# 网络空间安全2024年硕士研究生
# 入学考试专业课考研大纲

## 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，一共为 150 分。

## 二、数据结构与 C 语言程序设计部分的考试大纲

### （一）整体要求

1. 数据的逻辑结构与存储结构的基本概念;

2. 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. C 语言的特点以及 C 语言程序的组成;

4. 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；理解原码、反码和补码；用 typedef 定义类型;

5. C 语言各种类型数据之间的混合运算;

6. 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. 数据结构概述

（1）数据的逻辑结构与存储结构的基本概念;

（2）算法的定义、基本性质以及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。

2. 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（包括线性链表、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）。

3. 数组

（1）一维数组和二维数组的存储;

（2）矩阵的压缩存储的基本概念;

（3）对称矩阵、对角矩阵的压缩存储;

（4）稀疏矩阵的三元组表表示。

4. 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。

5. 树与二叉树

（1）树与二叉树的基本概念、基本特征和名词术语;

（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。

6. 图

（1）图的基本概念、名词术语;

（2）图的邻接矩阵存储方法和邻接表（含逆邻接表）存储方法的构造原理及特点;

（3）图的深度优先搜索与广度优先搜索;

（4）最小（代价）生成树、最短路径、AOV 网与拓扑排序的基本概念。

7. 文件及查找

（1）顺序查找法以及平均查找长度（ASL）的计算;

（2）折半查找法以及平均查找长度（ASL）的计算，包括查找过程对应的

“判定树”的构造;

（3）杂凑表的构造、杂凑函数的构造，杂凑碰撞的基本概念、处理杂凑碰撞的基本方法以及杂凑表的查找和平均查找长度的计算。

8. 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）泡排序法;

（5）谢尔排序法;

（6）快速排序法;

（7）堆积排序法。

9. C 程序的基本结构

（1）C 语言的特点;

（2）C 程序的基本组成。

10. C 语言常量、变量和表达式

（1）常量：数字常量、字符常量和字符串字面量;

（2）变量：变量名和变量类型，变量的赋值和类型转换;

（3）算术表达式：算术运算符、增量（自增）和减量（自减）运算符、位运算和复合赋值运算符;

（4）强制类型转换;

（5）数据输入/输出函数;

（6）常量的符号表示方法：常量宏、枚举常量。

11. C 语言条件语句和开关语句

（1）关系运算符和逻辑运算符;

（2）运算符的优先级;

（3）逻辑表达式;

（4）条件语句：条件、复合语句、条件语句的嵌套和级联、条件运算符和

条件表达式;

（5）switch 语句。

12. C 语言循环语句和 goto 语句

（1）while 语句、for 语句和 do while 语句;

（2）循环语句的选择和使用;

（3）逗号表达式;

（4）循环语句的嵌套;

（5）循环中的非常规控制（break 和 continue）、goto 语句。

13. C 语言函数

（1）函数的基本概念;

（2）函数的调用、结构和定义;

（3）函数的调用关系和返回值;

（4）局部变量和全局变量;

（5）函数参数的传递;

（6）标准库函数;

（7）递归函数;

14. C 语言数组

（1）一维数组：定义和初始化、复制、数组参数;

（2）字符串和字符数组;

（3）标准字符串函数;

（4）二维数组：定义、引用、访问、数组参数。

15. C 语言指针

（1）地址与指针;

（2）指针变量：定义和赋值、访问、参数和返回值;

（3）指针运算：指针与整数的加减、指针相减和比较、强制类型转换和 void* 指针、不合法的指针运算、指针类型与数组类型的差异;

（4）指针与数组;

（5）指向二维数组的指针、多重指针和指针数组;

（6）函数指针;

