实验五RSA的相关实践

一、 实验目的：

1、理解并掌握RSA算法实现的原理及流程，体会公钥加密算法的思想及其与对称加密算法的不同。

2、掌握OAEP-RSA的实现技术，理解RSA算法在实际中的应用要求。

3、理解针对RSA的一些常见的攻击，进一步体会RSA算法的安全性。

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：**

**普通RSA算法的实现。包括加密和解密，解密要求采用中国剩余定理(CRT)来加快解密速度。**

**2、中级：**

**OAEP-RSA算法的实现。包括加密和解密，解密要求采用中国剩余定理(CRT)来加快解密速度。实验报告中要求分析OAEP-RSA如何抵抗适应性选择密文攻击(CCA2)攻击。**

**3、高级：**

**在中级的基础上，独立设计课上讲到的对RSA的一些攻击实验，如共模攻击、小指数攻击等。**

注意：

1. 生成的公私钥对最好可以本地保存以便实现独立的加解密。**密钥长度不少于1024bit**。

2、因为公钥加密算法对一定长度的明文加密后得到的密文长度不固定，故在解密时密文段的定界问题需要考虑。

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、大家阅读RSA标准，据此选择参数和哈希函数。标准在压缩包中。

5、一些和数论相关的函数，要求调用之前写过的函数。

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\_实验五.zip/rar…** 如：14061001\_XX\_实验五.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**。**5月20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。