**实验三 编程实现RSA公钥密码算法**

实验学时：4学时

实验类型：验证

实验要求：必修

**一、实验目的**

编程实现RSA公钥密码的加解密方法。

**二、实验内容**

(1)编程实现RSA算法的加密过程；

(2)编程实现RSA算法的解密过程。

**三、实验原理、方法和手段**

RSA算法过程如下：

（1）选取两个保密的大素数，（二者不可相差悬殊）

（2）计算，；

（3）选取整数，满足，且；

（4）计算，满足（一般）

则为加密密钥，为解密密钥。

加密过程为



解密过程为



**四、实验组织运行要求**

本实验采用集中授课形式，每个同学独立完成上述实验要求。

**五、实验条件**

每人一台计算机独立完成实验，有如下条件：

（1）硬件：微机；

（2）软件：VC++6.0、VC++.Net 2005。

**六、实验步骤**

（1）将各函数编写完成；

（2）在主函数中调用各函数，实现加密和解密。

**七、实验报告**

实验报告主要包括实验目的、实验内容、实验原理、源程序及结果。