**840网络空间安全专业综合专业课考研大纲**

**一、考试组成**

网络空间安全专业综合共包括两门课的内容：数据结构与C语言程序设计、密码学与网络安全，分别为150分。学生任选其中一门课的考试内容。

**二、数据结构与C语言程序设计部分的考试大纲（150分）**

**（一）整体要求**

1．理解数据的逻辑结构与存储结构的基本概念；

2．理解数据结构算法的定义、基本原理和性质，理解算法分析的基本概念，包括采用大O形式表示时间复杂度和空间复杂度；

3．理解C语言的特点以及C语言程序的组成；

4．理解C语言主要的数据类型，包括整型、实型、字符型等常量与变量和变量的赋值；用typedef定义类型；

5．理解C语言各种类型数据之间的混合运算；

6．理解C语言算术表达式、关系表达式和逻辑表达式，表达式sizeof的含义。

**（二）知识要点**

1.线性表

（1）线性关系、线性表的定义，线性表的基本操作；

（2）线性表的顺序存储结构与链式存储结构(包括单(向)链表、循环链表和双向链表)的构造原理；

（3）在以上两种存储结构的基础上对线性表实施的基本操作，包括顺序表的插入与删除、链表的建立、插入与删除、查找等操作对应的算法设计(含递归算法的设计)。

2．堆栈与队列

（1）堆栈与队列的基本概念与基本操作；

（2）堆栈与队列的顺序存储结构与链式存储结构的构造原理；

（3）在不同存储结构的基础上对堆栈与队列实施插入与删除等基本操作的算法设计；

（4）堆栈和队列在解决实际问题中应用。

3．树与二叉树

（1）树与二叉树的基本概念，基本特征、名词术语；

（2）完全二叉树与满二叉树的基本概念，二叉树的基本性质及其应用；

（3）二叉树的顺序存储结构与二叉链表存储结的基本原理；

（4）二叉树的前序遍历、中序遍历、后序遍历和按层次遍历，重点是二叉树在以二叉链表作为存储结构基础上各种遍历算法(包括非递归算法)的设计与应用；

（5）二叉排序树的基本概念、建立(插入)、查找以及平均查找长度ASL的计算。

4．内排序

（1）排序的基本概念，各种内排序方法的基本原理和特点，包括排序过程中进行的元素之间的比较次数，排序总趟数、排序稳定性以及时间复杂度与空间复杂度计算；

（2）插入排序法(含折半插入排序法)；

（3）选择排序法；

（4）(起)泡排序法；

（5）谢尔(Shell)排序法；

（6）快速排序法；

（7）堆积(Heap)排序法，包括堆积的定义与构造；

5．C语言基本语句

（1）赋值语句（含条件赋值语句）、条件语句（含if、if-else、switch）、循环语句（含while、do-while、for语句，包括循环嵌套和break语句与continue语句）；

（2）输入/输出语句，包括整型、实型、字符型（含字符串）等类型数据的格式输入函数scanf和格式输出函数printf。

6．C语言数组

（1）一维数组和二维数组的定义、引用与初始化；

（2）字符数组的定义、引用与初始化，字符数组的输入与输出，字符串和字符串处理函数的应用。

7．C语言函数

（1）函数的定义，函数参数（形参和实参）与函数的返回值；

（2）函数的调用，包括函数的嵌套调用和函数的递归调用；

（3）命令行参数的基本概念，带参数的主函数的概念和应用。

8．C语言指针

（1）指针的基本概念，包括定义、使用、指针变量作为函数参数和函数返回值以及函数指针；

（2）数组与指针，包括指向数组的指针变量的定义与赋值、通过指针引用数组元素、数组名作为函数参数；

（3）字符串与指针，指向字符串的指针变量。

9．预处理指令

（1）预处理指令的基本概念，文件包含和条件包含预处理指令;

（2）宏替换，带参数的宏。

10．结构体与共用体

（1）结构体的基本概念和特点，结构体变量的初始化与引用，结构体指针的使用；

（2）结构体数组，包括结构体数组的定义、初始化及应用；

（3）共用体的基本概念，共用体变量的引用。

11．文件

（1）文件的基本概念，包括文件类型指针FILE与文件的使用方式；

（2）文件的打开函数fopen与关闭函数fclose；

（3）文件的状态，包括feof函数和ferror函数；

（4）文件的读/写，包括fread和fwrite函数、fputc和fgetc函数、fgets与fputs函数的应用；

（5）文件的输入函数fscanf和输出函数fprintf的应用。

**（三）可参考书目**

1．《数据结构教程》（第3版）唐发根编著北京航空航天大学出版社2017

2．《C程序设计》谭浩强编著清华大学出版社(版次不限)

**二、密码学与网络安全部分的考试大纲（150分）**

**（一）整体要求**

1.理解信息安全的基本目标；

2.理解信息系统中常见的威胁；

3.理解安全攻击的分类及区别；

4.理解OSI的七层参考模型和Internet四层参考模型；

5.理解常用密码体制，密码算法和密码协议的工作原理；

6.理解X.800标准中的安全服务和安全机制及相互关系；

7.理解网络安全参考模型和网络访问参考模型。

**（二）知识要点**

1．TCP/IP协议族的安全性

（1）IPv4地址格式、MAC地址的概念；

（2）IPv4地址的分类及CIDR表示方法；

（3）IPv6地址的格式及表示方法；

（4）HTTP、FTP、TELNET、POP3、SMTP、SSH、DNS、DHCP等协议的功能、使用的端口及安全性；

（5）网络地址转换（NAT）的作用及安全性；

（6）UDP协议及TCP协议的优缺点。

2．单钥密码体制

（1）密码体制的分类；

（2）DES、AES的工作原理；

（3）流密码的工作原理；

（4）分组密码的5种工作模式及优缺点。

3．双钥密码体制

（1）双钥密码体制的基本概念；

（2）RSA公钥加密算法的工作原理；

（3）ElGamal公钥加密算法的工作原理。

4．消息认证与杂凑函数

（1）杂凑函数的概念及性质；

（2）消息论证码（MAC）、消息检测码（MDC）的概念及区别；

（3）杂凑算法（MD5，SHA-1）的基本知识；

（4）杂凑函数应用的基本方式。

5．数字签名

（1）数字签名算法的基本概念；

（2）RSA数字签名算法的基本原理；

（3）ElGamal数字签名算法的基本原理。

6．密码协议

（1）协议所具有的三个要素；

（2）密码协议的功能及分类；

（3）Diffie-Hellman协议的工作原理及中间人攻击过程描述。

7．数字证书与公钥基础设施

（1）PKI的定义、系统组成及应用；

（2）数字证书的概念、结构、生产及验证；

（3）X.509v3证书的格式。

8．网络加密与密钥管理

（1）四种网络加密的原理、特点及逻辑图；

（2）密钥管理的基本概念；

（3）密钥生成、分配与存储方法。

9．无线网络安全

（1）无线网络面临哪些安全威胁；

（2）GSM/CDMA系统的认证过程及主要安全缺陷；

（2）WCDMA蜂窝系统的认证过程及安全性改进。

**（三）可参考书目**

《网络安全——技术与实践》（第3版），刘建伟，王育民编编，清华大学出版社。