实验一 Sage 入门及基本数论算法的实现

一、实验目的：

通过本次实验，熟悉开源软件 sage 的使用，为后续实验做好准备。

回顾数论的基本算法，加深对其的理解，为本学期密码学课程及课程实践打好基础。

二、实验内容：

1．sage 的安装和使用：

“Sage 是一款由华盛顿大学开发的类似于 matlab/mathematica，并且整合了很多已有的开源软件包的开源数学软件。”Sage 目前只有 Linux 与 MacOS 版的，Windows 平台可以在虚拟机下安装使用。建议在 linux 下安装使用。各版本下载地址：http://www.sagemath.org/download.html 。选择下载服务器后可以选择下载各个平台上的版本。具体的安装指导请参照：http://www.sagemath.org/doc/installation/ 。里面有针对各个平台的安装说明，或参照附件 sage 安装教程

Sage 也可在线使用，不想安装的同学可以在云平台下在线使用 Sage。网址是 https://cloud.sagemath.com/ （个人认为不如终端方便，不推荐）。

Sage 教程：一些参考或相关的链接

官方教程：http://www.sagemath.org/doc/tutorial/index.html 。

官方中文：http://www.sagemath.org/zh/ 。（官网上东西挺多，多浏览，可能有时候官网不能下载甚至不能打开，就换个时间再试试吧）

国内博客 Lainme’ss Blog 的教程中文翻译，博客上还有一些 Sage 使用的帖子：http://www.lainme.com/doku.php/topic/sage/start 。

国内 amao 博客男单 618 的中文教程翻译，博客有很多关于 Sage 使用的帖子：http://ai7.org/wp/html/682.html 。

注意，中文教程只是便于大家入门，翻译总会有问题，建议大家阅读英文的官方教程。

Sage 是基于 Python 语言的，语法与 python 基本一致。

2．基本数论算法的实现：

虽然 Sage 提供了一些现有的数论库函数。但是为了加深对于上学期所学数论算法流程的理解，本次实验不允许调用现有的库函数。

本次实验需要完成的算法包括厄拉多塞筛法、扩展的欧几里德算法、费马素性测试、快速模幂算法、中国剩余定理、Solovay-Stassen 素性测试、Miller-Rabin 素性测试、元根生成。

三、实验要求：

1、每一个算法的实现独立为一个.sage 或.sagews 文件，同实验报告一起打包提交，压缩文件命名格式为： 学号_ 姓名_ 实验一.zip/rar，如：14061001_***_实验一.zip

2、代码鼓励写注释。实验报告应至少含有算法原理、算法流程、测试样例及运行结果，鼓励写心得体会或感想建议。

3、3 月 11 日实验课开始做第一次实验，第二次实验前完成本次实验，将源码及实验报告打包发送到邮箱 buaa2015_xinan@163.com。