RSA加密原理

1、准备知识

质数：除了1和自身外，没法被其他自然数整除的大于1的整数 如：2，3，5，7，11，13

互质数：公因数只有1的两个非零自然数，叫做互质数。 如5，12

欧拉函数：小于n的正整数中与n互质的数的数目。 1到7中，与8互质的整数位：1，3，5，7，所以如（φ(8)=4）

性质：

1、给定一个正整数m，如果两个整数a和b满足a-b能够被m整除，即(a-b)/m得到一个整数，那么就称整数a与b对模m同余，记作a≡b(mod m)
如：3≡5 （mod 2)

2、若n为质数则 φ(n)=n-1 注：n为质数，n的因数只有1和n,前n-1个数与n的公因数只有1，所以 φ(n)=n-1 即1，2，3，...，n-1

3、若m,n互质， φ(m * n)=φ(m) * φ(n) 特例当m,n都为质数时，φ(m*n)=φ(m) * φ(n) = (m-1) * (n-1) 备注：因为m, n 为质数，所以mn只与m的倍数，n的倍数不是互质数。

一共有m * n -1 个数， m的倍数有n-1个， n的倍数m-1个，所以φ(m * n)= (m * n-1) - (m-1) - (n-1)=(m-1) * (n-1)

4、若m,n 互质，则 m ** φ(n) ≡ 1 (mod n)

模反元素：若m,n 互质，一定存在一个整数a, 使得：m * a ≡ 1 (mod n)。称a为m对于n的模反元素

2、RSA生成过程

1、随机选择两个极大的不相等质数p, q； 方便计算取p = 13, q = 17

2、计算p与q的乘积n； n = 13 * 17 = 221

3、计算n的欧拉函数φ(n)； φ(n) = （13 - 1） * （17 - 1） = 192

4、随机选择一个整数e，1<e<φ(n)且e与φ(n)互质； e = 5

5、计算e对于φ(n)的模反元素d ed ≡ 1 (mod φ(n)) e * d = k * φ(n) + 1 d = (k * φ(n) + 1)/e k=0,1,2...计算d的数值，直到d为整数; d = 77（k = 2)

6、将n和e封装为公钥， n和d封装为私钥；公钥 221，5 私钥 221，77

3、加密过程

1、加密信息m必须为整数，字符串取ascii值或unicode值, 且m < n； m = 10

2、m ** e ≡ c (mod n) 公钥加密, c为密文; 10 ** 5 % 221 = 108 即c = 108

3、c ** d ≡ m (mod n) 私钥解密, m为明文； 108 ** 77 % 221 = 10 即m = 10

4、加密原理支持：

1、基于已知的公钥，是否能计算出私钥：即已知n,e 求 d

2、因为 d = (k * φ(n) + 1)/e， 所以只需计算出n的欧拉函数值φ(n), 已知n是两个质数p、q的乘积 φ(n) = φ(p * q) = φ(p) * φ(q) = (p-1) * (q-1)

3、难点就是在于n的因数分解。n是一个极大的数，计算机无法对其进行因数分解。