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）答案

一、填空

1、　认证业务　不可否认业务　2、反馈函数　3、　128

4、　数论　5、　有限域上离散对数问题

6、　行移位（ShiftRow）、列混合（MixColumn）

7、　24　8、王小云

二、名词解释

1、离散对数：设 p 是素数，a 是 p 的本原根。即 $a^1, a^2, \cdots, a^{p-1}$ 在 mod p 下产生 1 到 p-1 的所有值，所以对 $b\in\{1,\cdots,p-1\}$，有惟一的 $i\in\{1,\cdots,p-1\}$ 使得 $b\equiv a^i \bmod p$。称 i 为模 p 下以 a 为底 b 的离散对数，记为

$$i\equiv\log_a b\pmod p。$$

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、寻找函数H的具有相同输出的两个任意输入的攻击方式，称为第II类生日攻击。

4、在交互证明系统中，设P知道某一秘密，并向V证明自己掌握这一秘密，但又不向V泄露这一秘密，这就是最小泄露证明。进一步，如果V除了知道P能证明某一事实外，不能得到其他任何信息，则称P实现了零知识证明，相应的协议称为零知识证明协议。

三、问答题

1、答：　应考虑以下几个方面：

1) 加密算法。　（3 分）

2) 用于加密算法的秘密信息。（3 分）

3) 秘密信息的分布和共享。（8 分）

4) 使用加密算法和秘密信息以获得安全服务所需的协议。（10 分）

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？

答：最基本的设计原则是“密钥流生成器的不可预测性”，它可分解为下述基本原则：

答：① 长周期。② 高线性复杂度。③ 统计性能良好。④ 足够的“混乱”。⑤ 足够的“扩散”。⑥ 抵抗不同形式的攻击。　（少一个扣2分）

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。

答：具体实例如下：

① $X \to A$：$ID_X \| E_{SK_X}[ID_X \| E_{PK_Y}[E_{SK_X}[M]]]$。

② $A \to Y$：$E_{SK_A}[ID_X \| E_{PK_Y}[E_{SK_X}[M]] \| T]$。（4 分）

首先，在协议执行以前，各方都不必有共享的信息，从而可防止共谋。（6 分）

第二，只要仲裁者的秘密钥不被泄露，任何人包括发方就不能发送重放的消息。（8 分）

最后，对任何第三方（包括 A）来说，X 发往 Y 的消息都是保密的。（10 分）

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。

解：(1) 这里 $a=1, b=6, p=11$，则对于 $2G=G+G$，可首先计算

$$\lambda \equiv \frac{3x_1^2+a}{2y_1} \equiv \frac{3\times 2^2+1}{2\times 7} \equiv 8 \bmod 11$$

利用公式 $\begin{cases} x_3 \equiv \lambda^2 - x_1 - x_2 \bmod 11 \\ y_3 \equiv \lambda(x_1-x_3) - y_1 \bmod 11 \end{cases}$ 可得 （5分）

$2G=G+G=(2,7)+(2,7)=(5,2)$

同样可得 $4G=2G+2G=(5,2)+(5,2)=(10,2)$

$3G=2G+G=(5,2)+(2,7)=(8,3)$

$7G=4G+3G=(10,2)+(8,3)=(7,2)$

所以A的公开钥 $P_A=(7,2)$ （10分）

(2)利用椭圆曲线加密算法，得 $C_m=(P_m, kP_A)$。经计算可得

$C_1=kG=3G=(8,3)$ （12分）

$C_2=P_m+kP_A=(10,9)+3(7,2)=(10,9)+(3,5)=(10,2)$

即密文 $C_m=(10,2)$ （15 分）

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。

解：利用其中的 **3** 个子密钥 **f(2)=5,f(3)=4,f(5)=6**，就可按以下方式重构 **f(x)**：

$$5\frac{(x-3)\ (x-5)}{(2-3)\ (2-5)}=5\frac{(x-3)\ (x-5)}{(-1)\ (-3)}=5\frac{(x-3)\ (x-5)}{3}=5\cdot\left(3^{-1}\bmod 19\right)\cdot(x-3)\ (x-5)$$
$$=5\cdot 13\cdot(x-3)\ (x-5)=65\ (x-3)\ (x-5)$$
$$4\frac{(x-2)\ (x-5)}{(3-2)\ (3-5)}=4\frac{(x-2)\ (x-5)}{(1)\ (-2)}=4\frac{(x-2)\ (x-5)}{-2}=4\cdot\left((-2)^{-1}\bmod 19\right)\cdot(x-2)\ (x-5)$$
$$=4\cdot 9\cdot(x-2)\ (x-5)=36\ (x-2)\ (x-5)$$
$$6\frac{(x-2)\ (x-3)}{(5-2)\ (5-3)}=6\frac{(x-2)\ (x-3)}{(3)\ (2)}=6\frac{(x-2)\ (x-3)}{6}=6\cdot\left(6^{-1}\bmod 19\right)\cdot(x-2)\ (x-3)$$
$$=6\cdot 16\cdot(x-2)\ (x-3)=96\ (x-2)\ (x-3)$$

所以

$$f(x)=\left[65\ (x-3)\ (x-5)+36\ (x-2)\ (x-5)+96\ (x-2)\ (x-3)\right]\bmod 19$$
$$=\left[8\ (x-3)\ (x-5)+17\ (x-2)\ (x-5)+\ (x-2)\ (x-3)\right]\bmod 19$$
$$=\left(26x^2-188x+296\right)\bmod 19$$
$$=7x^2+2x+11$$

从而得秘密为 **s=11**。