# RSA加密算法

## 一．定义

## 1．三个随机数p、q、r  求私钥

找出三个数p、q、r

p、q是相异的中质数

r 是与 (p-1)(q-1) 互质的数

p, q, r 这三个数便是密钥的最原始的数据

private key = （r，pq）

## 2．求公钥

找出 m, 使得 rm = 1 mod (p-1)(q-1)

 public key  = （m，pq）

## 3．加密过程

a是要加密的资料，

b = a^m mod n, (0 <= b < n)，

b是加密后的密文

## 4．解密过程

a = b^r mod pq (0 <= c < pq)

## 二．示例

用3，11，7这三个数字，对数字2进行加密

