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**：古典加密技术实验 | **学号**：20151910042 | **上机实践日期**：2018-03-08 |
| **上机实践编号**：No.02 | **组号**： | **上机实践时间**：11:38 |

# 一、实验目的

熟悉古典密码学的思路和方法。

# 二、实验内容

1. 编程实现古典密码学的主要体制和算法

2. 编程实现古典密码学的主要分析方法。

# 三、实验平台

Windows 10 1703 Enterprise（Edit Reports）；

*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

（注意记录实验中遇到的问题。实验报告的评分依据之一是实验记录的细致程度、实验过程的真实性、实验结果的解释和分析。如果涉及实验结果截屏，应选择白底黑字。）

1题

在*SageMath*下，编程实现以凯撒加密为代表的古典加密方法（对字母表进行变换）。

**Solution**:

bash命令：

安装过程分析：

2题

根据sage tutorial手册，进行重要代码的实验。

**Solution**:

# 六、实验体会

# 七、参考文献

1. 主讲课教材 第二章及附录B.2