海 军 工 程 大 学

2024 年硕士研究生招生考试自命题科目考试大纲

科目代码：834　　科目名称：密码学

一、考试要求

主要考查学生对密码学基本概念的理解与掌握；对序列密码、分组密码、公钥密码及其应用的理解与掌握；对数字签名与认证及其应用的理解与掌握；对密钥管理基本知识及其应用的理解与掌握；以及运用基本理论和方法，分析解决密码算法工程应用问题的能力。

二、考试内容

1. 密码学概论

密码体制，密码学研究的基本问题及主要应用，密码学研究现状及发展趋势。编制密码的基本原理和方法，置换密码、代替密码、转轮密码。

2. 对称密码

序列密码的原理及工作方式，线性反馈移位寄存器，m-序列，非线性前馈和非线性组合模型，典型序列密码算法。分组密码的原理和设计原则，分组密码的两种典型结构，分组密码的主要工作模式，DES 算法，AES 算法，及其它典型分组密码算法。

3. 非对称密码

非对称密码的基本思想、工作方式，RSA 公钥密码算法，RSA 算法的安全性分析及其实现要点，Elgamal 公钥密码算法和 ECC 公钥密码算法。

4. 密码算法应用

数字签名的概念、原理及其主要应用，RSA、Elgamal 数字签名方案，特殊作用的数字签名方案。Hash 函数的性质，MD5 和 SHA-1 算法，Hash 函数的典型应用，消息认证，认证协议和身份认证。

5. 密钥管理

密钥的分类、层次结构、密钥的分散管理及 Shamir 门限秘密分割方案、密钥的生命周期、传统密码体制和公钥密码体制的密钥管理、数字证书的基本原理及应用。

三、考试形式

考试形式为闭卷、笔试，考试时间为 3 小时，满分 150 分。

题型包括：选题题 30 分、填空题 20 分、判断题 20 分、简答题 20 分、计算题 40 分、综合题 20 分。

四、参考书目

《应用密码学》. 胡向东等主编. 电子工业出版社，2019 年 6 月，第 4 版。