RSA算法

作者：zdy

前置知识

互质关系

如果两个正整数，除了1以外，没有其他公因子，我们就成这两个数是互质关系（co-prime）.

性质:

1. 两质数互质
2. 一质数，另一个数只要不是质数的倍数，则互质
3. 两个数中，较大的得是质数，则互质
4. 1和其他数互质
5. P是大于1的整数， P和P-1互质
6. P是大于1的奇数，P和P-2互质

欧拉函数

$$\varphi(n)\text{是求对于给定整数}n\text{，小于等于}n\text{的正整数中有多少个与}n\text{构成互质关系。}$$
$$1.n=1,\varphi(n)=1$$
$$2.n\text{为质数，}\varphi(n)=n-1$$
$$3.n\text{为质数的某一个次方，即}n=p^k,k>=1\text{，则}\varphi(p^k)=p^k-p^{k-1}$$
$$\text{证明：当一个数不包含质数}p\text{才可能与}n\text{互质，而包含}p\text{的数有}p^{k-1}\text{个，即}1\times p,2\times p,\ldots\varphi(p^{k-1})\times p$$
$$4.n\text{可以分解成两个互质的整数之积：}n=p_1\times p_2,\text{则}\varphi(n)=\varphi(p_1\times p_2)=\varphi(p_1)\times\varphi(p_2)$$
$$\text{证明：（中国剩余定理）}$$
$$5.\text{因为任意一个大于}1\text{的正整数，都可以写成一系列质数的乘积}n=p_1^{k_1}\times p_2^{k_2}\ldots\times p_{r-1}^{k_{r-1}}\times p_r^{k_r}\text{由第四条和第三条可知，}$$
$$\varphi(n)=\varphi(p_1^{k_1})\times\varphi(p_2^{k_2})\ldots\times\varphi(p_{r-1}^{k_{r-1}})\times\varphi(p_r^{k_r})=p_1^{k_1}\times p_2^{k_2}\ldots\times p_{r-1}^{k_{r-1}}\times p_r^{k_r}\times(1-\frac{1}{p_1})\times(1-\frac{1}{p_2})\ldots\times(1-\frac{1}{p_{r-1}})\times(1-\frac{1}{p_r})=n\times(1-\frac{1}{p_2}$$

欧拉定理

$$\text{如果两个正整数}a\text{与}n\text{互质，}n\text{的欧拉函数为}\varphi(n)\text{则}a^{\varphi(n)}\equiv 1(mod)n$$
$$\text{特别情况：}n\text{为质数，（费尔小定理）}a^{n-1}\equiv 1(mod)n$$

模反元素

$$\text{正整数}a\text{和}n\text{互质，那么一定能够找到整数}b\text{满足}ab\equiv 1(mod)n$$
$$a^{\varphi(n)}=a\times a^{(\varphi(n)-1)}\equiv 1(mod)n$$

欧几里得算法

$$gcd(a,b)=gcd(b,\mathrm{a\ mod\ b})=\ldots=gcd(m,0)=m$$
$$\text{证明①：}a\text{可以表示成}a=kb+r\text{（}a\text{，}b\text{，}k\text{，}r\text{皆为正整数)}$$
$$\text{假设}d\text{是}a,b\text{的一个公约数，记作}d|a,d|b\text{，即}a\text{和}b\text{都可以被}d\text{整除。}$$
$$\text{而}r=a-kb\text{，两边同时除以}d\text{，}r/d=a/d-kb/d\text{，由等式右边可知}m=r/d\text{为整数，因此}d|r$$
$$\text{因此}d\text{也是}b,amodb\text{的公约数。}$$
$$\text{因}(a,b)\text{和}(b,amodb)\text{的公约数相等，则其最大公约数也相等，得证。}$$

斐蜀定理

$$\text{若}a,b\text{是整数，且}d=gcd(a,b)\text{，那么对于任意整数}x,y,\text{总存在}ax+by\text{是}d\text{的倍数。}$$
$$\text{对于给定整数}a,b\text{，}ax+by=c\text{有整数解}(x,y)\text{的充要条件}c\text{是}gcd(a,b)\text{的倍数}$$

扩展欧几里得算法

$$ax+by=gcd(a,b)\ (1)$$
$$\text{现在：我们想求出符合条件的整数解}(x,y)$$
$$\text{根据欧几里得算法：}gcd(a,b)=gcd(b,a\%b)\ (2)$$
$$\text{根据斐蜀定理}:bx_1+(a\%b)y_1=gcd(b,a\%b)\ (3)$$
$$\text{根据}(2)\text{式}:ax+by=bx_1+(a\%b)y_1=bx_1+(a-b\lfloor\frac{a}{b}\rfloor)y_1$$
$$a(x-y_1)-b(x_1-y-\lfloor\frac{a}{b}\rfloor y_1)=0$$
$$\because a\text{和}b\text{都是素数，所以}x=y_1\text{ and }y=x_1-\lfloor\frac{a}{b}\rfloor y_1$$
$$x_1\text{，}y_1\text{的规模比}x,y\text{更小，可以用递归求解，递归终点：与欧几里得算法类似，}b==0,x=1,y=0$$

