备驱动程序、I/O 系统及设备管理技术, 文件管理技术, 典型的操作系统 (如 Unix 和 Windows 2000, MS-DOS) 文件系统的结构。

课 号: CS33011

课程名称 (中文): 编译原理和技术

课程名称 (英文): Principles and Techniques of Compilers

学 时: 60/30

学 分: 3.5

开课学期: 春

预修课程: CS02001 数据结构及其算法、汇编语言程序设计、CS01002C 语言程序设计

适用对象和学科方向: 信息科学与技术学院各学科

主要内容: 一、教学目标和基本要求:

本课程介绍编译器构造的一般原理、基本设计方法和主要实现技术。目的是让学生对程序设计语言的设计和实现技术有深刻的理解, 对和程序设计语言有关的理论有所了解, 对宏观上把握程序设计语言来说, 能起一个奠基的作用。

虽然只有少数人从事构造或维护程序设计语言编译器的工作, 但是编译原理和技术对高校学生和计算机工程技术人员来说是重要的基础知识之一。学生通过本课程的学习还有助于快速理解、定位和解决在程序调试与运行中出现的问题。对软件工程来说, 编译器是一个很好的实例 (基本设计、模块划分、基于事件驱动的编程等), 本课程所介绍的概念和技术能应用到一般的软件设计之中。

二、主要讲授：

本课程介绍编译器构造的一般原理、基本设计方法和主要实现技术，其内容包括词法分析、语法分析、语义分析、类型检查、运行时存储空间的组织和管理、中间代码生成、代码优化、目标代码生成、编译系统和运行系统等。

在介绍语言实现技术的同时，强调一些相关的理论知识，如形式语言和自动机理论、语法制导的定义和属性文法、类型论和类型系统等。它们是计算机专业理论知识的一个重要部分，在本课程中结合应用来介绍这些知识，有助于学生较快领会和掌握。

在介绍编译器各逻辑阶段的实现时，强调形式化描述技术，并以语法制导定义作为翻译的主要描述工具。

本课程强调对编译原理和技术的宏观理解及全局把握，而不把读者的注意力分散到一些枝节的算法上，如计算开始符号集和后继符号集的算法、回填技术等。出于同样的目的，本课程较详细地介绍了编译系统和运行系统。

本课程还介绍面向对象语言和函数式语言的实现技术，可加深学生对语言实现技术的理解。这两部分加上带星号的章节，作为教学的可选部分。

本课程鼓励读者用所学的知识去分析和解决实际问题，因此本课程的很多习题是从实际碰到的问题中抽象出来的。这些习题也能激发学生学习编译原理和技术的积极性。

课 号：CS33102

课程名称（中文）：面向对象程序设计语言

课程名称（英文）：Object-oriented Programming Language

学 时：40/30

学 分：2.5

开课学期：秋

预修课程：CS01002C 语言程序设计、CS02001 数据结构及其算法

适用对象和学科方向：信息安全等相关学科

主要内容：20 世纪 80 年代，特别是 90 年代以来，软件的规模进一步扩大，对软件可靠性和代码可重用性的要求也进一步提高。在这样的背景下，面向对象的程序设计方法应运而生。和传统的程序设计方法相比，面向对象的程序设计具有抽象、封装、继承和多态性等特征。“面向对象”不仅仅作为一种技术，更作为一种方法论贯穿于软件设计的各个阶段。面向对象的技术在系统程序设计、数据库及多媒体开发等领域都得到广泛应用。目前，面向对象的程序设计思想已经主导了程序设计语言的发展。

主要讲授：对象的概念（抽象的过程、具有界面的对象、隐藏实现、重用实现、继承和重用界面、多态、创建和撤销对象、异常处理、分析和设计、极限编程、迁移的策略）、创建和使用对象（语言翻译的过程、分离编译的工具、Iostreams、Strings、读和写文件、向量）、数据抽象（基本对象、抽象数据类型、对象的细节、头文件、内嵌的结构）、隐藏实现（设置极限、存取控制、友元、类、处理类）、内联函数（预处理器的缺陷、内联函数、内联函数和编译器、预处理器的特点、改进的错误检查）、命名控制（静态成员、名字空间、静态初始化的依赖因素、转换连接指定）、引用和拷贝构造函数（指针、引用、拷贝构造函数、指向成员的指针）、运算符重载（警告和确信、语法、可重载的运算符、非成员运算符、重载赋值符、自动类型转换）、动态对象创建（对象创建、重新设计前面的例子、用于数组的 new 和 delete、用完内存、重载 new 和 delete）、继承和组合（组合语法、继承语法、构造函数的初始化表达式表、组合和继承的联合组合和继承的选择、保护、多重继承、渐增式开发向上映射）、多态和虚函数（向上映射、问题、虚函数、晚捆绑、为什么需要虚函数、抽象基类和纯虚函数、继承和 VTABLE、虚函数和构造函数、析

