RSA

加密

RSA的加密可以用下面的公式来表示：

$$密文 = 明文^{E} mod N$$

通过公式我们可以知道RSA的密文是通过明文的E次方再对N进行mod运算得到的。这个加密过程只用到了阶乘和取模运算，可以算是非常简单明了了。

简洁的才是最好的，这可能也是RSA算法这么通用的原因吧。

如果知道了E和N，那么就可以得到密文，所以我们把E和N的组合称为公钥，可以这样表示 公钥{E,N}。

如何选择E和N是一个复杂的数学过程，我们会在后面讲到。

解密

先看一下RSA解密的公式：

$$明文 = 密文^{D} mod N$$

通过公式可以看到，明文是通过密文的D次方，再和N取模得到的。这里的N和加密的N是同一个数字。

D和N的组合表示为私钥{D,N}。

N,E,D的生成

生成过程如下：

1. 生成N

生成N的公式如下：

$$N = p * q$$

p和q是两个很大的质数，太小的话容易被破译，太大的话会影响计算速度。通常p和q的大小为1024比特。这两个数是通过伪随机数生成器生成的。伪随机数生成器不能直接生成质数，它是通过不断的重试得到的。

2. 求L

L是一个中间数，它和p，q一样，不会出现在RSA的加密和解密过程。 L的计算公式如下：

$$L = lcm(p-1, q-1)$$

L是p-1和q-1的最小公倍数

3. 求E

E就是用来加密的公钥了，E是一个比1大，比L小的数。并且E和L必须互质。只有E和L互质才能计算出D值。

$$1 < E < L$$

$$gcd(E, L) = 1$$

这里E也是通过伪随机数生成器来生成的。

找到了E和N，我们的公钥就生成了。

4. 求D

计算D的公式如下：

$$1 < D < E$$

$$E * DmodL = 1$$