rsa-math

一：简介

rsa加密算法是一种非对称加密算法。主要原理是利用大整数因式分解十分困难来确保加密的安全性。举一个简单的例子两个素数的乘积 65537 * 65539 = 4295360521，这样计算很容易，但是想把4295360521因式分解成65537*65539却不太容易。更不用说因式分解以下实际使用的类似以下1024位数字：

> 125265898721415905440644507839315409700563546724528072091122281772620164539979309237727718945936762358969294653557264794356653367016303596899076547394629237020038327801702039954468887621264217111908402487768089808095965495841873677675609617642946005275888729089454967979950045095657604271198840576401001170037

二：涉及数学

rsa主要涉及以下数学原理：欧拉函数,费马小定理,欧拉定理

三：数学原理详解

符号说明:

gcd(a,m)=x代表a和m的最大公约数为x,假如x为1也代表a和m互质

a≡b (mod n) 注意是≡不是=,这就是同余式,表示a模n余数和b模n余数相等,即a%n=b%n

3.1欧拉函数

给定一个正整数n，计算1和n之间与n互质的整数个数的计算方法就叫欧拉函数。

数学记号为φ(n)，比如φ(8)=4,因为1到8之间与8互质的有1，3，5，7。

欧拉函数有下面几种情况和性质：

1.如果n=1，则φ(n)=1，因为1和任何数都互质

2.如果n为质数则φ(n)=n-1,因为质数和比它小的数都互质

3.如果n为质数的幂次数，即:

$$n = p^k$$

则：

$$\varphi(n) = p^k - p^{k-1}$$

这是因为只有一个数不包括因数p才能和n互质,含有因数p的数有:

$$1p, 2p, 3p, 4p, ..., p^{k-1} * p \quad (\text{一共是}p^{k-1}\text{个数})$$

4.如果gcd (m, n) = 1, 则 φ(mn) = φ(m)φ(n)

证明之前假设有两个集合,第一个为小于mn且mn互质的整数a集合为下图左的集合, 第二个为满足小于m且与m互质的整数b和满足小于n且与n互质的整数c的组合对集合为下图右边的集合.

$$\left\{a: \begin{array}{l} 1 \leqslant a \leqslant mn \\ \gcd(a,mn) = 1 \end{array}\right\} \rightarrow \left\{(b,c): \begin{array}{ll} 1 \leqslant b \leqslant m, & \gcd(b,m) = 1 \\ 1 \leqslant c \leqslant n, & \gcd(c,n) = 1 \end{array}\right\}$$
$$a \bmod mn \quad \mapsto \quad (a \bmod m, a \bmod n)$$

举一个更具体的例子,假设m=4,n=5, 则第一个集合有与20互质的数组成{1,3,7,9,11,13,17,19},第二集合由序对 {(1,1),(1,2),(1,3),(1,4),(3,1),(3,2),(3,3),(3,4)}组成,刚好都是8个,即 ϕ(45)=*ϕ(4)*ϕ(5)

要证明它只需要证明下面两点:

(1) 第一个集合的不同数对应第二个集合的不同序对

(2)第二个集合的每个序对都对应第一个集合的某个数

下面先证明(1):取第一个集合的数a1,a2,假设它们对应第二个集合相同的序对.则有a1≡a2(mod m),a1 ≡ a2 (mod n).

因此a1-a2一定能被m和n整除,然而,m与n互质,所有a1-a2一定能被整除mn.因为a1,a2等小于mn,显然只有a1=a2才能满足a1-a2=0被mn整除.这表明a1和a2是第一个集合中相同的数.这就完成(1)的证明.

证明(2)的陈述需要用到"中国剩余定理"来证明.那么下面就说明以下中国剩余定理.

中国剩余定理定义: 设m与n是整数,gcd (m , n) = 1, b 与 c 是 任意整数.则对同余式组 x ≡ b (mod m) 与 x ≡ c (mod n) 求解,恰好有一个解0 ≤ x < mn.