构函数和虚拟析构函数)、模板和容器类(容器和循环子、模板综述、模板的语法、Stash & stack 模板、字符串和整型、向量、模板和继承、多态性和容器、容器类型、函数模板、控制实例)、多重继承(概述、子对象重叠、向上映射的二义性、虚基类、开销、向上映射、避免 MI、修复接口)、异常处理(抛出异常、异常捕获、清除、构造函数、异常匹配、标准异常、含有异常的程序设计、开销)、运行时类型识别(什么是 RTTI、语法细节、引用、多重继承、合理使用 RTTI、RTTI 的机制及花费、创建自己的 RTTI、新的映射语法)。

课 号: IN13001

课程名称(中文): 信号与系统

课程名称(英文): Signal and System

学 时: 80

学 分: 4

开课学期: 春

预修课程: 多变量微积分, 线性电子线路

适用对象和学科方向: 信息安全等相关学科

主要内容: 信号与系统是电子工程、计算机、自动化、信息安全等专业的一门重要的基础课。通过本课程的学习, 使学生能够掌握信号与系统的基本理论, 能够采用时域和变换域的方法来解决信号处理和通信中的信号系统问题, 为学习后续课程打下重要的基础。

信号与系统主要内容包括连续与离散时间的信号与系统两部分内容, 信号主要包括时域以及变换域描述; 系统的分析和处理是本课程的核心问题, 主要包括线性时不变系统和用差分方程和微分方程描述的两大类系统。按照知识点来分, 本课程包含的内容有: 卷积运算, 差分方程和微分方程的求解, 零输入响应和零状态响应的求解, 系统的直接 I 型和直接 II 型实现结构, 连续时间和离散时间傅立叶变换, 傅立叶级数, 双边拉普拉斯变换, 双边 Z 变换, 变换的性质及其在信号与系统处理中的应用, 单边拉普拉斯变换, 单边 Z 变换, 最小相位系统, 全通系统, 系统的并联和级联实现结构, 相位均衡, 滤波和滤波器的设计, 调制和解调等。

课 号: IN13005

课程名称(中文): 现代通信原理

课程名称(英文): Principles of Modern Communication

学 时: 60/20

学 分: 3.5

开课学期: 春

预修课程: 概率论与随机过程、IN13001 信号与系统

适用对象和学科方向: 信息安全等相关学科

主要内容: 通信系统组成、分类及主要性能指标; 信道容量和信道噪声; 信源编码; 数字基带传输; 数字带通调制/解调; 信道编码; 多路复用和多址接入; 同步原理; 数字通信系统设计分析和新技术介绍。

主要讲授: 数字通信基本概念和通信系统框图; 信号与噪声、信道模型和信道容量(Shannon 公式); 通信系统主要性能指标; 信源编码(PCM、 ΔM 、DPCM、VQ); 无码间串扰(ISI)基带传输、高斯噪声干扰下二进制信号检测、相关编码(部分响应信号)、时域均衡; 二进制和多进制带通调制/解调(ASK, FSK, PSK/DPSK, QPSK, DQPSK, QAM, MSK)和差错性能分析; 高效带通调制; 信道编码(线性分组码、卷积码)、调制和编码权衡; 载波同步、

码元同步、帧同步；通信资源共享和分配、多路复用和多址接入(FDM/FDMA、TDM/TDMA)；多载波调制(MCM)；通信系统设计分析。

课 号：CN23108

课程名称（中文）：模式识别导论

课程名称（英文）：Introduction to Pattern Recognition

学 时：40/20

学 分：2.5

开课学期：秋

预修课程：MA02504 概率论与数理统计（B）、MA01003 线性代数

适用学科方向：信息安全等相关学科

主要内容：本课程是我校自动化专业选修课之一。该课程是一个导论性质的课，只介绍一些模式识别中最基本的内容，通过该课程的学习，使得学生了解模式识别的基本概念，基本方法和算法原理，为将来研究和利用模式识别奠定一个良好的基础。