16. C 语言结构和联合

（1）结构：结构类型的定义和访问、包含结构的结构；

（2）联合：联合类型的定义和访问；

（3）类型定义语句（typedef）。

17. 输入/输出和文件

（1）输入/输出的基本过程和文件类型；

（2）文件的打开、创建和关闭；

（3）文件数据的正文（文本）格式读写；

（4）读写操作中的定位；

（5）文件数据的二进制格式读写。

**（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 程序设计导引》，尹宝林，机械工业出版社，版次不限

## 三、密码学与网络安全部分的考试大纲

**（一）整体要求**

（1）密码学所涉及的数学基础；

（2）常见信息安全系统所基于的工作原理；

（3）常用密码体制、密码算法和密码协议的工作原理；

（4）信息安全的基本目标；

（5）信息系统中常见的威胁；

（6）安全攻击的分类及区别；

（7）OSI 的七层参考模型和 Internet 四层参考模型；

（8）X.800 标准中的安全服务和安全机制及相互关系；

（9）网络安全参考模型和网络访问参考模型。

**（二）知识要点**

1. 数论基础

（1）整除性和带余除法；

（2）欧几里得算法，扩展欧几里得算法；

（3）模运算；

（4）素数，素性测试；

（5）欧拉定理，费马小定理；

（6）中国剩余定理；

（7）离散对数。

2. 有限域

（1）群的概念及性质；

（2）环的概念及性质；

（3）域的概念及性质；

（4）有限域的概念及性质；

（5）有限域 GF(p)和 $GF(2^n)$

（6）多项式运算。

3. 单钥密码体制

（1）密码体制的定义；

（2）对称密码基本概念，分组密码常见结构；

（3）DES/AES/SM4 的工作原理；

（4）流密码的基本概念，RC4、祖冲之算法；

（5）分组密码的工作模式及特点；

（6）伪随机数发生器和伪随机函数。

4. 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）椭圆曲线密码系统；

（5）SM2 算法。

5. 消息认证与杂凑函数

（1）杂凑函数的概念、性质及基本结构；

（2）常用杂凑函数（MD5、SHA-1、SHA-3、SM3 等）的基本知识；

（3）杂凑函数应用的基本方式；

（4）消息认证码（MAC），消息检测码（MDC）；

（5）HMAC;

（6）使用杂凑函数和 MAC 的伪随机数生成器。

6. 数字签名

（1）数字签名算法基本概念;

（2）RSA 数字签名算法;

（3）ElGamal 数字签名算法;

（4）Schnorr 数字签名算法;

（5）DSS 数字签名标准;

（6）椭圆曲线数字签名算法;

（7）SM2 签名算法;

（8）门限签名算法。

7. 密码协议

（1）协议的基本概念;

（2）密码协议分类及基本密码协议;

（3）Diffie-Hellman 协议;

（4）Kerberos 协议;

（5）秘密分拆协议;

（6）密码协议的安全性分析。

8. 数字证书与公钥基础设施

（1）PKI 的定义、组成及应用;

（2）数字证书的概念、结构、生成、签名及验证;

（3）交叉证书;

（4）X.509 证书。

9. 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。

10. 网络加密与密钥管理

（1）四种网络加密模式的原理、特点；

（2）密钥管理的基本概念；

（3）层次化密钥管理方法；

（4）密钥分发协议。

11. 无线网络安全

（1）无线网络面临哪些安全威胁；

（2）GSM/CDMA /3G 系统的认证过程及主要安全缺陷；

（3）WCDMA 蜂窝系统的认证过程及安全性改进。

12. 防火墙

（1）防火墙的类型和结构；

（2）静态包过滤器；

（3）动态包过滤器；

（4）电路级网关；

（5）应用级网关。

13. 入侵检测技术

（1）入侵检测概述；

（2）入侵检测原理及主要方法；

（3）IDS 的结构与分类；

（4）NIDS/HIDS/DIDS 原理及部署。

14. VPN

（1）VPN 的基本概念；

（2）VPN 的分类；

（3）VPN 的部署。

**（三）可参考书目**

1.《网络安全——技术与实践》（第 3 版），刘建伟，王育民编，清华大学出版社，2017。

2.《密码编码学与网络安全——原理与实践（第七版）》, William Stallings 著，王后珍等译，电子工业出版社，2017。