哈尔滨工业大学大学计算机科学与技术学院

《RSA加密试验》

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： | 韩越 |
| 组 号： | 第二组11号 |
| 实验日期： | 2018-03-10 |
| 实验地点： | 哈尔滨工业大学 |
| 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。

普及素数、欧拉定理等基本数论知识，以及快速幂、Rabin-Miller素数测试、欧几里得辗转相除法、Stein法、扩展欧几里得法等基础数论算法。

二、实验环境

操作系统：运行Windows ，g++ (GCC) 5.3.0编译环境。

验证软件：bmrsall软件，该软件位于桌面“RSA加解密实验”文件夹内。

三、实验内容与实验要求

1. **实验内容**

任务一：学习RSA加解密算法的原理 并 画出算法流程图

1. 产生密钥
   1. 随机产生两个长度为K/2位的素数P 和 Q；
   2. 计算公钥;(publicKey 是K位的长度)
   3. 随机产生一个加密密钥 , 其中；

注：这是保证解密密钥有解的充要条件，称为N的欧拉函数,值为:

* 1. 求解解密密钥，为加密密钥关于的逆元 ，此公式原方程为
  2. 由此公钥，加密密钥，解密密钥全部产生。

1. 加密

。其中M表示明文，C表示密文

1. 解密

。其中M表示明文，C表示密文

任务二：使用C语言实现RSA加密算法

编译运行提供的RSA加密算法代码，并对代码进行分析。

1. **原理分析**

RSA算法本质上使用了欧拉定理，欧拉定理表明，若n, a为正整数，且n, a互质，则:

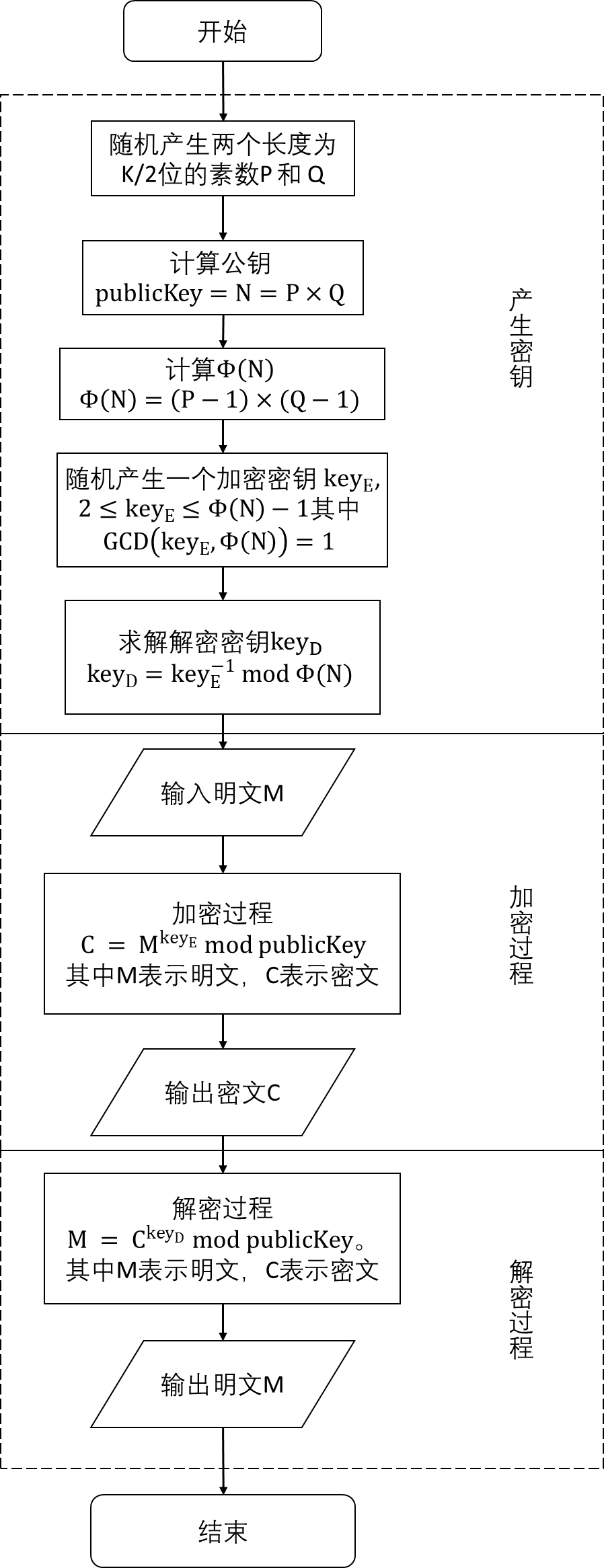
容易得到：

那么我们的解密过程可以写成

显然明文得到了还原。

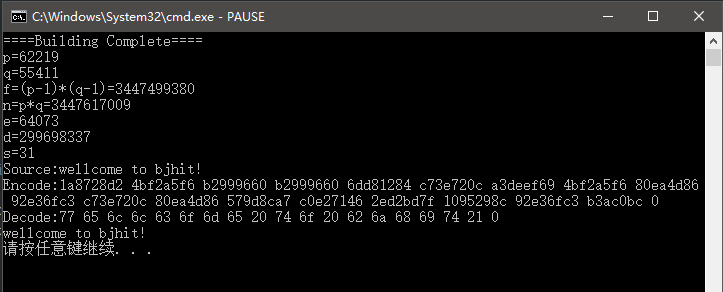
四、实验过程与分析

任务一：算法流程图



任务二：使用C语言实现RSA加密算法





**代码分析：**

首先准备明文串pSrc[]="wellcome to bjhit!"用于加密。

1. **根据RSA算法产生密钥**

先生成p, q, n=p\*q, f=(p-1)\*(q-1)。

RandomPrime()函数产生随机素数。RandomPrime函数循环产生随机奇数，素数密度是所以期望logN次就能产生一个素数。

RabinMiller()函数检测产生的数是否是素数。由RabinMiller素数测试方法检测是否为素数，RabinMiller素数测试方法根据费马小定理，测试30个a来判断p是否是素数。通过RabinMiller素数测试方法的数是非素数的概率很小。

接着生成加密密钥e。循环生成65536以下的奇数，然后使用SteinGcd方法判断生成的e与f是否互质，接着使用扩展欧几里得算法求得e关于f的逆，即解密密钥d。

SteinGcd()函数使用SteinGcd方法求得e和f的最大公约数。和欧几里德算法 算法不同的是，Stein算法只有整数的移位和加减法，这对计算机处理大素数比较有利。

Euclid ()函数是扩展欧几里得算法。在求在最大公因数的过程中解得a\*x-b\*y=1的最小整数解。

最后处理出公钥n长度s。

1. **加密过程**

加密过程使将明文的ascll码序列切分成64位的片段，使用加密公式和快速幂算法将每个片段加密成密文。

1. **解密过程**

解密过程使将密文使用解密公式和快速幂算法将每个片段转变回ascll码序列。

快速幂算法，每次将幂数折半处理。。

五、实验结果总结

**C语言实现RSA结果分析**

产生的素数p=62219, q=55411，确实为素数。

f为p-1, q-1乘积，f=3447499380。

公钥n=p\*q=3447617009。

加密密钥e=64073，与f互质。

解密密钥d=299698337，满足e\*d mod f=1。

最终公钥长度s=31。

明文wellcome to bjhit!被加密成：



解密还原为明文ascll序列：



**思考题目：**

1. 通过本实验，论述RSA算法的加密原理是什么？

RSA算法基于一个十分简单的数论事实：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。

算法本质使用欧拉定理，欧拉定理能够还原明文的原理已经在前文原理分析中解释，这里不再赘述。

1. 在上述算法中哪些模块是该算法的核心模块？

核心模块是素数生成模块，互质模块，求逆模块和快速幂模块。

素数生成模块由RandomPrime()和RabinMiller()两个核心函数组成，产生随机数和检测素数，为算法提供重要的随机素数。

互质模块用来测试生成加密密钥。

求逆模块生成解密密钥。

快速幂模块是加密解密过程的核心操作。

3）对于一个RSA加密算法的密文，要得到明文需要哪些要素？

需要密文，公钥和解密密钥。

或者密文，公钥，公钥分解得的素数p,q，以及加密密钥。

**心得体会：**

密码学博大精深，使用简单的数论知识构造出精妙的非对称加密算法RSA算法，把破解难度转移到大数分解这个难题上。

加深了我对密码学和信息安全的认识，让我受益匪浅。

**实验改进意见：**

可以让学生自己实现部分算法来加深对算法的理解，如RabinMiller、快速幂、SteinGcd等。