【初试】2026年 西安邮电大学830密码学基础考研精品资料

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、西安邮电大学830密码学基础考研大纲

1．**西安邮电大学830密码学基础考研大纲**

①2025年西安邮电大学830密码学基础考研大纲。

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年西安邮电大学830密码学基础考研资料

2．**《新编密码学》考研相关资料**

(1)《新编密码学》[笔记+提纲]

①西安邮电大学830密码学基础之《新编密码学》考研复习笔记。

说明：本书重点复习笔记，条理清晰，重难点突出，提高复习效率，基础强化阶段推荐资料。

②西安邮电大学830密码学基础之《新编密码学》复习提纲。

说明：该科目复习重难点提纲，提炼出重难点，有的放矢，提高复习针对性。

(2)《新编密码学》考研核心题库(含答案)

①西安邮电大学830密码学基础考研核心题库精编。

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。

(3)《新编密码学》考研题库[仿真+强化+冲刺]

①2026年西安邮电大学830密码学基础考研专业课五套仿真模拟题。

说明：严格按照本科目最新专业课真题题型和难度出题，共五套全仿真模拟试题含答案解析。

②2026年西安邮电大学830密码学基础考研强化五套模拟题及详细答案解析。

说明：专业课强化检测使用。共五套强化模拟题，均含有详细答案解析，考研强化复习推荐。

③2026年西安邮电大学830密码学基础考研冲刺五套模拟题及详细答案解析。

说明：专业课冲刺检测使用。共五套冲刺预测试题，均有详细答案解析，最后冲刺推荐资料。

三、电子版资料全国统一零售价

本套考研资料包含以上一、二部分(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)

西安邮电大学830密码学基础考研初试参考书

范九伦，张雪锋，侯红霞，《新编密码学》，第一版，西安电子科技大学出版社。

五、本套考研资料适用学院

网络空间安全学院

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。

版权声明

目录

西安邮电大学 830 密码学基础考研大纲

2025 年西安邮电大学 830 密码学基础考研大纲

西安邮电大学硕士研究生招生考试大纲
科目代码：830
科目名称：《密码学基础》
一、 课程性质和任务
本课程是信息安全专业的一门核心专业基础课，它在整个专业培养的知识结 构中占据重要的地位。通过该课程的学习，学生将熟练掌握常见密码技术的基本 原理，为将来从事信息安全研究和安全系统的设计提供必要的基础知识。
二、 课程内容和要求
第一章绪论
1. 1 了解密码学的发展历程
1. 2 掌握保密通信的基本模型
1. 3 掌握密码学的基本概念
第二章基础知识
2. 1 熟练掌握密码学所需数论基础知识
2. 2 理解密码学常用的计算复杂性问题
第三章古典密码
3. 1 掌握常见古典密码算法的加解密原理
3. 2 掌握针对古典密码算法的密码分析技术
3. 3 了解衡量密码体制安全性的基本准则
第四章分组密码
4. 1 理解分组密码的设计准则
4. 2 熟练掌握 DES 算法的加解密原理和密钥生成方法
4. 3 熟练掌握 AES 算法的加解密原理和密钥生成方法
4. 4 熟练掌握 IDEA 算法的加解密原理和密钥生成方法
4. 5 了解 RC5 算法的加解密原理和密钥生成方法
4. 6 掌握分组密码的常用工作模式
第五章序列密码
5. 1 掌握序列密码的基本原理
5. 2 掌握反馈移位寄存器的构造原理
5. 3 掌握常见密钥流生成器的构造方式
5. 4 了解序列密码常见的攻击方法
5. 5 理解 RC4 算法和 A5 算法的加解密原理
第六章 Hash 函数
6. 1 掌握密码学 Hash 函数的概念
6. 2 了解迭代 Hash 函数的通用构造方法
6. 3 熟练掌握 MD5 算法的构造原理
6. 4 熟练掌握 SHA-1 算法的构造原理
6. 5 了解常见消息认证码的构造方法
6. 6 理解 HMAC 算法的构造原理
第七章公钥密码
7. L 理解公钥密码体制的基本思想

