

# 953 网络空间安全基础综合 考试大纲

(研招考试主要考察考生分析问题与解决问题的能力,大纲所列内容为考生需掌握的基本内容,仅供复习参考使用,考试范围不限于此)

## 一、总体要求

《953 网络空间安全基础综合》要求考生比较系统地掌握网络空间安全相关基础课程的基本概念、基本原理和基本方法,能够综合运用所学的基本原理和基本方法分析、判断和解决有关理论问题和实际问题。

## 二、知识要点

### 数据结构:

#### (一) 数据结构基本概念

1. 数据结构的概念、名词和术语
2. 数据结构的逻辑结构
3. 数据结构的物理结构

#### (二) 线性表

1. 线性表的概念和基本运算
2. 线性表的顺序存储表示及算法
3. 顺序表的基本运算
4. 单链表、循环链表、双向链表的基本运算,
5. 线性表的链式存储表示及算法
6. 顺序表及链表的应用

#### (三) 栈和队列

1. 栈和队列的基本概念和基本操作
2. 栈和队列的顺序存储结构
3. 栈和队列的链式存储结构
4. 栈和队列的应用

#### (四) 串和数组

1. 串的基本概念和基本操作
2. 串的存储结构

- 3.模式匹配算法
- 4.数组的概念
- 5.数组的存储结构
- 6.矩阵压缩存储

### **(五) 树**

- 1.数、二叉树、森林的基本概念
- 2.二叉树的性质和存储表示。
- 3.二叉树的遍历及递归算法的运用
- 4.树和森林的转换方法
- 5.二叉树的应用

### **(六) 图**

- 1.图的基本概念、术语
- 2.图的存储方法
- 3.图的遍历
- 4.生成树和最小生成树
- 5.最短路径
- 6.拓扑排序
- 7.关键路径

### **(七) 索引结构与散列技术**

- 1.索引结构的表示
- 2.索引结构的应用
- 3.散列表的概念
- 4.散列表的构造
- 5.散列表的查找

### **(八) 缩小规模算法**

- 1.递归与分治算法
- 2.动态规划算法
- 3.掌握贪心算法

## 计算机网络:

### (一) 计算机网络体系结构

#### 1. 计算机网络概述

- (1) 计算机网络的概念、组成与功能
- (2) 计算机网络的分类
- (3) 计算机网络与互联网的发展历史
- (4) 计算机网络的标准化工作及相关组织

#### 2. 计算机网络体系结构与参考模型

- (1) 计算机网络分层结构
- (2) 计算机网络协议、接口、服务等概念
- (3) ISO/OSI 参考模型和 TCP/IP 模型

### (二) 物理层

#### 1. 通信基础

- (1) 信道、信号、宽带、码元、波特、速率、信道容量等基本概念
- (2) 奈奎斯特定理与香农定理
- (3) 编码与调制、多路复用与扩频
- (4) 电路交换、报文交换与分组交换
- (5) 数据报与虚电路

