【初试】2026年 湖北大学834应用密码学考研精品资料

说明：本套资料由高分研究生潜心整理编写，高清电子版支持打印，考研推荐资料。

一、考研大纲

1.**湖北大学834应用密码学考研大纲**

①2025年湖北大学834应用密码学考研大纲。

说明：考研大纲给出了考试范围及考试内容，是考研出题的重要依据，同时也是分清重难点进行针对性复习的推荐资料，本项为免费提供。

二、2026年湖北大学834应用密码学考研资料

2.**湖北大学834应用密码学考研核心题库(含答案)**

①湖北大学834应用密码学之应用密码学考研核心题库综合简答题精编。

说明：本题库涵盖了该考研科目常考题型及重点题型，根据历年考研大纲要求，结合考研真题进行的分类汇编并给出了详细答案，针对性强，是考研复习推荐资料。

三、电子版资料全国统一零售价

本套考研资料包含以上部分(不含教材)，全国统一零售价：[￥]

四、2026年研究生入学考试指定/推荐参考书目(资料不包括教材)

湖北大学834应用密码学考研初试参考书

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.

五、本套考研资料适用学院及考试题型

网络空间安全学院

选择题，填空题，计算题，综合题

六、本专业一对一辅导(资料不包含，需另付费)

提供本专业高分学长一对一辅导及答疑服务，需另付费，具体辅导内容计划、课时、辅导方式、收费标准等详情请咨询机构或商家。

七、本专业报录数据分析报告(资料不包含，需另付费)

提供本专业近年报考录取数据及调剂分析报告，需另付费，报录数据包括：

①报录数据-本专业招生计划、院校分数线、录取情况分析及详细录取名单；

②调剂去向-报考本专业未被录取的考生调剂去向院校及详细名单。

编写组依法对本书享有专有著作权，同时我们尊重知识产权，对本电子书部分内容参考和引用的市面上已出版或发行图书及来自互联网等资料的文字、图片、表格数据等资料，均要求注明作者和来源。但由于各种原因，如资料引用时未能联系上作者或者无法确认内容来源等，因而有部分未注明作者或来源，在此对原作者或权利人表示感谢。若使用过程中对本书有任何异议请直接联系我们，我们会在第一时间与您沟通处理。

因编撰此电子书属于首次，加之作者水平和时间所限，书中错漏之处在所难免，恳切希望广大考生读者批评指正。

目录

湖北大学 834 应用密码学考研大纲

2025 年湖北大学 834 应用密码学考研大纲

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。