7. 2 掌握构造公钥密码算法应满足的基本要求
7. 3 熟练掌握 RSA 算法的加解密原理
7. 4 理解针对 RSA 算法常见的攻击方法原理及相应的防范方法
7. 5 掌握 RSA 算法的参数选择应满足的基本要求
7. 6 熟练掌握 ElGamal 算法的加解密原理
7. 7 理解 ElGamal 算法的安全性分析
7. 8 熟练掌握有限域上椭圆曲线的定义与性质
7. 9 了解有椭圆曲线密码体制的特性
7. 10 理解基于身份公钥密码体制的思想
7. 11 理解 Boneh 和 Franklin 的 IBE 密码体制
7. 12 了解公钥密码体制的基本应用

第八章数字签名与身份认证

8. 1 熟练掌握数字签名的基本原理
8. 2 熟练掌握 RSA 数字签名算法
8. 3 熟练掌握 ElGamal 数字签名算法
8. 4 熟练掌握 DSS 数字签名标准
8. 5 了解特殊数字签名的构造原理和应用场景
8. 6 掌握常用身份认证协议的构造方法

第九章密钥管理

9. 1 了解密钥管理的重要性
9. 2 掌握单钥体制的密钥管理方法
9. 3 掌握公钥体制的密钥管理方法
9. 4 熟练掌握 Shamir 秘密共享方案

第十章现代密码学发展前沿及应用

10. 1 了解相关前沿密码技术的发展现状
10. 2 了解相关前沿密码技术的应用现状

三、参考书目

范九伦，张雪锋，侯红霞，《新编密码学》，第一版，西安电子科技大学出 版社。

2026 年西安邮电大学 830 密码学基础考研核心笔记

《新编密码学》考研核心笔记

第 1 章　绪论

考研提纲及考试要求

考点：密码学的基本概念
考点：保密通信的基本模型

考研核心笔记

全球信息化的飞速发展，特别是计算机技术与通信技术相结合而诞生的计算机互联网的发展和广泛应用.打破了传统的时间和空间的限制，极大地改变了人们的工作方式和生活方式，促进了经济和社会的发展，提高了人们的工作水平和生活质量。

在信息化日益普及的今天，伴随着信息技术的广泛应用，信息资源不仅成为人们日常工作、学习、生活中的基础资源，而且日益成为国家和社会发展的重要战略资源。国际上围绕信息的获取、使用和控制的竞争愈演愈烈，信息安全已成为维护国家安全和社会稳定的一个焦点，各国都给予极大的关注和投入。

目前信息安全已成为亟待解决、影响国家大局和长远利益的重大关键问题之一，它不但是发挥信息革命带来的高效率、高效益的有力保证，而且是抵御信息侵略的重要屏障。信息安全保障能力是 21 世纪综合国力、经济竞争实力和生存能力的重要组成部分，是世界各国都在奋力攀登的制高点。从大的方面来说，信息安全问题已威胁到国家的政治、经济和国防等领域；从小的方面来说，信息安全问题已威胁到个人的隐私等。因此，信息安全已成为社会稳定与安全的必要前提条件。

信息安全不仅要保证信息的保密性、完整性，也就是关注信息自身的安全，防止偶然的或未授权者对信息的恶意泄露、修改和破坏，从而导致信息的泄密或被非法使用等问题，而且还要保证信息的可用性、可控性，保证人们对信息资源的有效使用和管理。

密码技术是信息安全的核心技术，它的发展有着悠久而神秘的历史。当前，掌握核心密码技术是关系到国家信息安全战略成败的关键之一。为了对密码技术的发展和基本概念有一个概要认识，本章将简要介绍密码技术的发展历程，并给出密码技术涉及的相关基本概念和模型。

【核心笔记】概述

密码学有着悠久而神秘的历史，人们很难对密码学的起始时间给出准确的定义。一般认为人类对密码学的研究与应用已经有几千年的历史，它最早应用在军事和外交领域，随着科技的发展而逐渐进入人们的生活中。密码学研究的是密码编码和破译的技术与方法，其中通过研究密码变化的客观规律，并将其应用于编制密码，实现保密通信的技术被称为编码学；通过研究密码变化的客观规律，并将其应用于破译密码，实现获取通信信息的技术被称为破译学。编码学和破译学统称为密码学。David Kahn 在他的被称为“密码学圣经”的著作《Kahnon Codes：Secrets of the New Cryptology》中这样定义密码学：“Cryptology，the science of communication secrecy"。

密码学研究的是，对通信双方要传输的信息进行何种保密变换，才能防止未被授权的第三方对信息的窃取。此外，密码技术还可以被用来进行信息鉴别、数据完整性检验、数字签名等。密码学作为保护信息的手段，其发展主要经历了三个阶段。

1.第一阶段，从古代到 1949 年。