**杭州电子科技大学 全国硕士研究生复试同等学力加试科目考试大纲**

**考试科目名称：密码学 科目代码：**

一、密码学的基本概念

1．古典密码术。

2．Caesar密码与Hill密码 。

3．古典密码的两种基本方法。

4．密码学的基本原理与流程图。

5．密码体制的分类。

6. 密码系统的安全原则。

二、对称密码算法

1．DES加密算法。

2．AES加密算法。

3．国家密码标准算法SM2。

4．对称密码算法的设计基础（经典方法）。

5．对称密码的原理、特点与基本要求。

6. DES、AES、SM2等对称密码算法中的基本特性及优缺点。

三、公钥密码算法

1．RSA公钥加密算法与数字签名算法。

2．ElGamal公钥加密算法与数字签名算法。

3．椭圆曲线公钥加密算法与数字签名算法。

4. 对称加密算法与公钥加密算法的特点与数字。

5. 一般数字签名算法的概念、基本特性、组成结构。

6. RSA、ElGamal、ECC等公钥加密与数字签名的计算。

四、Hash函数

1．Hash函数的定义。

2．Hash函数的三个安全性要求。

1. Hash函数MD5与SHA-1的基本特性。

五、密码管理

1．密钥管理基本内容和概念。

2. Diffie-Hellman密钥交换协议及安全性基础。

3. 利用Diffie-Hellman协议简单地建立一个双方共享的密钥。

4. 认证机构CA与信任链。

5. 公钥证书X.509与基本内容。

**参考书目：《信息安全与密码学》(2007年版)，徐茂智、游林编著，清华大学出版社，2007.01**