主要讲授：模式识别的发展概况和应用前景。2. 几何分类法（判别函数、线性判别函数、线性判别函数的性质、线性分类器的设计、广义线性判别函数、非线性判别函数、非线性形分类器的设计）。3. 概率分类法（最小错误率判决规则、最小风险判决规则、最大似然比判决规则、Neyman-Pearson 判决规则、最小最大判决规则、分类器设计、正态分布时的统计决策、参数估计与非参数估计）。4. 聚类方法（相似性准则、聚类准则函数、两种简单的聚类算法、系统聚类、分解聚类、动态聚类、最小张树聚类）。5. 句法模式识别（形式语言理论基础、自动机理论、基元提取、句法分析）。

课 号：IS53006

课程名称（中文）：离散数学 I

课程名称（英文）：Discrete Mathematics I

学 时：60

学 分：3

开课学期：秋

预修课程：高等代数或线性代数、数学分析或微积分

适用对象和学科方向：信息安全等相关学科

主要内容：离散数学是现代数学的一个重要分支，课程充分描述了计算机科学离散性的特点，是计算机科学的数学基础，是计算机专业的专业基础课程。本课程的目的是使学生掌握计算机科学技术所必需的数学知识，结合离散数学在计算机科学中的应用，掌握处理离散量的基本数学方法，培养和提高学生的抽象思维能力和逻辑推理能力，为学习专业课奠定良好的数学基础。本课程主要讲授以下三方面内容：（1）数理逻辑：命题与命题公式、范式、命题推理理论、命题公理系统，个体谓词与量词、谓词公式、谓词推理理论、谓词公理系统；（2）集合论：集合、集合的运算性质，关系、关系性质、关系的运算、等价关系、序关系，映射（函数）及性质与运算；（3）代数结构：代数结构，同态、同构、同余，半群、独异点与群、子群及其性质，环、域与格及其性质，布尔代数。

课程编号：IS53007

课程名称（中文）：离散数学 II

英文名称（英文）：Discrete Mathematics (2)

学 时：60

学 分：3

开课学期：秋

预修课程：离散数学 I

适用对象和学科方向：信息安全等相关学科

主要内容：本课程讲述图论与算法图论的基本概念、理论、算法及其应用，主要内容包括：(1) 各种类型的图(包括图、树、平面图、Euler 图、Hamilton 图、有向图)的基本概念与性质；(2) 图论的基本理论(包括匹配理论、着色理论、连通度、图矩阵)与算法(包括 Dijkstra 算法、树相关算法、最大流算法等)。

课程编号：MA03015

课程名称(中文)：计算数论

英文名称(英文)：Computational Number Theory

学 时：60

学 分：3

开课学期：春

预修课程：

适用对象和学科方向：信息安全等相关学科

主要内容：计算数论是研究数论中计算方法的一门学科，其中两个最核心的问题是大整数的素性检验和因子分解。现代快速计算机的出现促进了计算数论的发展，只有利用先进的计算机，很多算法才可能实现。而且计算数论与现代密码学有着密切的关系。

本课程包括下面三部分内容：1. 初等数论，主要讲授数论的基础知识，包括整除理论、同余理论、椭圆曲线等。2. 计算/算法数论，主要讲授数论中几个重要问题的计算机算法，包括素数判定、因式分解和离散对数。3. 数论在计算机和密码学中的应用。

课 号：CS33009

课程名称(中文)：算法基础

课程名称(引文)：Introduction to Algorithm

学 时：60/30

学 分：3.5

开课学期：春

预修课程：离散数学、C 语言程序设计、数据结构

适用对象和学科方向：信息安全等相关学科

主要内容：本课程以介绍计算机算法的分析和设计技术为核心，系统地介绍了基本的算法分析技术、高级数据结构和常见的算法设计策略。课程主要内容包括算法分析基础、排序问题、高级数据结构、动态规划、贪心算法、回溯法、分支限界法、随机化算法等。此外，课程还将对算法研究中的一些经典问题(如矩阵运算、数论算法、字符串匹配等)进行专题讲解，分析相关的经典算法，以加深学生对算法设计和分析技术的理解与掌握。最后，课程还将安排一系列实验，结合实际例子提高学生分析问题和解决问题的能力。

课 号：IS53004

课程名称(中文)：密码学导论

课程名称(英文)：Introduction to Contemporary Cryptography

学 时：60

学 分：3

开课学期：秋

预修课程：MA02004 初等数论、CS53001 离散数学

适用对象和学科方向：信息安全等相关学科

主要内容：课程主要介绍现代密码学的基本理论、概念与方法，介绍现代密码学的从简单到复杂的各种协议、算法和理论证明，以及在计算机和网络安全中的具体应用。课程详细讨论基本数据加密原理和数论基础，各种密码技术及实现，密钥管理与分发、身份认证、数字签名、数据完整性保护、鉴别技术及应用、Internet 网络安全等。同时介绍密码学在数据安全和信息安全中的实际应用。

