一、试卷满分及考试时间

试卷满分为　　分，考试时间为　　分钟。

二、考试形式

考试形式为闭卷、笔试。

三、学习内容

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：

．理解置换与代替两种基本形式的古典密码。

．了解根据统计特性对代替密码的攻击原理。

．掌握无条件安全性与计算安全性概念。

序列密码基本原理；　　；　序列的伪随机性；　　算法与非线性综合。

学习要求：

．掌握序列密码设计的基本思想。

．掌握　　的工作原理。

．掌握　序列的伪随机性。

．掌握　　算法，了解　　非线性综合的原理。

分组密码基本原理；　　算法；　　算法；分组密码算法的工作模式。

学习要求：

．掌握分组密码设计的基本思想。

．掌握　　算法的原理。

．掌握　　算法的原理及关键密码模块的计算方法。

．了解分组密码常见的几种工作模式。

函数基本原理；　　的构造方法；　　系列的　　函数；消息认证码。

学习要求：

．掌握　　函数的安全性定义。

．了解　　函数的构造方法。

．了解　　系列的　　函数。

．了解消息认证码的地位和作用。

公钥密码基本原理；　　；　　；　　；数字签名基本原理；　　签名。

学习要求：

．掌握公钥密码设计原理。

．掌握　　加密过程及计算方法。

．掌握　　加密算法。

．掌握椭圆曲线点加计算。

．掌握数字签名的原理及其安全性定义。

．了解　　数字签名方案。

密码协议基本概念；　　密钥协商协议；秘密共享协议；身份认证协议。

学习要求：

．掌握密码协议的基本特点。

．掌握　　密钥协商及其计算方法。

．掌握秘密共享的原理及其计算方法。

．掌握身份认证地位、作用。

四、考核主要形式

．选择、填空题（涵盖较广，包括概念、性质、计算、常识）。

．简答题（简要回答算法的原理，包括分析、作图等）。

．综合计算题（包括密码知识的分析和计算等）。

五、 参考书

《现代密码学》（第　版），陈鲁生、沈世镒编著，