实验四 AES的相关实践

一、 实验目的：

1、深刻理解AES算法实现的原理，掌握AES加解密实现的流程，体会对称加密算法的特点，并注意比较AES与DES的相同与不同之处。

2、熟悉AES差分攻击的原理以及实现流程。

3、理解分组密码的工作模式，体会不同模式的特点以及对于加密强度的贡献。

4、通过设计程序结构，增强程序的实用性和可扩展性，提高编程能力。

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。

三、 实验内容：

**1、初级：**

**完成10轮AES的加密与解密，消息长度128bit，密钥长度128bit。**为了实现容易，建议按照课本5.5“一个AES例子”部分来实现。关于列混淆的计算，可以参考课本4.7“有限域GF(2^n)”来手工编程实现，也可以使用sage里的方法，参见附录B.4。

**2、中级：**

**完成初级的内容，自选工作模式，实现10轮ASE算法对大批量报文的加解密。**注：分组密码的工作模式参照课本第六章，选择ECB模式分数相对低。

**3、高级：**

**完成中级内容，并做出界面。提示：使用python的Tkinter库可以写出界面，这个在sage里也可以使用。推荐个学习的链接**[**http://www.cnblogs.com/kaituorensheng/p/3287652.html**](http://www.cnblogs.com/kaituorensheng/p/3287652.html)

**另外，额外的附加作业，完成可以加分，每个难度都可以做。AES的差分攻击，3轮、2轮差分攻击都可以，难度比较大。希望有精力的同学进行探索。**

注意：

1、AES加密、解密的算法是一致的，但注意加解密时四个阶段顺序的细微变化。

2、建议将加密与解密的操作分开执行，加密后得到密文输出，即一个密文文件；同时给定一个密文文件，可以进行解密，得到明文输出。

3、以上课本章节数是指第五版的课本。

四、 实验要求：

1、请合理划分程序结构，每一部分独立为一个.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\_实验四.zip/rar…** 如：14061001\_\*\*\_实验四.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。**由于每个人的程序的输入流程、输出位置的不同，请在报告的测试样例及运行结果处进行详细说明。**

3、本次实验进行时间为**两周**。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课程邮箱：buaa2015\_xinan@163.com。截止至第五次实验课前(5月6日)。