#### 2. 传输介质

- (1) 双绞线、同轴电缆、光纤与无线传输介质
- (2) 物理层接口的特性

#### 3. 物理层设备

- (1) 中继器
- (2) 集线器

### (三) 数据链路层

#### 1. 数据链路层的功能

#### 2. 组帧

#### 3. 差错控制

- (1) 检错编码

(2) 纠错编码

#### 4. 流量控制与可靠传输机制

(1) 流量控制、可靠传输与滑窗窗口机制

(2) 停止-等待协议

(3) 后退 N 帧协议

(4) 选择重传协议

#### 5. 典型数据链路层协议

(1) HDLC 协议

(2) PPP 协议

(3) ADSL 协议

#### 6. 介质访问控制

(1) 信道划分介质访问控制

频分多路复用、时分多路复用、码分多路复用的概念和基本原理。

(2) 随即访问介质访问控制

ALOHA 协议；CSMA 协议；CSMA/CD 协议；CSMA/CA 协议；码分多址访问方法。

#### 7. 局域网

(1) 局域网的基本概念与体系结构

(2) 以太网与 IEEE 802.3

(3) 无线局域网 IEEE 802.11

(4) 其他类型的局域网（令牌环网、双总线）

(5) 局域网的互联原理与技术、虚拟局域网 VLAN

(6) 局域网互联设备的工作原理与配置方法

(7) 网桥、二层交换机、三层交换机

#### 8. 广域网

(1) 广域网的基本概念

(2) 帧中继

(3) ATM

(4) 同步光纤网络 SONET/SDH

#### 9. 数据链路层设备

- (1) 网桥的概念和基本原理
- (2) 局域网交换机及其工作原理

#### **(四) 网络层**

##### **1. 网络层的功能**

- (1) 异构网络互联
- (2) 路由与转发
- (3) 拥塞控制

##### **2. 路由算法**

- (1) 静态路由与动态路由
- (2) 距离-向量路由算法
- (3) 链路状态路由算法
- (4) 层次路由

##### **3. IPv4**

- (1) IPv4 分组
- (2) IPv4 地址与 NAT
- (3) 子网划分与子网掩码、CIDR
- (4) ARP 协议、DHCP 协议与 ICMP 协议

##### **4. IPv6**

- (1) IPv6 的主要特点
- (2) IPv6 地址

##### **5. 路由协议**

- (1) 自治系统
- (2) 域内路由与域间路由
- (3) RIP 路由协议
- (4) OSPF 路由协议
- (5) BGP 路由协议

##### **6. IP 组播**

- (1) 组播的概念
- (2) IP 组播地址

## **7. 移动 IP**

- (1) 移动 IP 的概念

## **8. 网络层设备**

- (1) 路由器的组成和功能
- (2) 路由表与路由转发

## **(五) 传输层**

### **1. 传输层提供的服务**

- (1) 传输层的功能
- (2) 传输层寻址与端口
- (3) 无连接服务与面向连接服务

### **2. UDP 协议**

- (1) UDP 数据报
- (2) UDP 校验

### **3. TCP 协议**

- (1) TCP 段
- (2) TCP 连接管理
- (3) TCP 可靠传输
- (4) TCP 流量控制与拥塞控制

## **(六) 应用层**

### **1. 网络应用模型**

- (1) 客户/服务器模型
- (2) 浏览器/服务器模型

### **2. DNS 系统**

- (1) 层次域名空间
- (2) 域名解析过程

### **3. 电子邮件与文件传输**

- (1) FTP 协议的工作原理
- (2) IMAP、SMTP 与 POP3 协议基本概念

### **4. 万维网 WWW**

(1) WWW 的概念与组成结构

(2) HTTP 协议

## 5. 简单网络管理

(1) 简单网络管理协议 SNMP

## 密码学:

### (一) 密码学基础

1. 密码学的基本概念: 明文、密文、加密密钥、解密密钥、加密算法、解密算法

2. 密码体制分类: 对称密码体制、非对称密码体制

3. 古典密码: 凯撒密码、维吉尼亚密码等古典密码的原理、攻击和实现

### (二) 对称密码体制

1. 信息论安全的基本概念和一次一密

2. 流密码算法的定义和模型, 伪随机序列发生器的基本设计原理

3. 分组密码的基本原理及发展现状

4. Feistel 结构和 DES 算法

5. AES 算法

6. 分组密码的工作模式: CBC、CTR、CFB、OFB

### (三) 公钥密码体制

1. 单向函数和陷门单向函数的概念, 数学困难问题: 大整数分解困难问题、离散对数困难问题和椭圆曲线离散对数困难问题

2. 公钥密码算法的设计原理

3. Diffie-Hellman 密钥协商协议与中间人攻击

4. RSA 加密算法

5. Rabin、ElGamal 密码体制

6. 椭圆曲线 ElGamal 密码体制

### (四) 哈希函数与消息认证码

1. 哈希函数的定义、原理和使用方式

2. MD5 算法、SHA 系列算法

3. 消息认证码的定义和使用方式

4. HMAC 算法、CBC-MAC 算法

## **(五) 数字签名**

1.数字签名的基本概念与原理

2.RSA 签名体制、ElGamal 签名体制、Schnorr 签名体制、DSA 签名体制等

## **(六) 安全协议**

1.密钥分发与用户认证协议：基于对称加密的密钥分发，基于非对称的加密的对称密钥分发、Kerberos、X.509 和 PKI

2.传输层安全：SSL、TLS

3.IP 安全：IPsec、IKE 协议

## **三、考试形式和试卷结构**

### **1.考试时间**

180 分钟。

### **2.试卷分值**

150 分，其中数据结构 55 分、计算机网络 55 分、密码学 40 分。

### **3.考试方式**

闭卷考试。