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。