**实验2：RSA密码系统的实现及其应用**

实验时数：4学时。

**一、实验目的**

1. 熟练掌握RSA密码算法及其签名算法。

2. 掌握交换律的概念。

3. 应用RSA密码算法。

4. 熟练掌握RSA批签名方案。

**二、实验内容**

1. 任选C或Python语言实现RSA密码算法，其中参数p,q的长度可调整，例如512bits,1024bits。

2. 验证具有相同模数的RSA密码算法是否满足交换律。

3. 利用RSA密码算法实现两方智力扑克游戏。

4. 编写RSA签名算法以及批签名方案(两个消息的批签名)。

1）实例化：令p,q均为512bits的参数，m1=4,随机选择一对公私钥(e，d)，计算其签名。

2）令m1=4,m2=7,随机选择两对公私钥(e1,d1),(e2,d2),计算其批签名，并从批签名中划分出单个消息m1,m2的签名。

**三、实验报告编写**

1. 实验报告文件命名规则：学号+姓名+实验n，例：201922222222张三实验1。

2. 按实验报告格式，遵从实验要求完成：

3. 请同学们每次实验记得签到，把每次上机的内容保存好，完成报告后，实验后的第二周统一发送到D盘/实现报告/安全协议/相应班级。