主要讲授：传统加密技术、分组密码与数据加密标准、有限域理论、高级加密标准、对称密码及应用、数论入门、公钥密码学与 RSA、密钥管理和其他公钥密码体制、消息认证和 Hash 函数、Hash 算法、数字签名和认证协议、认证的实际应用等。

课 号：IN04201

课程名称（中文）：网络安全协议

课程名称（英文）：Network Security Protocols

学 时：40

学 分：2

开课学期：秋

预修课程：CS02003 计算机网络

适用对象和学科方向：信息安全等相关学科

主要内容：介绍计算机网络安全的基本知识和基本理论，网络安全提供的服务和各种安全技术，系统地介绍网络层、传输层及应用层的各种安全协议，其中包括 IPSec、SSL/TLS 和 PGP、SSH 等，介绍公钥基础设施（PKI）和虚拟专网（VPN）技术。

主要讲授：网络安全概述、公钥基础设施 PKI、安全电子交易协议 SET、网络层安全中的 AH 和 ESP、因特网密钥交换协议 IKE、SSL、TLS、应用层安全协议中的 Email 安全协议、远程登陆安全协议 SSH、web 安全协议 S-HTTP、防火墙、VPN 技术等。

课 号：IN04202

课程名称（中文）：计算机安全

课程名称（英文）：Computer Security

学 时：60

学 分：3

开课学期：秋

预修课程：计算机原理、计算机网络、操作系统、数据库基础、编译原理

适用对象和学科方向：信息安全等相关学科

主要内容：在计算机网络信息时代，计算机及其系统的安全已成为目前计算机科学中的一个研究热点，也直接关系到一个单位、国防和国家的信息安全。计算机安全旨在培养学生的计算机及其系统安全的基本知识和安全机制和基本原理、计算机安全模型、软件安全技术、操作系统的安全技术、数据库系统的安全技术和可信系统的评测标准。

主要讲授：计算机安全系统地介绍信息系统安全的层次结构，计算机系统安全的基础知识和基本原理、安全模型、用户鉴别与授权、访问控制等技术；软件安全；操作系统安全，安全内核的基本概念，可信操作系统设计；Unix 和 Windows 操作系统的安全机制和系统结构、攻防技术；web 网站及浏览器安全；数据库安全；安全评估及评测标准。

课 号：IN04201

课程名称（中文）：信息安全综合设计与实践

课程名称（英文）：Experiments of Information Security

学 时：20/60

学 分：3

开课学期：秋

预修课程：CS02003 计算机网络, CS53002 操作系统, 编译原理

适用对象和学科方向：信息安全等相关学科

主要内容：课程主要介绍信息安全实践中常用技术与相关原理，涉及网络安全、系统安全、软件安全以及 WEB 安全等方面。系统、全面地介绍了端口扫描、漏洞扫描、防火墙、NAT、IPSec、入侵检测、网络嗅探、计算机病毒、安全编程、缓冲区溢出、程序静态分析、软件测试、sql 注入等。对以上各种安全技术给出了详实的理论讲解和实例分析，并配合大量实际操作验证实验。

主要讲授与实验：常用 linux 和 dos 命令；端口扫描技原理与实践；DoS 攻击；Ddos 攻击与防范；防火墙原理及其基本配置；入侵检测原理与 Snort 使用；古典密码学实验；PGP 的原理与使用；程序调试基础；安全编程；缓冲区溢出基础；高级缓冲区溢出技巧与防范；shellcode 及 exploit 编写方法；文件格式与 crack 原理；windows 系统安全；linux 系统安全；web 安全；程序分析原理与实践；软件测试；病毒蠕虫。

课 号：IS53101

课程名称（中文）：信息安全法律基础

课程名称（英文）：Introduction to Information Security Law

学 时：40

学 分：2

开课学期：秋

预修课程：计算机文化基础

适用对象和学科方向：信息安全等相关学科

主要内容：随着计算机和网络技术的发展，信息安全问题得到社会各界的广泛关注。从维护国家安全和社会稳定，保障计算机与网络安全，维护社会主义市场经济秩序，保护公民、法人和其他组织的合法权益的角度出发，有必要对有关信息安全法的相关问题进行探讨，对学生强调信息法的概念。本课程的主要内容包括：信息法基础、信息公开法、个人信息保护法、信息安全法、计算机信息网络法、信息犯罪及其追诉程序等，并将对电子政务、电子商务、网络知识产权和远程教育等热点领域的相关法律问题展开专题讨论。