实验二 传统加密技术实践

一、 实验目的：

1、熟悉重要的传统加密技术，体会其中使用的代替和置换的重要思想。

2、通过实验，掌握sage中求模以及矩阵求逆的方法，以及sage中重要内置数据类型的使用。

二、 实验说明：

本次实验内容按照难度不同分为初级、中级与高级三个等级，得分会以选定的实验等级为基准。鉴于本次实验内容较为容易，鼓励选中高级。

三、 实验内容（参照课本P45编程题）

**1、初级：**

**完成2.21与2.25。**

**2、中级：**

**完成2.22与2.26。**其中2.26，要求先实现m维Hill密码的加密和解密。然后根据明文及其对应的密文，攻击得到密钥。为了能够成功攻击，需要加密的明文具有一定的长度。明文可以只有acsii码字符，如果有中文更好。

**3、高级：**

**完成2.22、2.24与2.26。**其中2.24，要求先用自选的单表代替密码将某段明文加密，之后再针对密文进行字母频率的攻击。提示：题目中提到“按可能性大小的顺序给出可能的明文”，请思考这个可能性怎么界定，并在实验报告中进行说明；另外，因为涉及到字母频率的问题，故加密前的明文应尽量长以便符合字母出现频率的规律。实验报告中测试部分应当有加密前的明文，加密后的密文以及破解得到的按照可能性大小排列的前N个明文。

推荐一个统计频率解密的网站<http://quipqiup.com/index.php>。

四、 实验要求

1、每一个题目的实现独立为一个.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\_实验二.zip/rar…** 如：14061001\_XX\_实验二.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、本次实验进行时间为**两周**。4月8日实验课上检查。希望大家能及时上交sage文件以及实验报告。打包后的文件请发送到邮箱：buaa2015\_xinan@163.com。发送截止时间为**2016年4月8日晚24点**。