**云南大学数学与与统计学院**

**上机实践报告**

|  |  |  |
| --- | --- | --- |
| **课程名称**：近代密码学实验 | **年级**： | **上机实践成绩**： |
| **指导教师**：陆正福 | **姓名**： |  |
| **上机实践名称**：椭圆曲线离散对数问题实验 | **学号**： | **上机实践日期**： |
| **上机实践编号**：No.06 | **组号**： | **上机实践时间**： |

**一、实验目的**

1. 熟悉椭圆曲线离散对数问题(ECDLP)及其有关的密码体制
2. 实现与ECDLP有关的基本算法
3. 了解参数与参数规模
4. **实验内容**
5. 编程椭圆曲线离散对数问题(ECDLP)有关的算法
6. 编程实现Diffie-Hellman密钥交换协议的椭圆曲线版本。
7. 编程实现ElGamal加密体制的椭圆曲线版本。

说明：

* **基础有限域为素域GF(p)（p为大素数）的情形为必做实验**
* **基础有限域为GF（2\*\*m）的情形为选做实验**

**三、实验环境**

个人计算机，建议选择Java 8平台。

对于基础有限域为素域GF(p)的实验情形，可利用Java的BigInteger实现

对于基础有限域为GF（2\*\*m的实验情形，可采用支持有限域的任意平台（包括数学软件）进行研究型或验证型实验。

对于非信息与计算科学专业的学生，可以选择任意编程平台

**四、实验记录与实验结果分析**

（注意记录实验中遇到的问题。实验报告的评分依据之一是实验记录的细致程度、实验过程的真实性、实验结果的解释和分析。**如果涉及实验结果截屏，应选择白底黑字。**）

**五、实验体会**

**（请认真填写自己的真实体会）**

**六、参考文献**

1. 主讲课教材（数学密码学导论）第五章

**2.（如有其它参考文献，请列出）**