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）答案

一、填空

1、　自然威胁　2、单钥体制　双钥体制

3、　有无记忆性　4、数字签字　5、　扩散　混淆

6、　56　64　7、　160

二、名词解释（每个 5 分，共 20 分）

1、m 序列：周期达到最大值的序列，称为 m 序列。

2、陷门单向函数：t 是与 f 有关的一个参数。已知 x，计算 y 使得 y=f(x)容易；如果不知道 t，已知 y，计算 x 使得 y=f(x)是难的，但知道 t 时，已知 y，计算 x 使得 y=f(x)是容易的。参数 t 称为陷门（Trapdoor）。

3、椭圆曲线上的离散对数问题：在椭圆曲线构成的 Abel 群 Ep(a,b) :P∈Ep(a,b)，P 的阶是一个非常大的素数，P 的阶是满足 nP=O 的最小正整数 n。Q=kP，已知 k 和 P 易求 Q；已知 P、Q 求 k 则是困难的。这就是椭圆曲线上的离散对数问题。

4、设秘密s被分成n个部分信息，每一部分信息称为一个子密钥或影子，由一个参与者持有，使得：

①由k个或多于k个参与者所持有的部分信息可重构s。

②由少于k个参与者所持有的部分信息则无法重构s。

则称这种方案为(k,n)-秘密分割门限方案，k称为方案的门限值。

三、问答题

1、答：对密码系统的攻击类型列表如下

攻击类型	攻击者掌握的内容
唯密文攻击	加密算法、截获的部分密文　（3分）
已知明文攻击	加密算法、截获的部分密文（6分） 一个或多个明文密文对
选择明文攻击	加密算法、截获的部分密文（8分） 自己选择的明文消息以及由密钥产生的相应密文
选择密文攻击	加密算法、截获的部分密文（10分） 自己选择的密文消息以及相应的被解密的明文

2、数字签字应具有哪些性质？

答：数字签字应满足以下要求：

① 签字的产生必须使用发方独有的一些信息以防伪造和否认。（3 分）

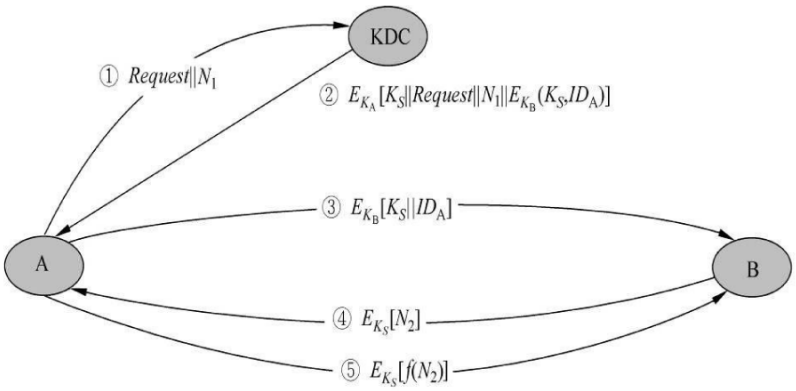
③ 签字的产生应较为容易。（6 分）

④ 签字的识别和验证应较为容易。（8 分）

⑤ 对已知的数字签字构造一新的消息或对已知的消息构造一假冒的数字签字在计算上都是不可行的。（10分）

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。

答：



四、计算题(**30** 分，每小题 **15** 分)

略