

陕西科技大学大学 2014 年硕士研究生入学考试

专业课 944 密码学 考试大纲:

适用招生专业: 先进控制算法与应用

一、考试内容

1. 密码学基本知识

密码学的基本概念, 保密通信系统模型, 密码体制的基本概念, 密码体制的攻击类型, 密码编码学和密码分析学的概念, 密码体制的分类。

2. 古典密码体制

什么是代换密码, 代换密码的分类, 会使用 Kaiser 密码、Vigenere 密码、Playfair 密码、Hill 密码和置换密码进行加密和解密。

3. 分组密码基本原理

分组密码的概念, 分组密码的构造原则, 什么是混乱和扩散, 掌握 feistel 密码结构, DES 加密算法过程, IDEA 密码算法描述, AES 加密算法原理, 加密轮变换, RC5 加密算法, TEA 密码。

4. 流密码

流密码的保密通信原理, 同步流密码和自同步流密码的概念和特点, 有限状态机, 反馈移位寄存器、线性反馈移位寄存器、非线性反馈移位寄存器。

5. 公钥密码体制

公钥密码体制的加密和认证模型, 公钥密码体制的基本原理和要求, RSA 的加密和解密算法和安全性, ELGamal 的加密和解密算法和安全性, 背包公钥密码、Diffie-Hellman 密钥协商方案和安全性。

6. 密钥管理

密钥管理的主要内容, 密钥的种类, 密钥管理的架构模式, 密钥建立协议的基本方法, 公开密钥分发主要有哪几种, shamir 密钥协议, 密钥托管的概念, 密钥托管加解密系统原理。

7.Hash 函数

什么是 Hash 函数，Hash 函数的安全性，强抗碰撞性，弱抗碰撞性，MD5 和 SHA 算法的过程，两种算法的异同，什么是消息认证码。

8.数字签名

数字签名的定义、特征和分类，数字签名体制，RSA 和 ELGamal 数字签名方案，数字签名标准（DSS）。

9.椭圆曲线与椭圆曲线上的公钥密码

有限域上的椭圆曲线，椭圆曲线上的群，椭圆曲线上的公钥密码。

10 认证理论和技术

认证的概念，认证和保密的区别，单向认证和双向认证，认证协议的分类，零知识证明的认证协议，Kerberos 协议步骤，数字证书。

11 密码学数学基础

数论、群论、有限域理论

二、建议参考书

- 1、卢开澄编著《计算机密码学》（第三版），清华大学出版社