《0914 密码学》硕士研究生招生考试大纲

一、试卷满分及考试时间

试卷满分为 100 分，考试时间为 90 分钟。

二、考试形式

考试形式为闭卷、笔试。

三、学习内容

（一）古典密码

置换密码；代替密码；代替密码的破译；香农保密通信理论；数论的基本概念。

学习要求：

1．理解置换与代替两种基本形式的古典密码。

2．了解根据统计特性对代替密码的攻击原理。

3．掌握无条件安全性与计算安全性概念。

（二）序列密码

序列密码基本原理；LFSR；m 序列的伪随机性；B-M 算法与非线性综合。

学习要求：

1．掌握序列密码设计的基本思想。

2．掌握 LFSR 的工作原理。

3．掌握 m 序列的伪随机性。

4．掌握 B-M 算法，了解 LFSR 非线性综合的原理。

（三）分组密码

分组密码基本原理；DES 算法；AES 算法；分组密码算法的工作模式。

学习要求：

1．掌握分组密码设计的基本思想。

2．掌握 DES 算法的原理。

3．掌握 AES 算法的原理及关键密码模块的计算方法。

4．了解分组密码常见的几种工作模式。

（四）Hash 函数

Hash 函数基本原理；Hash 的构造方法；MD 系列的 Hash 函数；消息认证码。

学习要求：

1．掌握 Hash 函数的安全性定义。

2．了解 Hash 函数的构造方法。

3．了解 MD 系列的 Hash 函数。

4．了解消息认证码的地位和作用。

（五）公钥密码

公钥密码基本原理；RSA；ElGamal；ECC；数字签名基本原理；ElGamal 签名。

学习要求：

1．掌握公钥密码设计原理。

2．掌握 RSA 加密过程及计算方法。

3．掌握 ElGamal 加密算法。

4．掌握椭圆曲线点加计算。

5．掌握数字签名的原理及其安全性定义。

6．了解 ElGamal 数字签名方案。

（六）密码协议

密码协议基本概念；DH 密钥协商协议；秘密共享协议；身份认证协议。

学习要求：

1．掌握密码协议的基本特点。

2．掌握 DH 密钥协商及其计算方法。

3．掌握秘密共享的原理及其计算方法。

4．掌握身份认证地位、作用。

四、考核主要形式

1．选择、填空题（涵盖较广，包括概念、性质、计算、常识）。

2．简答题（简要回答算法的原理，包括分析、作图等）。

3．综合计算题（包括密码知识的分析和计算等）。

五、 参考书

1.《现代密码学》（第 2 版），陈鲁生、沈世镒编著，科学出版社，2008 年。