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（A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、安全业务指安全防护措施，有保密业务、_____、完整性业务、_____以及访问控制。

2、线性反馈移位寄存器LFSR输出序列的性质完全由其_____决定。

3、IDEA是瑞士联邦技术学院的James Massey和来学嘉等人提出的加密算法，它的分组长度为64比特，密钥长度为_____比特。

4、RSA 算法是 1978 年由 R. Rivest、A. Shamir 和 L. Adleman 提出的一种用_____构造的、也是迄今为止理论止最为成熟完善的公钥密码体制，该体制已得到广泛的应用。

5、Diffie-Hellman 和 ElGamal 密码体制是基于_____的公钥体制。

6、Rijndael 算法的轮函数由 4 个不同的计算部件组成，分别是：字节代换（ByteSub）、_____、_____、密钥加（AddRoundKey）。

7、如果令 $n=35$，则 n 的 Euler 函数 $\phi(n)$ ＝_____。

8、2005 年，_____等人提出了对 SHA－1 的碰撞搜索攻击，该方法用于攻击完全版的 SHA－0 时，所需的运算次数少于 2^{39}，攻击 58 步的 SHA－1 时，所需的运算次数少于 2^{33}。

二、名词解释（每个**5**分，共**20**分）

1、离散对数　　2、陷门单向函数

3、第 II 类生日攻击　　4、零知识证明

三、问答题（每题**10**分，共**30**分）

1、安全的网络通信必须考虑哪些方面？

2、设计一个性能良好的序列密码最基本的设计原则是什么？它又可分为哪些基本原则？

3、在具有仲裁方式的数字签字中，如果仲裁方和发送方共谋否认曾发过的消息，也可和接收方共谋以伪造发送方的签字，如何解决这个问题，请给出实例。

四、计算题(**30**分，每小题**15**分)

1、利用椭圆曲线实现ElGamal密码体制，设椭圆曲线是 $E_{11}=(1,6)$，生成元 $G=(2,7)$，接收方A的秘密钥 $n_A=7$。

(1) 求A的公开钥 P_A。

(2) 发送方B欲发送消息 $P_m=(10,9)$，选择随机数 k=3，求密文 C_m。

2、在 Shamir 秘密分割门限方案中，设 $k=3$， $n=5$， $q=19$，5 个子密钥分别是 $f(1)=1$， $f(2)=5$， $f(3)=4$， $f(4)=17$， $f(5)=6$，根据插值多项式并求秘密数据 s。