山东科技大学2014—2015学年第一学期

《信息安全基础》期末考试试卷（B卷）

班级_____ 姓名_____ 学号_____

题号	一	二	三	四	总得分	评卷人	审核人
得分							

一、填空（每空2分，共20分）

1、信息安全所面临的威胁来自很多方面，并且随着时间的变化而变化。这些威胁可以宏观地分为人为威胁和_____。

2、密码体制从原理上可分为_____和_____。

3、分组密码与流密码的区别在于_____。

4、公钥密码体制目前主要用于密钥管理和_____。

5、_____和_____是由Shannon提出的设计密码系统的两个基本方法，目的是抗击敌手对密码系统的统计分析。

6、DES是迄今为止世界上最为广泛使用和流行的一种分组密码算法，它的分组长度为_____比特，密钥长度为_____比特，是早期的称作Lucifer密码的一种发展和修改。

7、SHA-1算法的输入为小于2^{64}比特长的消息，分为512比特长的分组，输出为_____比特的消息摘要。

二、名词解释（每个5分，共20分）

1、 m序列　　2、陷门单向函数

3、椭圆曲线上的离散对数问题　　4、（k,n）-秘密分割门限方案

三、问答题（每题**10**分，共**30**分）

1、对密码系统的攻击类型主要有哪些？各个类型攻击者所掌握的内容有哪些（可用表格给出）？

2、数字签字应具有哪些性质？

3、假定两个用户A、B分别与密钥分配中心KDC（Key Distribution Center）有一个共享的主密钥 K_A 和 K_B，A希望与B建立一个共享的一次性会话密钥，应该如何进行？画出分配实例图。

四、计算题(**30**分，每小题**15**分)

1、设多表代换密码 $C_i \equiv AM_i + B \pmod{26}$ 中，**A**是 2×2 矩阵，**B**是0矩阵，又知明文“dont”被加密为“elni”，求矩阵A。

2、在Diffie-Hellman密钥交换过程中，设大素数 $p=11$，$a=2$ 是 p 的本原根。求解下列问题：

(1) 用户A的公开钥是 $Y_A=9$，求其秘密钥 X_A。

(2) 设用户B的公开钥 $Y_B=3$，求A和B的共享密钥K。