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 1703 Enterprise（Edit Report）；

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

*Ubuntu* 17.10 x86-64（take Experiments）

*Xshell* 5 Build 1339。

# 四、实验记录与实验结果分析

1题

*SageMath*的安装与调用。

**Solution**:

SageMath是开源的软件，可以在官网上进行免费下载。由于SageMath不原生支持Windows，用虚拟机存在文件的读写问题，所以这里采用实体机安装。下载官方推荐[1]的二进制程序，免得自己编译。之后安装ssh工具，可以远程访问。具体bash命令如下

bash命令：

程序代码 1

ssh界面

打开ssh软件，连接到Ubuntu，就可以在命令行中调用sage软件了。简单运行一下几个交互式命令。

安装过程分析：

# 六、实验体会

# 七、参考文献

[1] 开发组 S. Sage Tutorial [M]. Release 4.3 ed., 2010.