实验三 DES的相关实践

一、 实验目的：

1、深刻理解DES算法实现的原理，掌握DES加解密实现的流程，体会对称加密算法加解密密钥相同的特点和DES加密、解密算法的一致性。

2、熟悉差分攻击的原理以及实现流程。

3、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16轮DES的加密与解密。**

**2、中级：**

**完成以下两者之一：**

**（1）完成16轮DES的加密与解密。并同时实现ECB、CBC、CFB、OFB、CTB五种模式之一的加解密(ECB最简单，分数略低)。**

**（2）完成16轮DES的加密与解密，并对3轮DES进行差分攻击。**

**3、高级：**

**完成16轮DES的加密与解密，并同时实现ECB、CBC、CFB、OFB、CTB五种模式之一的加解密。并对3轮DES进行差分攻击。**

注意：

1、DES加密、解密的算法是一致的，只是密钥的使用顺序不同。

2、鉴于sage已经能够方便地支持大数运算，在实现过程中，密钥长度应不小于56bit（扩展为64bit）。

3、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。

4、程序要模块化，把各个功能封装成模块。**16轮DES加解密，只需要对64bit的块进行加解密即可。五种加密模式要求实现长消息的加解密。**

5、附件中给出了13级刘保证的的3轮DES差分攻击的实验报告，方便大家更好的理解DES差分。

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\_实验三.zip/rar…** 如：14061001\_\*\*\_实验三.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。截止至第四次实验前(4月22日)。