RSA加密原理

附带一个实现RSA算法的简单Demo

基本过程：

1. 任取两个不同的质数p和q，计算乘积 n = pq （p,q越大越安全）
2. 计算pq的欧拉函数m = ϕ(n)
3. 随机选一个整数e,满足e与m互质，且 1 < e < m
4. 选一整数d，d为e对于$\phi(n)$ 的模反元素， 即 $ed \equiv 1\ mod\ \phi(n)$
5. 公钥为（n,e） 私钥为（n,d）
6. 将明文P加密为密文C. $C \equiv P^e mod\ n$ 且C < n， 即 $C = P^e\ mod\ n$
7. 将密文C解密为明文P. $P \equiv C^d mod\ n$ 且 P < n, 即 $P = C^e\ mod\ n$

涉及到的数学定义

欧拉函数 ϕ(n) 含义：给定任意正整数n，在小等于n的正整数中，有多少个与n互质。

欧拉定理 $a^{\phi(n)} \equiv 1(mod\ n)$ 含义：当两个正整数a与n互质，a的欧拉n（读作fai n）次方被n除的余数为1

费马小定理 $a^{p-1} \equiv 1(mod\ p)$ 含义：欧拉定理的一种特殊情况，p为质数的情况

模反元素 $ab \equiv 1(mod\ n)$ 含义：如果两个正整数a和n互质，那么一定可以找到b，使得ab-1被n除余1

模P相等 含义：a,b满足a mod p = b mod p,则他们模p相等，记做a$\equiv$b(mod p)。 a$\equiv$b(mod p) <==> a = kp +b

消去律 含义：如果gcd(a,p) = 1,则 ab $\equiv$ ac mod p <==> b$\equiv$c mod p

完全余数集合 含义：定义小于n且和n互质的数构成的集合为Zn，这个集合叫做n的完全余数集 合。$|Sn|$ = \phi$(n)

算术基本定理 含义：每个大于1的自然数，要么本身就是质数，要么可以写为2个或以上的质 数的积，而且这些质因子按大小排列之后，写法仅有一种方式。

模反元素存在的证明：

利用欧拉定理， $a \times a^{\phi(n)-1} \equiv 1(mod\ n)$ ，则 $a^{\phi(n)-1}$ 就是a的模反元素。

费马小定理的证明：

因为是欧拉定理的特殊情况，所以也可以用欧拉定理证明。

欧拉定理的证明：

假设n的完全余数集合为Sn={x1,x2,x3……xϕ(n)}，有这样一个集合San = {ax1,ax2,ax3……axϕ(n)}。当i!=j时, xi 与 xj 模n结果不等，根据消去律，axi 与 axj 也模n 不等。则 $Sn \equiv San\ mod\ n$, 把San的a提出来，则 $x1x2\ldots\ldots x\phi(n) * a^{\phi(n)} \equiv x1x2\ldots\ldots x\phi(n)\ mod\ n$ 根据消去律可得 $a^{\phi(n)} \equiv 1\ mod\ n$

欧拉函数的性质：

1. 若n=1, ϕ(n) = 1.
2. 若n为质数，则 ϕ(n) = n-1. 因为质数与小于他的每个数都互质。
3. 若n是为质数的次方。 $\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$. 因为当一个数不是p的倍数都可以与n互质
4. 若n可以分解为两个互质数之积, n=pq. 则$\phi(n) = \phi(p) * \phi(q) = (p-1)(q-1)$. 因为 Zn = {1,2,3……，n-1} - {p,2p,……,(q-1)*p} - {q,2q,……,(p-1)*q} 。 则 $\phi(n) = (n-1) - (q-1) - (p-1) = \phi(p)\phi(q)$
5. 任意正整数n。n可以写成一系列质数的乘积（算术基本定理） $n = p_1^{k1}p_2^{k2}\ldots\ldots p_r^{kr}$.根据4.则 $\phi(n) = \phi(p_1^{k1})\phi(p_2^{k2})\ldots\ldots\phi(p_r^{kr})$ 。再根据3 则 $\phi(n) = p_1^{k1}p_2^{k2}\ldots\ldots p_r^{kr}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\ldots\ldots(1 - \frac{1}{p_r})$

   即 $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\ldots\ldots(1 - \frac{1}{p_r})$. 这也是**欧拉函数的通用计算公式**

准确性：

证明准确性的本质就是证明 $P \equiv C^d mod\ n$ 成立,其中P为原文，C为密文。下面开始推导：

密文C由原文P生成 $C \equiv P^e mod\ n$ ， 则 C = kn + P^e

将C带入要证明的式子 则 $P \equiv (kn + P^e)^d mod\ n$ ==> $P \equiv P^{ed} mod\ n$

再来看看ed的由来，$ed \equiv 1\ mod\ \phi(n)$ 。 则 ed = h$\phi(n)$ + 1

则 证明式继续可以写成 $P \equiv P^{h\phi(n)+1}\ mod\ n$

此时可分为两种情况：

一. Pn互质

则根据消去律直接得到 $P^{h\phi(n)} \equiv 1\ mod\ n$ 。根据欧拉定理，该式一定成立。

二. Pn不互质

因为n=pq,则P=kp或P=kq。这里我们假设P=kp,因为pq为质数，所以P与q互质，

根据欧拉定理可以写成 $P^{\phi(q)} \equiv 1\ mod\ q$ ==> $kp^{\phi(q)} \equiv 1\ mod\ q$

此时 $kp^{\phi(q)} = 1 + yq$ ，等式两边进行$h\phi(p)$ 次幂运算，则 $kp^{h\phi(p)\phi(q)} = (1 + yq)^{h\phi(p)}$

可以得到 $kp^{h\phi(p)\phi(q)} \equiv 1\ mod\ q$

根据消去律 两边乘以 kp 可以写成 $kp^{h\phi(p)\phi(q)} * kp \equiv kp\ mod\ q$

带入可以写成 $kp^{ed} \equiv kp\ mod\ q$

则 $kp^{ed} = kp + tq$ 由于pq互质，可以知道t是可以被p整除的，$t = t^{'}p$

则 $kp^{ed} = kp + t^{'}pq$

则 $m^{ed} = m + t^{'}n$

根据模P相等可知 $m^{ed} \equiv m\ mod\ n$

得证。

安全性：

在加密解密的过程中，我们一共接触了这样六个数字 p q n ϕn e d

其中(n,e)是公钥用于流传, (n,d)是不发送出去的秘钥，最关键的是d，因为一旦d泄露等于秘钥泄露。那么我们根据n，e能否推导出d呢。

先看看d是怎么来的：

$ed \equiv 1\ mod\ \phi(n)$

$d = (k\phi(n) + 1)e$

可以看出推导出d的关键是算出$\phi(n)$, 因为我们知道n=pq，根据欧拉函数性质可以很轻易的算出$\phi(n)$ 不然只能通过暴力循环的方式破解，如果我们选取的pq很小的情况下，很容易被破解，一般rsa秘钥是1024位，证书类的是2048位(n的二进制位数是2048) 。对于现今科技来说分解这样的大整数是非常困难的，以最先进的超级计算机来说破解一个2048位的rsa秘钥，也要60万年，所以说rsa加密还是很安全的。