**密码学第八次作业**

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和多用于硬件应用的定义在。

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

（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：。

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。

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。

（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。

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）【ElGamal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。

**注意：**

以上作业请使用**pdf**文档格式提交，于**2023年4月28日（星期五）23:59**之前在OJ系统上提交，并将作业命名为“**学号\_姓名\_密码学第八次作业**”。如“21371234\_张三\_密码学第八次作业”。