

科目：《信息安全综合》， 适用专业：信息安全（0812Z1）

中国地质大学（武汉）计算机学院

2021 年硕士研究生复试

《信息安全综合》考试大纲

（包括两部分）

适用专业：信息安全 0812Z1

A、《密码学》

一、考试要求：

- 1) 理解并掌握密码学的基本概念和常见密码算法的基本原理；
- 2) 理解并掌握分组密码、公钥密码、流密码的基本思想和方法；
- 3) 理解并掌握 Hash 函数、数字签名、身份识别、认证理论的基本概念和特点；

二、考试内容：

1. 分组密码

分组密码原理和设计原则、Feistel 框架、DES 算法、AES 算法、多重 DES 及其安全性、分组密码工作模式

2. 公钥密码

公钥密码的数学基础、RSA 公钥密码体制、ElGamal 公钥密码体制、Diffie-Hellman 密钥交换协议

3. 流密码

流密码基本原理、伪随机数发生器、线性反馈移位寄存器

4. Hash 函数

单向函数的基本概念，散列函数的设计与构造，MD5、SHA 算法基本结构

5. 数字签名

数字签名的基本概念，RSA 签名方案，ElGamal 签名方案

6. 身份识别

身份识别基本概念，强弱身份识别，身份识别协议及其安全性

7. 认证理论与密码协议

认证的理论和技术，身份认证方案及协议，盲签名协议，Kerberos 系统

8. 密码分析

现代密码算法的安全性分析、中间相遇统计、生日攻击

9. 密钥管理与应用

密钥管理中的安全问题，密钥协商、秘密共享、密钥分发和托管

三、参考书目

《现代密码学》（第 4 版），杨波，2017，清华大学出版社，ISBN：9787302465553.

B、《信息安全基础》

一、考试要求：

- 1) 理解并掌握网络安全相关基本概念、原理和方法；
- 2) 掌握访问控制、网络安全攻击与防御技术相关基本概念、理论和技术；
- 3) 能够运用相关知识分析计算机系统与网络中存在的各类信息安全问题；
- 4) 能够针对各类网络安全问题设计和提供综合解决方案。

二、考试内容：

1. 网络与信息安全基础

网络与信息安全概念和技术，网络安全特征，网络安全模型，网络访问安全模型，常见网络威胁原理和方法

2. 防火墙与入侵检测技术

防火墙种类和功能，包过滤防火墙与状态检测型防火墙的差异、网络地址转换技术，网络设备隔离技术，入侵检测功能和技术，防火墙和入侵检测系统的部署、功能及其特点

3. 网络安全攻击与防御技术

常见网络扫描技术，电子邮件、DNS 系统、WEB 系统等中的常见网络攻击及其防御手段；常见网络威胁（如 DDOS、僵尸网络、病毒、蠕虫等）原理及其防护方法；常见恶意软件（如

间谍软件、网络钓鱼软件、后门及木马) 的原理及防御方法

4. 网络安全协议及其应用

常见网络安全协议的基本概念，接入控制和访问控制原理，NAT 基本原理和作用，传输模式与隧道模式，网络身份鉴别方法，SSL 协议，IPSec 协议，握手协议、会话重用，相关密钥的派生方法

5. 应用层安全和无线安全

PGP 的基本功能、安全服务、SET 协议的基本概念、双重数字签名、WLAN 的基本概念，WEP 安全服务、增强方案等

三、参考书目

《密码编码学与网络安全：原理与实践(第 7 版)》，William Stallings, 2017, 电子工业出版社，ISBN: 9787121329210。