云南大学数学与统计学院

上机实践报告

|  |  |  |
| --- | --- | --- |
| **课程名称**：近代密码学实验 | **年级**：2015级 | **上机实践成绩**： |
| **指导教师**：陆正福 | **姓名**：刘鹏 |  |
| **上机实践名称**：椭圆曲线离散对数问题实验 | **学号**：20151910042 | **上机实践日期**：2018-05-14 |
| **上机实践编号**：No.06 | **组号**： | **上机实践时间**：11:56 |

# 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

# 二、实验内容

1. 编程椭圆曲线离散对数问题(ECDLP)有关的算法

2. 编程实现Diffie-Hellman密钥交换协议的椭圆曲线版本。

3. 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、实验平台

Windows 10 Pro Workstation 1803；

*SageMath* version 8.1, Release Date: 2017-12-07；

# 四、实验记录与实验结果分析

1题

**Solution**:

bash命令：

程序代码1

ssh界面

安装过程分析：

# 六、实验体会

# 七、参考文献