文章参考了<http://www.ruanyifeng.com/blog/2013/06/rsa_algorithm_part_one.html>。

## 一点历史

对称加密算法的弱点：甲方必须把加密规则告诉乙方，否则无法解密。保存和传递密钥，就成了最头疼的问题。

非对称加密算法的性质：

* 乙方生成两把密钥（公钥和私钥）。公钥是公开的，任何人都可以获得，私钥则是保密的。
* 甲方获取乙方的公钥，然后用它对信息加密。
* 乙方得到加密后的信息，用私钥解密。

## 数学基础

### 同余

定义1：给定一个正整数，如果两个整数除以的余数相同，则称对模同余，记做

不同余怎么写？把等价号换成不等号就行。

定义2：若，则对模同余。

定义3：给定整数，若，则对模同余。

性质：

1. 自反性：
2. 对称性：若则
3. 传递性：若，则

若，则：

1. 若，则，其中为整数。
2. 若，则，其中为正整数。
3. 若，则；特别地，当也就是互质时，有.

还有几个较复杂的定理，用到了再搬运。

### 欧拉函数

欧拉函数表示小于且和互质（coprime）的整数的个数。

其中，是的一个质因子（不计重复）。公式1可以用容斥原理证出来，在我的组合数学笔记中有记载。

而我们要用到的是欧拉函数的完全积性：积的欧拉函数等于各个因子的欧拉函数的积。

公式2可以从公式1中观察出来。

以及质数的欧拉函数：

显然，所有小于质数的正整数都和互质。

### 欧拉定理和费马小定理

欧拉的很多定理都叫欧拉定理。数论中的欧拉定理又叫费马-欧拉定理。

若为正整数，且互质，则

欧拉定理有一个特例，这也是著名的费马小定理：

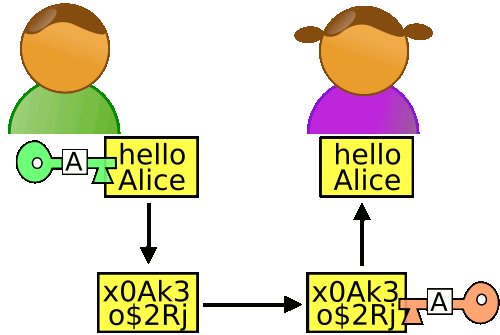
假设正整数与**质数**互质，则

### 模反元素

如果两个正整数和互质，那么一定能找到整数使得

此时，就叫做的模反元素。由欧拉定理知，就是的模反元素。

## 密钥生成步骤



假设Alice要与Bob进行加密通信，她该怎么生成公钥和私钥呢？

### 随机选择两个不相等的质数和

Alice选择了61和53。实际应用中，这两个质数越大，越难破解。

### 计算乘积

这个密钥就是12位的。实际应用中，RSA密钥一般是1024位，重要场合则为2048位。

### 计算的欧拉函数

### 随机选择一个小于且与互质的整数

为了方便，我们一般选择小于且不是它的质因数的质数。Alice在1到3120之间随机选择了17。

### 计算对于的模反元素

这也就是求关于的二元一次方程

的一组整数解。可以用扩展欧几里得算法（扩展辗转相除法）求解。总之，Alice算出一组整数解为。

### 封装公钥和私钥

在Alice的例子中，n=3233，e=17，d=2753，所以公钥就是(3233,17)，私钥就是(3233, 2753)。

**注意这里的小括号的意思不是最大公约数，而是数对。**

实际应用中，公钥和私钥的数据都采用ASN.1格式表达。

## 加密和解密

### 用公钥加密

假设Bob要向Alice发送加密信息 （明文，英文术语message，这里是一个小于的非负整数），那么可以求解如下关于的同余方程，就是的密文（cipher）。

换个更直观的式子，也就是

### 用私钥解密

Alice拿到Bob发来的2790以后，就用自己的私钥(3233, 2753)进行解密。可以证明，下面的等式一定成立：

换个更直观的式子，就是

对于本例，要求的是。这样就算回了明文65。

### 理论细节：私钥解密的正确性

证明

设，则上式能化为

把展开，所有含有的项对余数的贡献都为0。因此，证明（3）实际上就是证明

也就是

由中国剩余定理，要证明式子（6），等价于证明左右两边分别模和模同余。

先证明左右两边模同余。考虑这两种情况：

由同余的性质，有

由和关于互为模反元素，以及，有

此时。由费马小定理，有

从而

同理可以证明

综上式子(6)得证。

### 技术细节：幂模

但是这么大的数，用机器根本表示不了，怎么求模呢？首先我们研究一下幂模的性质：

1. 积的模：
2. 引理-幂的模：

基于这种性质，可以得出求幂模的数值算法：

ulong modexp(ulong base, ulong exp, ulong mod)

{

ulong s = 1;

**while** (exp > 0)

{

**if** (exp % 2 == 1) *// if exp is odd*

s = (s \* base) % mod;

base = (base \* base) % mod;

exp = exp / 2;

}

**return** s;

}

还有算法比赛中常用的快速幂取模算法：

ulong modexp(ulong base, ulong exp, ulong mod)

{

ulong res=1;

**while**(exp > 0)

{

**if**(exp & 1)

res = res \* base % mod;

base = (base \* base) % mod;

exp = exp >> 1;

}

**return** res;

}

## 附录

### 欧拉定理的直接证明

设集合为小于且与互质的数的集合。显然集合的大小为。

再设集合。观察集合发现

1. 集合中的任意两个数都不关于同余。否则，也就是存在。根据同余的定义，有  
   也就是说能整除，从而。但这与和互质的前提矛盾。
2. 对于每个，由于与互质，因此与互质。根据欧几里得算法，有

由（1）和（2）可知，中的数除以的余数，恰好取遍集合的每一个元素。因此必然存在某种的排列，使得和的对应元素关于同余。从而

其中perm代表自然数序列的一个乱序全排列。根据同余的性质4，有

从而

从而