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**：离散对数问题实验 | **学号**：20151910042 | **上机实践日期**：2018-03-07 |
| **上机实践编号**：No.01 | **组号**： | **上机实践时间**：22:39 |

# 一、实验目的

熟悉离散对数问题（DLP）及其有关的密码体制。

# 二、实验内容

1. 编程实现与离散对数问题（DLP）有关的算法；
2. 编程实现Deffie-Hellman体制；
3. 编程实现EIGamal体制。

# 三、实验平台

Windows 10 Pro Workstation 1709（Edit Report）；

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

*Ubuntu* 18.10 x86-64（take Experiments）

*Xshell* 5 Build 1339。

# 四、实验记录与实验结果分析

1题

编程实现与离散对数问题（DLP）有关的算法。求解离散对数问题常见的算法有：Shanks的大步小步算法（baby-step giant-step algorithm）、Pollard rho算法、Pohlig-Hellman算法、Index Calculus算法等。对于是兼职三十位以上的素数，已知最优的模剩余类域中离散对数求解算法是应用了数域筛法技术的Index Calculus算法。

**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