本体

密钥生成步骤:

1. 随机选择两个不相等的质数p和q（越大越安全）假设选择61,53
2. 计算p个q的乘积n。 n = 61 * 53 = 3233 n的二进制位数为秘钥长度，3233二进制：110010100001（12位）， RSA密钥长度一般是1024位，重要场合为2048位。

3. 计算n的欧拉函数

$$\varphi(n)=\varphi(p)\times\varphi(q)=(p-1)\times(q-1)$$
$$\text{例子：}\varphi(3233)=60\times 52=3120$$

4. 随机选择一个整数e

$$1<e<\varphi(n),e\text{与}\varphi(n)\text{互质。}$$
$$\text{例子里随机选取}17$$

5. $$\text{计算}e\text{对}\varphi(n)\text{的模反}d\text{。}e\times d\equiv 1(mod)\varphi(n)$$
$$\text{利用扩展欧几里得算法解：}e\times x+\varphi(n)\times y=1$$

6. 将n和e封装成公钥，n和d封装成私钥

可靠性检测

$$\text{一共出现了}6\text{个数字：}p,q,n,\varphi(n),e,d,\text{已知}n\text{和}e\text{的情况，推算出}d\text{:}$$
$$1.e\times d\equiv 1(mod)\varphi(n)\text{只有知道}e\text{和}\varphi(n)\text{才能算出}d$$
$$2.\varphi(n)=(p-1)\times(q-1)\text{只有算出}p\text{，}q\text{，才能算出}\varphi(n)$$
$$3.n=p\times q,\text{只有将}p,q\text{因素分解，才能算出}p\text{和}q$$
$$\text{结论，如果}n\text{可以被因式分解，}d\text{就可以算出，私钥被破解。而大整数因式分解非常困难}$$

加密过程

$$\text{加密用（}n,e\text{），信息}m\text{为整数，且}m<n\text{。通过公式}m^e\equiv c(mod)n\text{求出}c$$
$$\text{假设公钥为（}3233,17\text{），}m=65.$$
$$65^{17}\equiv 2790(mod)3233$$

公钥（n, e）只能加密小于n的整数m，如果要加密小于n的整数，一般采取两种方法

1. 将长信息分割成若干短信息
2. 对称性加密算法

解密过程

$$\text{解密用（}n,d),\text{公式为}c^d\equiv m(mod)n$$
$$\text{假设私钥为（}3233\text{，}2753\text{），}c=2790$$
$$2790^{2753}\equiv 65(\text{mod } 3233)$$
$$\text{此时求出加密前的信息}m$$

正确性证明

$$\begin{aligned}
&\text{在 } m<n \text{ 的状况下证明 } m=c^d\%n\text{，就是证明 } c^d\%n-m=0\\
&c^d\%n-m\\
&=(m^e\%n)^d\%n-m\\
&=m^{ed}\%n-m\quad\because a^b\%p=\left((a\%p)^b\right)\%p\\
&=m^{k(p-1)(q-1)+1}\%n-m\\
&=m*\left(m^{k(p-1)(q-1)}-1\right)\%n\\
&\text{当}m\text{与}n\text{互质时，根据费马小定理公式}\\
&a^{p-1}\equiv 1(\text{mod p})\\
&=>(m^{k(q-1)})^{p-1}\equiv 1(\text{mod p})\\
&=>(m^{k(p-1)})^{q-1}\equiv 1(\text{mod q})\\
&=>m^{k(p-1)(q-1)}\equiv 1(\text{mod pq})\\
&=>m^{k(p-1)(q-1)}\equiv 1(\text{mod n})\\
&=>m*\left(m^{k(p-1)(q-1)}-1\right)\%n=0\\
&\text{当}m\text{与}n\text{不互质时，不妨设公因子为}p\text{，则}m=ph_1(h1<q),\text{此时}m\text{和}q\text{互质，根据费马小定理公式}\\
&a^{p-1}\equiv 1(\text{mod p})\\
&=>m^{q-1}\equiv 1(\text{mod q})\\
&=>m^{k(p-1)(q-1)}\equiv 1(\text{mod q})\\
&=>m^{k(p-1)(q-1)}-1=qh_2\\
&=>m*\left(m^{k(p-1)(q-1)}-1\right)\%n=ph_1*qh_2\%n=n*h_1h_2\%n=0,\text{证明完成}
\end{aligned}$$