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

2023年硕士研究生复试考试大纲

（包括两部分）

A、《密码学基础》

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和应用；

2）理解并掌握杂凑函数、数字签名、数字证书、密钥管理的基本概念和特点；

二、考试内容：

1. 分组密码

分组密码原理和设计原则、DES和AES算法、多重DES及其安全性、分组密码工作模式及其优缺点

2. 公钥密码

公钥密码的数学基础、RSA公钥密码体制、EIGamal公钥密码体制、DH密钥交换协议

3. 流密码

流密码工作原理、伪随机数发生器和伪随机函数

4. 消息认证和杂凑函数

杂凑函数的概念及性质，散列函数的设计与构造方法，MD5和SHA-1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，EIGamal签名方案

6. 密码协议

密码协议的功能与分类，强弱身份识别，Diffie-Hellman协议的工作原理及中间人攻击

7. 数字证书与公钥基础设施

PKI的定义、系统组成与应用，数字证书的概念和管理

8. 密钥管理与应用

密钥管理中的基本概念，密钥协商、密钥分发和托管方法

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。

B、《网络安全基础》

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并提供解决方案。

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

防火墙类型和功能，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. 网路安全协议及其应用

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

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、WEP 安全服务、安全增强方案等

三、参考书目

《网络安全——技术与实践》第 3 版 ，刘建伟、王育民 著，清华大学出版社，2017，ISBN: 9787302467588。