湖北大学硕士研究生入学考试《数据结构》参考书目

（科目代码：811）

参考书目

《数据结构教程》，李春葆，清华大学出版社，第 5 版

湖北大学硕士研究生入学考试《应用密码学》考试大纲

（科目代码：834）

第一部分　考试说明

一、考试性质

应用密码学是为全国硕士研究生入学考试网络空间安全各专业设置的课程，评价标准是高等学校优秀本科毕业生能达到及格及以上水平。

二、考试范围

密码学概述、古典密码技术、分组密码、公钥密码、散列（哈希）函数与消息鉴别、数字签名技术、序列密码、密钥管理技术等。

三、考试形式与试卷结构

(一)　答卷方式：闭卷、笔试。

(二)　答题时间：180分钟。

(三)　题型比例：

选择题约20%、填空题约 10%、计算题约40%、综合题约30%

第二部分　考查要点

一、密码学概述

1.　密码的基本概念

二、古典密码技术

1.　替代密码（单表替代、同音替代、多元替代、多表替代等）

2.　置换密码

三、分组密码

1. 分组密码的设计原理

2. 分组密码设计的常见结构

3. 数据加密标准DES

4. 高级加密标准AES

5. 中国商密标准SM4

6. 分组密码的工作模式

四、公钥密码体制

1. 公钥密码体制的基本概念

2. RSA公钥密码体制

3. ElGamal公钥密码体制

4. 椭圆曲线公钥密码体制

五、散列函数与消息鉴别

1. 散列（哈希）函数的概念、性质和安全性需求

2. 生日悖论

3. 散列函数的常见设计结构

六、数字签名技术

1. 数字签名的基本概念

2. 基于RSA的数字签名技术

七、密钥管理技术

1. 密钥协商的基本概念和方法

2. 数字证书的概念以及使用方法

八、序列密码

1. 序列密码的基本概念

2. 线性反馈移位寄存器的概念和原理。

参考书目：

杨波，《现代密码学（第5版）》，清华大学出版社，2022年第五版。

任德斌，胡勇，方勇.《应用密码学（第2 版）》，清华大学出版社，2014 年11月第二版。

李子臣，《密码学-基础理论与应用》，中国工信出版集团，2019年9月第一版。