哈尔滨工业大学

计算机科学与技术学院

《信息安全概论》

实验报告

计算机科学与技术学院

计算机系网络教研室制

|  |  |
| --- | --- |
| 课程名称： | 信息安全概论 |
| 实验名称： | RSA加密实验 |
| 指导教师： | 韩琦 |
| 学生姓名： | 马婷婷 |
| 组 号： | 2-34 |
| 实验日期： | 18-03-10 |
| 实验地点： | 远程桌面 |
| 实验成绩： |  |

一、实验目的

通过用RSA算法对实际数据进行加密和解密来深刻了解RSA的运行原理及其特点，能够编译并分析RSA算法，进而加深对非对称加密算法的理解与认识。

# 二、实验环境

实验设备：个人计算机建立远程桌面连接(winxp32-word-dym)

操作系统：运行Windows ，VS2010编译环境。

验证软件：位于远程桌面的“RSA加解密实验”文件夹中的一个压缩包：bmrsall.zip

# 三、实验内容与实验要求

**实验内容：**

（1）任务一：RSA加解密算法的原理，画出算法流程图。

（2）任务二：使用C语言实现RSA加密算法，编译运行给出的实验代码，并对代码进行分析。

**原理分析：**

**1.秘钥的产生：**

(1)公钥：

随机产生两个长度为K/2位的素数P 和 Q；

计算公钥 ;( 是K位的长度)

(2)加密秘钥（公开的）：

随机产生一个加密密钥 满足如下条件：

而且是保证解密密钥有解的充要条件。 其中。

(3)解密秘钥（保密的）：

求解解密密钥

其中为解密密钥 的逆元

**2.加密解密**

(1)加密过程:

其中M表示明文，C表示密文

(2)解密过程:

其中M表示明文，C表示密文

**3.算法的可靠性：**

（1）。只有知道和，才能算出。

（2）。只有知道和，才能算出。

（3）。只有将因数分解，才能算出和。

将两个大质数相乘十分容易，但是想要对其乘积进行因式分解却极其困难，因此可以将乘积公开作为加密密钥。这种困难程度保证了算法的可靠性。

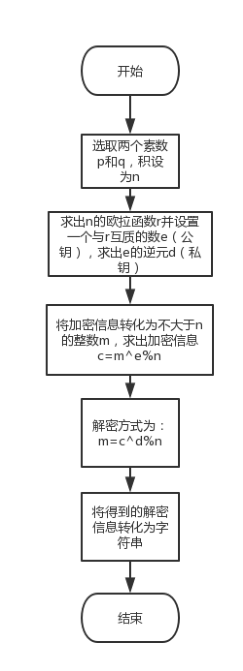
**实验要求：**

分析实验代码，画出算法流程图，对实验结果进行分析，完成思考题目，总结实验的心得体会，并提出实验的改进意见。

# 四、实验过程与分析

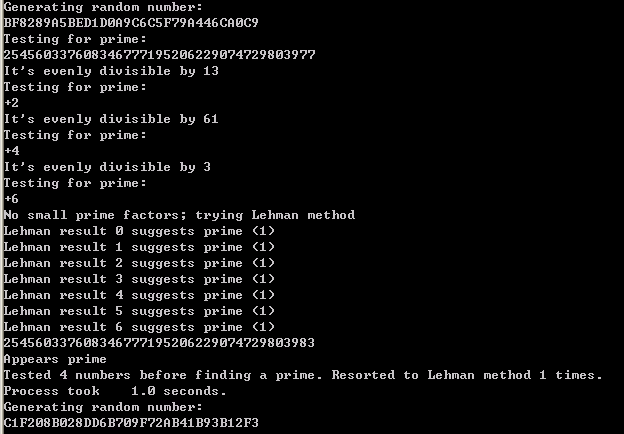
**实验过程：**

算法流程图：

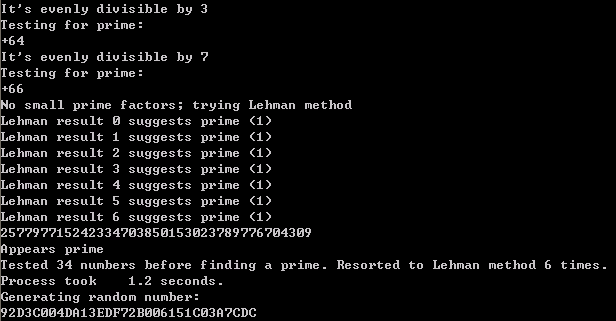


**运行结果:**

随机生成第一个大素数：



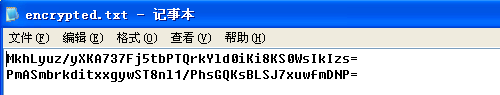
随机生成第二个大素数：



明文：

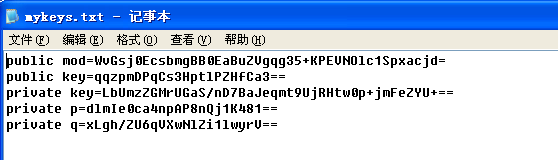


密文：

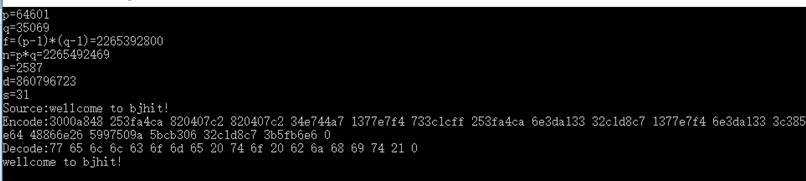


密文解密结果：





较弱的RSA结果：



**实验问题与分析：**

1. 运行demo.bat时运行完窗口就关闭了，不利于观察结果，因此右键编辑，加入一行pause，使运行完等待。
2. 任务二中生成密钥的较弱，密钥二进制的长度最多16位，而bmrsall.zip里给的代码是使用了高精度的，所以能产生大长度的密钥，这样保证了RSA的安全性，但是同样会带来问题就是涉及过多大数运算，使得运算速度较慢。代码中关于实行大素数的方法是先生成一个大的伪随机数，通过多次素数测试rabin-miller算法筛选，直到生成一个通过多次测试的数，为选中的素数。
3. 对于秘钥的生成，基本过程就是如上，先生成两个大素数，计算其乘积。随机生成的奇数keyE，直到与φ(n)互素。拓展欧几里得算法可以得到keyD。
4. 之后的加密解密过程安装上面的公式计算即可，这里面涉及到大数的幂指数运算，，采用了快速幂来解决。

五、实验结果总结

**结果分析：**

RSA算法是一种非对称密码算法，所谓非对称，就是指该算法需要一对秘钥，使用其中一个加密，则需要用另一个才能解密。通过先生成大随机数再判定该随机数是否是素数来实现大随机素数的生成，循环测试来降低非素数通过的概率以提升安全性，由于进行的都是大数计算，使得RSA最快的情况也比DES慢上好几倍。一般来说只用于少量数据加密。本次实验中RSA秘钥的长度并没有特别长，因此安全性不是很高，容易破解。另外这里生成素数的时候，是先用了一个伪随机数生成器，随机种子是time(NULL)，如果攻击者能够通过某种方式，获取生成时间，也就是随机种子，这样生成的序列就带有了可预测性，使得密文被破解。寻找质数的算法不能给攻击者任何信息，这些质数是怎样找到的，尤其产生随机数的软件必须非常好。要求是随机和不可预测。

**分析与思考：**

1. 通过本实验，论述RSA算法的加密原理是什么？

RSA算法利用了单向函数正向求解很简单，而反向求解很复杂的特性。具体来讲就是：

1. 计算两个大质数的乘积很简单，而已知其相乘的合数，将其分解为两个大质数很难。
2. ，已知明文M、publicKey(n) 和 keyE求密文C简单，而已知keyE、publicKey(n)、C求解M很困难。
3. 在上述算法中哪些模块是该算法的核心模块？

RSA的核心算法是模幂运算，以及随机大素数的生成等等。这些都会影响RSA算法的速度和安全性。

1. 对于一个RSA加密算法的密文，要得到明文需要哪些要素？

由上述过程我们可以看出，keyE和keyD形成非对称密钥关系，加密者使用keyE加密，解密者使用keyD解密，假设第三者拦截了密文、keyE和n，keyE，不知道P和Q的前提下，无法推算出keyD，也就无法获得明文A。也就是说获取明文要么知道keyD，要么知道P或者Q。

**心得体会：**

通过本实验我了解掌握了RSA加密解密算法的基本原理，进一步加深了对RSA算法的理解。同时也对RSA算法的安全性和可靠性方面，通过查阅资料获得了更多的了解。比如RSA的秘钥生成中，随机序列的不可预测性和随机性必须足够好，由于进行的是大数计算，运算速度慢，一般来说只用于少量数据加密。而对于一些攻击手段，比如第三方讲自己的加密秘钥传递给对话者的某一方，截取对话者的公钥和密文，用自己的秘钥来解密之后，用对话者公钥加密，从而实现窃听对话的攻击。这些都使得我对RSA算法进一步加深了了解。

**改进意见：**

实验环境方面有些简陋，基本的IDE没有，实验指导书上的代码看着难受，但是助教很负责的给出了格式规范的代码，方便了我们的阅读。希望下次比如像这次windows环境下的实验，可以直接给出源码下载，这样就不用远程操作受到实验室电脑配置的影响了。