证明:

由 x ≡ b (mod m) , 设 x = my + b (y为整数). 代入第二个同余式得: my ≡ c - b (mod n). 已知 gcd (m, n) = 1 则恰有一个解y1, 0 ≤ y1 < n. 则x = my1 *+ b.

由中国剩余定理显然(2)的陈述也被证明了.

3.2费马小定理

证明:

先举一个具体的例子:验证以下同余式是否成立:

$$3^6 = 1\,(mod\,7)$$

我们先来看分别取整数为1,2,3,4,5,6模7和分别乘以3后模7来的结果:

x (mod 7)	1	2	3	4	5	6
3x (mod 7)	3	6	2	5	1	4

我们观察到虽然顺序不同但第一列的每个数在第二列都有.根据余式的性质,把第二列的所有数撑起来和第一列所有数的乘积模7的结果也相同.

$$\text{即}(3*3)(3*6)(3*2)(3*5)(3*1)(3*4) \equiv 1*2*3*4*5*6(mod\,7),$$
$$\text{用阶乘简化得}: 3^6 * 6! \equiv 6!(mod\,7), \text{两边消去}6!\text{则得}:$$
$$3^6 \equiv 1(mod\,7)$$

然后我们来进行一般化的证明:

首先根据上面的启发,我们证明以下引理:

$$\text{设}p\text{是素数}, a\text{是任何整数且}a\text{不被}p\text{整除}, \text{则}$$
$$\text{数}a, 2a, 3a, ..., (p-1)a\ (mod\,p)\text{与}$$

$$数1, 2, 3, ..., (p-1)\ (mod\, p)相同, 尽管次序不同.$$

我们采用反证法证明.数列a,2a,3a,...,(p-1)a 包含 p-1个数,显然没有一个数被p整除.假设从数列中取两个数ja和ka,并假设它们同余, ja ≡ ka (mod p). 则p | (j-a)a , 因为假设p不整除a,所以 p | j-a.又因为 1 ≤ j,k ≤ p - 1, 则 | j-k| < p - 1. 所以仅当 j = k时 p | j - a.则推出a,2a,3a,...,(p-1)a 中的每个数都不同余,同时数列的个数为p-1个,所以尽管次序不能不同,a,2a,3a,...,(p-1)a 和 1,2,3,...,(p-1) 包含相同的数(mod p).

利用该引理,很容易推导出费马小定理的证明.即:

$$\begin{gathered} a, 2a, 3a, ..., (p-1)a\ (mod\, p)与数列1, 2, 3, ..., (p-1)\ (mod\, p)的数相同 \\ 所以它们的乘积也相同： \\ a * 2a * 3a * * * ((p-1)a) \equiv 1 * 2 * 3 * * * (p-1)\ (mod\, p) \\ 简化得： \\ a^{p-1} * (p-1)! \equiv (p-1)! (mod\, p) \end{gathered}$$

3.3欧拉定理

$$如果gcd(a, m) = 1, 则a^{\varphi(m)} \equiv 1(mod\, m)$$

欧拉定理相比费马小定理更一般化了.区别在于模m不需要是质数,而费马小定理里的模p得是质数.证明的过程其实和费马小定理类似.我们先证明以下引理:

$$\begin{gathered} 如果gcd(a, m) = 1, 则数列b_1 a, b_2 a, b_3 a, ..., b_{\varphi(m)} a\ (mod\, m)与 \\ 数列b_1, b_2, b_3, ..., b_{\varphi(m)}\ (mod\, m)的数相同, 尽管次序不一致. \end{gathered}$$

我们采用和费马小定理类似的方式证明:

$$\begin{gathered} 如果b与m互质, 则ab也与m互质. 从而b_1 a, b_2 a, b_3 a, ..., b_{\varphi(m)} a\ (mod\, m) \\ 同余于数列b_1, b_2, b_3, ..., b_{\varphi(m)}\ (mod\, m)中的某个数. \\ 从第一个数列取两个数b_j a, b_k a, 假设它们同余, 即b_j a \equiv b_k a (mod\, m). \\ 则m|(b_j - b_k)a. 但是m和a互质, 因此m|b_j - b_k. 然而b_j, b_k在1到m之间, \\ 因此|b_j - b_k| \leq m-1. \\ 只有0能满足m|(b_j - b_k). 从而b_j = b_k. \\ 这说明b_1 a, b_2 a, b_3 a, ..., b_{\varphi(m)} a\ (mod\, m)中每个数模m都不一样. \\ 因此完成了上述引理的证明 \end{gathered}$$

