### **RSA加密解密涉及元素**

### N：大整数N，我们称之为模数（modulus）

### p 和 q ：大整数N的两个因子（factor）

### e 和 d：互为模反数的两个指数（exponent）

### c 和 m：分别是密文和明文，这里一般指的是一个十进制的数还有一个就是n的欧拉函数值，在求解d的时候常用

### **RSA算法密钥的产生:**

（1）选择两个满足需要的大素数p和q，计算n=p\*q，IMG_256，其中IMG_257是n的欧拉函数值。

（2）选一个整数e,满足条件1<e<IMG_258,且gcd(IMG_259,e)=1。通过IMG_260，计算出d. 备注：gcd（最大公约数）

（3）以{e,n}为公开密钥，{d,n}为秘密密钥。

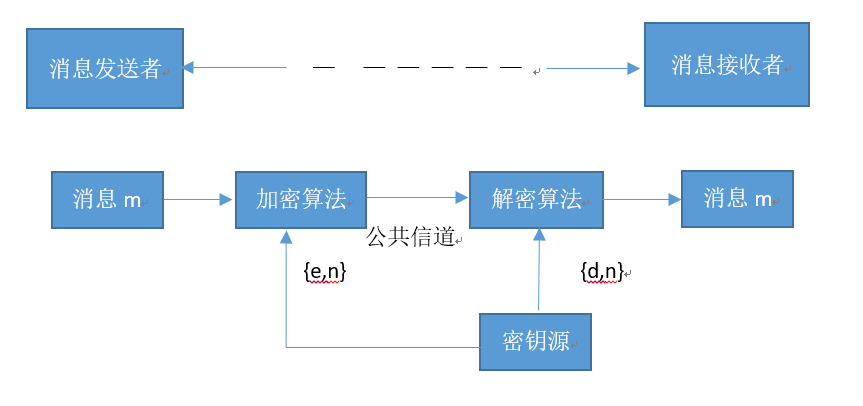
如果两个正整数a和n互质，那么一定可以找到整数b，使得 ab-1 被n整除，或者说ab被n除的余数是1。

IMG_256

这时，b就叫做a的["模反元素"](http://zh.wikipedia.org/wiki/%E6%A8%A1%E5%8F%8D%E5%85%83%E7%B4%A0" \t "https://www.kancloud.cn/kancloud/rsa_algorithm/_blank)。

### **RSA加密解密原理图**

公钥：{e,n}       私钥：{d,n}



d = gmpy2.invert(e,n) # 求逆元，de = 1 mod n