《网络空间安全综合基础》考试大纲及推荐书目

一、考试要求

《网络空间安全综合基础》专业课涵盖《密码学》、《程序设计基础（C)》两部分内容。

1. 了解《密码学》和《程序设计基础（C)》的基础理论和基本概念
2. 掌握《密码学》和《程序设计基础（C)》的重点算法
3. 熟练运用《密码学》和《程序设计基础（C)》的重点算法解决具体问题。

二、考试题型

满分 150 分，题型有简答题、综合分析题。

三、考试大纲内容

第一部分：《密码学》课程

第一章　绪论

1．密码体制及其分类；

第二章　古典密码体制及其破译

1．代替密码；

2．移位密码。

第三章　序列密码与移位寄存器

1．序列密码概念及其密钥序列的简单要求；

2．线性反馈移位寄存器、m-序列及其特性；

3．线性反馈移位寄存器的代数理论与本原多项式；

4．线性反馈移位寄存器的综合；

5．对偶移位寄存器概念；

6．典型密钥序列发生器——非线性组合。

第四章　分组密码

1．分组密码概论；

2．数据加密标准（DES）；

3．高级加密标准（AES）；

4．SM4 国家商用密码算法；

5. 分组密码的应用模式介绍。

第五章　公钥密钥密码

1．公钥密码的基本思想与典型应用（数字信封与数字签名）；

2．基于大整数分解的 RSA 体制及其安全性要求；

3．基于离散对数的 ElGamal 体制及其安全性要求；

4．椭圆曲线密码（ECC）体制；

5.　SM2、SM9 国家商用密码算法

第六章　其它现代密码技术

1．密码杂凑函数，MD5、SHA-1、SHA-3、国密 SM3 等密码杂凑函数；

2．数字签名的一般原理、实现方法及其安全性要点，ElGamal、DSS 等数字签名方案；

3．密钥的层次设置及各环节安全控制方法，Diffe-Hellman 密钥交换协议，Shamir、Simmons 等秘密共享门限方案；

第二部分：《程序设计基础（C）》课程

第一章 程序设计和 C 语言

1.什么是计算机程序

2.什么是计算机语言

3.C 语言的发展及特点

4.C 语言的程序结构

5.运行 C 语言的步骤与方法

第二章 C 语言数据类型和表达式

1.什么是算法

2.算法的特性

3.怎样表示一个算法。

掌握以下算法表示方法：

（1）用自然语言表示算法

（2）用流程图表示算法

（3）用 N-S 流程图表示算法

（4）用伪代码表示算法

（5）用计算机语言表示算法

第三章 C 语言数据类型和表达式

1. 熟悉 C 语言的数据类型，掌握常量和变量的表示方法。
2. 掌握变量的赋值方法。
3. 熟悉 C 语言的各种运算符。
4. 掌握 C 语言的算数表达式、赋值表达式、关系表达式、逻辑表达式。
5. 掌握混合运算的优先级和结合性，能正确计算混合表达式的结果。
6. 能根据要求将数学表达式、自然语言描述的功能翻译成 C 语言的表达式。

第四章 简单的 C 程序设计——顺序结构

1. 熟悉 C 语句的特点，掌握赋值语句的使用。
2. 掌握格式输入函数 scanf 与格式输出 printf 函数的使用方法。
3. 掌握字符输入函数 getchar 与格式输出 putchar 函数的使用方法。

第五章 分支结构

1. 掌握 if 语句的三种表达形式。
2. 掌握 if 语句的嵌套用法。
3. 熟悉条件表达式的用法。
4. 掌握 switch-case 语句的特点和用法。
5. 能阅读分支结构为主体的 C 程序并分析其功能，能跟踪变量值的变化并得出输出结果。
6. 会综合使用分支语句编程解决典型的实际应用问题。

第六章 循环结构

1. 掌握 for 语句的使用方法。
2. 掌握 while 语句的使用方法。
3. 掌握 do-while 语句的使用方法。
4. 循环的嵌套。
5. 能阅读循环结构为主体的 C 程序并分析其功能，能跟踪变量值的变化并得出输出结果。
6. 会综合使用循环语句编程解决实际应用问题。

第七章 数组

1. 掌握一维、二维数组的定义、初始化和引用方法。
2. 掌握字符数组的定义、初始化和引用方法。
3. 能阅读与数组类型数据相关的 C 程序并分析其功能，能跟踪变量值的变化并得出输出结果。
4. 会使用数组有关的编程技巧解决典型的实际应用问题。

第八章 函数

1. 熟悉函数定义的一般形式，熟悉函数的参数和函数的值类型。

2. 熟悉函数的形式参数和实际参数的用法。

3. 掌握函数的各种调用方法，能跟踪函数参数的传递过程。

4. 掌握局部变量和全局变量的使用方法。

5. 熟悉和掌握变量的存储类型。

6. 能阅读与函数定义和调用有关的 C 程序并分析其功能，能跟踪函数值、变量值的变化并得出输出结果。

7. 根据要求定义函数和调用函数，解决实际应用问题。

第九章 指针

1. 熟悉指针的基本概念，掌握指针变量的定义、引用方法。

2. 掌握数组指针和指向数组的指针变量定义和引用方法。

3. 掌握字符串指针和指向字符串的指针变量定义、引用方法。

4. 能阅读与指针类型数据有关的 C 程序并分析其功能。

四、推荐书目

1. 李子臣：《密码学-基础理论与应用》，电子工业出版社，2019 年。

2. 谭浩强：《C 程序设计（第四版）》，清华大学出版社，2020 年。