**密码学第八次作业参考答案**

1.【ECC基础知识】

（1）密码应用中所使用的两类椭圆曲线分别为多用于软件应用的定义在上的素曲线和多用于硬件应用的定义在上的二元曲线。

（2）对于上的椭圆曲线，含有3个公共参数，分别为，其方程形式为。给定，该方程最少有0个解，最多有2个解。

（3）对于上的椭圆曲线，设，其中为无穷远点，则加法运算定义如下：

i.

ii.若，则

iii.，则按如下方法计算：，其中。

iv.乘法定义为重复相加。

ECC的安全性建立在由和确定的困难问题上的，该问题称为椭圆曲线对数问题。

1. 由（2）和（3）可知，对于上的椭圆曲线和生成元，设，，若，则和满足，点为无穷远点。
2. 椭圆曲线上同在一条直线上的三个点的和是无穷远点

\*写出负元的情况即可；第二空有多种等价形式；可以不写

2.【ECC计算】

（1）【上的椭圆曲线】确定椭圆曲线上的所有点，指出这些点中所有的生成元，并选取其中一个生成元，写出计算、所对应点的计算过程。

迭代计算，迭代计算，可知点集为

该群有素数个元素，因此除零元（无穷远点）外均为生成元。

、计算参考表（计算过程略）：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 点 | 序号 | 点 | 序号 | 点 |
| 1 |  | 5 |  | 9 |  |
| 2 |  | 6 |  | 10 |  |
| 3 |  | 7 |  | 11 |  |
| 4 |  | 8 |  | 12 |  |

\*该表使用方法如下：选取的生成元序号为，则对应的序号为，对应的序号为。

（2）【上的椭圆曲线】（选做）使用不可约多项式定义的有限域，令，确定椭圆曲线上的所有点。

首先计算，然后打表计算如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  | |
|  | 11 |  |  | 00 |
|  | 01 |
|  | 11 |
|  | 10 |
|  | 01  ( |  |  | 00 |
|  | 00 |
|  | 01 |
|  | 01( |
|  | 00 |  |  | 00 |
|  | 11 |
|  | 00 |
|  | 11 |
|  | 11  ( |  |  | 00 |
|  | 10 |
|  | 10 |
|  | 00 |

点集为。

3.【基于ECC的公钥密码体制】：

（1）【DH密钥交换】选用上的椭圆曲线，生成元，Alice的私钥，Bob的私钥。求通信双方共享的密钥，以及在有中间人Darth存在（其私钥）的情况下共享的密钥和。

（2）【ElGamel加解密】选用上的椭圆曲线，生成元，Bob的私钥。

i.求Bob的公钥。

ii.Alice加密明文消息，选取随机值，求密文。

iii.写出Bob收到后解密得到的过程。