科目：863，《信息安全》，　适用专业：信息安全 （0812Z1）

中国地质大学（武汉）计算机学院

2021年硕士研究生入学考试

《信息安全》考试大纲

（包括两部分）

A、《密码学》

一、考试要求：

1）掌握密码学的基本概念和常见密码算法的加解密原理；

2）掌握分组密、公钥密码、流密码的基本思想和主要特点；

3）掌握单向函数、数字签名、身份识别、认证理论的基本概念和特点；

4）能够利用密码学理论和技术分析和解决应用问题。

二、考试内容：

1. 概述

密码学的发展历史、密码体制分类、密码体制的攻击分类

2. 古典密码

常见古典密码的概念、加解密算法及其分析方法、一次一密体制

3. 分组密码

分组密码原理和设计原则、代替置换网络、DES数据加密标准、AES高级数据加密标准、多重DES及其安全性、分组密码工作模式

4. 公钥密码

公钥密码的数学基础、RSA公钥密码体制、EIGamal公钥密码体制和椭圆曲线公钥密码体制、Diffie-Hellman密钥交换协议、主要安全性分析和攻击方法

5. 流密码

流密码基本原理、密钥流生成器结构、线性反馈移位寄存器

6. 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

7. 数字签名

数字签名的基本概念，RSA 签名方案、EIGamal 签名方案、掌握数字签名标准 DSS

8. 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

9. 认证理论与技术

认证的理论与技术，认证模型和认证协议，Kerberos 系统和 X.509 认证服务

10. 密钥管理

密钥管理基本概念与管理模式、密钥种类、密钥传送、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.
《密码学引论（第三版）》，张焕国，唐明，2015，武汉大学出版社，ISBN：9787307167360。

B、《信息安全基础》

一、考试要求：

1）掌握信息安全学科相关基本概念、原理和方法；

2）掌握密码学算法、访问控制、安全协议、网络安全攻击技术、网络安全防御技术相关基本概念、基础理论和基本技术；

3）能够运用相关知识分析计算机与网络系统中存在的各类信息安全问题；

4）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，TCP/IP 协议及其安全隐患，常见网络威胁与防御技术，常见网络侦查、扫描工具及其使用方法

2. 防火墙与入侵检测技术

防火墙原理与技术，网络地址转换技术，网络设备隔离技术，入侵检测原理与技术，防火墙和入侵检测系统的实际部署、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方法；常见网络威胁（如 DDOS、僵尸网络、病毒、蠕虫、垃圾邮件等）原理及其防护方法；常见恶意软件（如间谍软件、广告软件、网络钓鱼软件、后门及木马）的原理及防御方法；安全编码与缓冲区溢出基本原理及防御方法；蜜罐技术及其基本原理

4. 安全协议及其应用

安全协议的基本概念，接入控制和访问控制原理，网络身份鉴别方法，PGP、S/MIME 及电子邮件安全，SSH 协议及其应用，SSL 协议及 WEB 安全，IPSec 协议、Kerberos 和 X.509 协议的实践应用

5. 系统安全原理和技术

计算机系统物理安全，系统可靠性技术，访问控制技术，多级安全与安全策略模型，多边安全技术，UNIX 和 Windows 系统访问控制技术

6. 信息安全管理与安全评估

安全工程与安全管理基本理论与方法，安全机制与综合防御方案，快速响应、灾难备份与恢复技术，信息安全评估方法，主要信息安全标准、法律和法规

三、参考书目

《信息安全导论》，翟健宏，2018，科学出版社，ISBN：9787030317544。

《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。