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：密码学分析实验 | 学号：20151910042 | 上机实践日期：2018-07-17 |
| 上机实践编号：No.08 | 组号： | 上机实践时间：08:30 |

# 实验目的

1. 熟悉现代密码分析的基本概念

2. 掌握格中与密码分析有关的基本算法

3. 了解其它密码分析算法

# 实验内容

1. 实现LLL算法或其变种。

2. 利用LLL算法攻击已有的密码体制。

提示 往届学生已经完成的攻击实验有：RSA体制，背包体制GGH体制，NTRU体制等）

3. 选做与密码分析有关的其它方面的算法实现

（1）离散对数的分析算法

（2）因子分解的分析算法

（3）纠错密码的分析算法

（4）基于椭圆曲线的分析算法

（5）基于格论的分析算法

# 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

## 1题

# 实验体会

# 参考文献

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

[2] 主讲课英文教材chapter 6,2,3,5