实验 3 RSA 非对称加密算法

1. 实验目的

1) 了解非对称加密机制。

2) 理解 RSA 算法的加解密原理。

3) 能够使用 RSA 算法对数据进行加解密处理。

2. 实验原理

非对称密钥加密也称为公开密钥加密，或者叫做公钥加密算法。使用公开密钥密码的每一个用户都分别拥有两个密钥：加密密钥和解密密钥，它们两者并不相同，并且由加密密钥得到解密密钥在计算机上是不可行的。每一个用户的加密密钥都是公开的。因此，加密密钥也称为公开密钥。所有用户的公开密钥都将记录在作用类似于电话号码薄的密钥本上，而它可以被所有用户访问，这样每一个用户都可以得到其他所有用户的公开密钥。同时，每一个用户的解密密钥将由用户保存并严格保密。因此，解密密钥也称为私有密钥。

非对称密码算法解决了对称密码体制中密钥管理的难题，并提供了对信息发送人的身份进行验证的手段，是现代密码学最重要的发明。公钥加密算法一般是将对密钥的求解转化为对数学上的困难问题的求解，例如 RSA 算法的安全性是建立在“大数分解和素性检测”这个数论难题的基础上。

RSA加密算法于1977年由美国麻省理工学院的Ronal Rivest,Adi Shamir和Len Adleman三位年轻教授提出，并以三人的姓氏Rivest,Shamir和Adleman命名为RSA算法。这三位科学家荣获2002年度图灵奖，以表彰他们在算法方面的突出贡献。该算法利用了数论领域的一个事实，那就是虽然把两个大质数相乘生成一个合数是件十分容易的事情，但要把一个合数分解为两个质数的乘积却十分困难。合数分解问题目前仍然是数学领域尚未解决的一大难题，至今没有任何高效的分解方法。它无须收发双方同时参与加密过程，既可以用于保密也可以用于签名，因而非常适合于电子邮件系统的加密，互联网和信用卡安全系统。

RSA 参数生成：

1) 生成两个大素数，p 和 q。

2) n = pq,且Φ(n) = (p - 1)(q - 1)。

3) 选择一个随机数 b(1 < b < Φ(n)),使得 gcd(b,Φ(n)) = 1。

4) $a = b^{-1} \bmod \Phi(n)$。

5) 公钥为(n,b),私钥为(p,q,a)。

RSA 加解密过程：

假定 Bob 选取 p=101，q=113。那么 n = 11413 和Φ(n)=100*112 = 11200。假设 Bob 选取 b = 3533。那么 $a = b^{-1} \bmod \Phi(n) = 6597$。因此 Bob 的秘密解密指数为 a = 6597。如果 Alice 想加密明文 9726 并发给 Bob。她将计算：$9726^{3533} \bmod 11413 = 5761$。然后把密文 5761 通过信道发出。当 Bob 收到密文 5761 后，用解密指数 a 来计算：$5761^{6597} \bmod 11413 = 9726$。

3. 实验的软硬件环境要求

运行 Windows 操作系统的计算机，具有 C++语言编译环境。

4. 实验内容

用 c\c++语言实现 RSA 加解密程序。

说明：

1）p,q,b 均为程序随机产生的值，且 p,q 为 128 bits 的整数。

2）加密的数据由人工输入，且为 10000 以内的整数。

3）将 p,q,a,b,n,Φ(n)的值以及加密后的密文、解密后的明文输出到文件或屏幕。

4）可以使用开源运算库（例如：GMP）。

注：RSA 实验是最后一个实验，实验时间为第 13 周，第 15 周实验课提交纸质实验报告，并将源代码以压缩包的形式命名为“实验 3-学号-姓名”发送至邮箱 17212010065@fudan.edu.cn