以此类推:

$$b_1 a * b_2 a * b_3 a * * * b_{\varphi(m)} a \equiv b_1 * b_2 * b_3 * * * b_{\varphi(m)}\ (mod\, m)$$

从而完成欧拉定理的证明.

四：rsa加密算法

4.1 公私钥生成步骤

1. 选择两个不同的质数p和q
2. 计算p和q的乘积n
3. 计算n的欧拉函数φ(n)
4. 随机选择一个整数e，条件是1< e < φ(n)，且e与φ(n) 互质。
5. 计算一个和e相乘然后模φ(n)为1的数d,即ed≡1(mod φ(n))
6. 把上面生成的n和e作为公钥,n和d作为私钥.

4.2加密和解密步骤

首先需要把需要发送的消息转换成数字形式,假设转化后数字格式消息为m,则加密公式为:

$$m^e\ (mod\, n) \equiv c(mod\, n), 即求m^e模m余数, 假设结果为c$$

解密公式为:

$$c^d(mod\, n) \equiv m(mod\, n), 即求c^d模n得原消息m$$

举一个简单的例子来验证下:(实际位数会比下面的例子大的多)

公私钥等相关数:

```
p=61
q=53
n=p*q=61*53=3233
e=17
d=2753
```

假设消息m为65,则加密计算结果为

$$m^e(mod\, n) \equiv 65^{17}(mod\, 3233) \equiv 2790(mod\, 3233), 即c = 2790$$

解密结果为:

$$c^d(mod\, n) = 2790^{2753}(mod\, 3233) \equiv 65(mod\, 3233), 即m = 65$$

五: rsa的正确性

$$
\begin{gathered}
加密公式m^e \equiv c(mod\, n), 则c可以写成以下形式: \\
c = m^e - kn \\
将c代入解密公式, 则 \\
(m^e - kn)^d \equiv m(mod\, n) \\
等同于证明m^{ed} \equiv m(mod\, n) \\
由于ed \equiv 1(mod\, \varphi(n)) \\
所以ed = h(\varphi(n)) + 1 \\
所以m^{h\varphi(n)+1} \equiv m(mod\, n) \\
\\
①假设m与n互质, 根据欧拉定理, 则 \\
m^{\varphi}(n) \equiv 1(mod\, n) \\
那么(m^{\varphi}(n))^h m \equiv m(mod\, n), 原式得到证明. \\
\\
②假设m与n不互质, 由于n等于pq, 所以m要么等于kp或kq. \\
假设m = kp, 那么kp与q也必然互质, 根据欧拉定理: \\
(kp)^{q-1} \equiv 1(mod\, q) \\
进一步得到: \\
((kp)^{q-1})^{h(p-1)}kp \equiv kp(mod\, q) \\
进一步整理得: \\
(kp)^{h(q-1)(p-1)}kp \equiv kp(mod\, q) \\
因为\varphi(n) = (q-1)*(p-1), 所以: \\
(kp)^e d = tq + kp, 此时t必然能被p整除, 设t = t'p, 则: \\
(kp)^e d = t'pq + kp, 又因为m = kp, n = pq, 所以:
\end{gathered}
$$

$$m^e d \equiv m(mod\, n)成立, 证毕.$$

参考资料:

[1]阮一峰_RSA算法原理

https://www.ruanyifeng.com/blog/2013/06/rsa_algorithm_part_one.html

https://www.ruanyifeng.com/blog/2013/07/rsa_algorithm_part_two.html

[2]初等数论概论

华章数学译丛 数论概论 （原书第三版）