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：格密码实验 | 学号：20151910042 | 上机实践日期：2018-07-17 |
| 上机实践编号：No.07 | 组号： | 上机实践时间：21:37 |

# 实验目的

1. 熟悉格密码学的基本概念
2. 掌握格中与密码学有关的基本算法
3. 掌握格论与密码设计有关联的几个难题

# 实验内容

1. 熟悉课本中的同余体制、背包体制、GGH体制、NTRU体制。
2. 探索格中好基的选择，建议先通过一些数学软件进行探索，再设计算法，继而通过通用编程语言进行实现。
3. 实现Babai算法，通过实验验证算法的正确性。
4. 实现GGH体制。
5. 实现NTRU体制（选做）。

# 实验平台

Microsoft Windows 10 Pro Workstation 1803；

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

Ubuntu17.10 x86-64;

Xshell 5 Build1339。

# 实验记录与实验结果分析

## 理论补充学习

### 格

在数学中，格是其非空有限子集都有一个上确界（并）和一个下确界（交）的偏序集合（poset）。

偏序集合：给定集合，是上的二元关系，若满足：

（1）自反性：，有；

（2）反对称性：，且，则；

（3）传递性：，且，则；

则称是上的非严格偏序或者自反偏序。

# 实验体会

通过这次实验，我懂得了如何配置SageMath的运行环境，同时还知道了SageMath与Python2语言的关系。虽然这个报告尚不全面，不过在通读文档之后，可以在使用中继续学习。

另外，我发现去年十二月底，Sage团队发布了原生Windows版本的软件，我的认知在完成本实验时还停留在大一阶段，所以采用了Linux平台。以后的实验报告均采用Windows原生Sage进行，但是这里不再更改，因为除了平台，其他方面都是相同的。

# 参考文献

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