链滴

RSA 加密的原理——为什么被公钥加密的可以被私钥解密

作者：zqliang

原文链接：https://ld246.com/article/1544619327267

来源网站：链滴

RSA加密的原理——为什么被公钥加密的可以被私钥解密?

目录

引言

在密码学最开始，都是使用的普通加密模式

A 用加密规则加密了字符串m 然后发给B

B 用A的加密规则来解密，得到原始信息m

在这个过程中A必须把自己的加密规则告诉B，否则B无法解密这段密文，但是如果把加密规则也告诉，在传递密钥的过程中，可能就会被拦截获取，这就是最大的问题。

所以，后来又3位数学家提供了一种算法，实现非对称加密，后来算法也以他们三个的首字母命名，R Rivest）S（Shamir ）A（Adleman ）算法。

最开始，我一直理解不了为什么公钥加密的可以被私钥解密，一直停留在使用层面，直到今天看到一博客，才解决了心中的疑惑。

一，RSA 必备数学理论基础

要理解整个rsa的流程，需要以下数学基础

1，互质关系

两个正整数，除1以外，再没有别的公因子。 比如 2 和3， 2和 9。

2，欧拉函数

任意给定正整数n，请问在小于等于n的正整数之中，有多少个与n构成互质关系？（比如，在1到8之，有多少个数与8构成互质关系？）

计算上面这个多少个的函数就被成为欧拉函数，以φ(n)表示。在1到8之中，与8形成互质关系的是1、、5、7，所以 φ(n) = 4。

3，欧拉定理

由上面的欧拉函数可以经过一系列的推导，得到欧拉定理

如果两个正整数a和n互质，则n的欧拉函数 φ(n) 可以让下面的等式成立：

4，特殊情况——费马小定理

欧拉定理的特殊情况，当第二个数n为质数的情况。

假设正整数a与质数p互质，因为质数p的φ(p)等于p-1，

5，模反元素

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

。

比如a = 3 ,n = 5,则一定有（a*b）%n =1 ,即3b -1 = 5y,即一定存在一个数2，可以满足上式。

6,快速幂取模计算

如果有两个大数a,b，a^b可能是一个计算机无法表示的大数，则(a^b)%c的值如何计算?

这里可以使用快速幂取模算法。

java代码如下:

```
/**
● 快速幂取模　计算 (a^b) %c
● @param a
● @param b
● @param c
● @return 计算结果
*/
private static int quick(int a,int b,int c) {
int ans=1;　//记录结果
a=a%c;　//预处理，使得a处于c的数据范围之下
while(b!=0)
{
if((b&1)==1){ //1即是0000000000000001，判断个位是否是1.如果b的二进制位是1，那么我们的果是要参与运算的
ans=(ans*a)%c;
}
b>>=1;　//二进制的移位操作，相当于每次除以2，用二进制看，就是我们不断的遍历b的二进制位
a=(a*a)%c;　//不断的加倍
}
return ans;
}
1
2
3
4
5
6
7
8
```

9
10
11
12
13
14
15
16
17
18
19
20
参考了文章

https://blog.csdn.net/ltyqljhwcm/article/details/53043646

二，RSA实现原理
第一步，选择两个不等质数p,q（实际密钥一般为1024位或2048位）
这里我们选择 61 和53。

第二步，计算乘积n ####
n = p*q = 3233 (二进制110010100001，只有12位)

第三步，计算n的欧拉函数φ(n)
φ(n) = φ(p)*φ(q)= (p-1)(q-1) = 3120 。一个质数p的欧拉函数等于p-1

第四步，随机选择一个整数e，条件是1< e < φ(n)，且e与φ(n) 互质。
取e = 17 (实际应用中，常常选择65537)。

第五步，计算e对于φ(n)的模反元素d。
即找出一个d满足 ed互质，且对于φ(n) 取模为1 ， 即 ed = 1 (mod φ(n))。

即 ed -1 = kφ(n) ，带入上面已知条件：

17d -1 = k3120 即 17x +3120y = 1 (据说可以使用 扩展欧几里得算法求解)

这里直接给出答案 d = 2753。

第六步，将n和e封装成公钥，n和d封装成私钥。
代入本次的推导过程中的数字，n = 3233,e = 17, d=2753。公钥为（3233，17），私钥为（3233，723）。

加密使用 （3233，17），解密使用（3233，2723）。

第七步，分析，私钥的获取

由六可以看出来，公钥和私钥的区别其实只是d，也就是说d的推导是否可以在已知n，e的情况下推出来。

由第五步，要得出d,已知n,e。需要φ(n)。

由第三部，要得出φ(n)，需要p，q。

而已知n=p*q。而n已知，只需要分解n因子即可。

结论：只要n可以被分解，公私玥加密即可被破解。

第八步，n可以被分解吗?

在本例中，3233可以很快被破解，但是实际应用中，两个大质数的积是不容易被分解出来的

例如：

123018668453011775513049495838496272077285356959533479219732245215172640050763657518745202199786469389956474942774063845925192557326303453731548268507910261221429134616704292143116022212404792747377940806653514195974598569021434 3

是以下两个质数的乘积：

a:

334780716989568987860441698482126908177047949837137685689124313889828837938700228761471165253174308773781446799948 9

b:

367460436667995904282446337996279526322791581643430876426760322838157396665127923337341714339681027009279873630891 7

人类已经分解的最大整数（232个十进制位，768个二进制位）。比它更大的因数分解，还没有被报过，因此目前被破解的最长RSA密钥就是768位。而RSA加密一般使用1024位或者2048位，基本可以解为不可破解

三，RSA加密的过程

1，公钥（n,e）加密

所有字符串都可以使用ascil码/unicode值来表示，假设一个字符 m = a，ascii码为65,需要满足 m < n 对他进行加密。

m^e ≡ c (mod n),c为加密字符串

n = 3233,e = 17。 上式可以表示为： (65^17)%3233 = c ,c = 2790。

2,私钥（n,d）解密

(n,d) = (3233,2723) 。在拿到c = 2790之后，进行以下操作：

c^d ≡ m (mod n) 即可得到m 。

推导,m = (2790^2723) %3233 ， 在这里使用 必备知识六中的快速幂取模，可以轻松得到答案，m = 65。

3，证明，

略略略略略略略略略略略略略略略略略略略略略略略略略略略略略略略略略略略略略略略。

四，参考文献

1，http://www.ruanyifeng.com/blog/2013/06/rsa_algorithm_part_one.html

2，http://www.ruanyifeng.com/blog/2013/07/rsa_algorithm_part_two.html

3，https://blog.csdn.net/ltyqljhwcm/article/details/5043646