RSA 算法

Author: Yugang Yang

Introduction

RSA 是一种非对称的分组加密算法，RSA 算法会产生一个公钥和一个私钥，公钥负责对数据加密，是可以公开让其他人知道的密钥，而私钥负责解密，只能让那些可以看到密文真正内容的人持有！

RSA 算法被认为是非常安全的，不过计算速度比 DES 慢很多，RSA 算法的安全性虽然没被证明过，但是要想攻破 RSA 算法，就必须要迈过一道坎，那就是涉及大数（至少 200 位的大数）的因子分解。这是一个极其困难的问题，当代计算机想要得到大数的因子分解是极其花费时间的。

RSA 算法涉及加密和解密两部分，且加密和解密都是围绕着模幂运算的，其模幂运算的基本形式如下：

$$c = m^e \bmod n$$

$$m = \mathrm{c}^d \bmod n$$

m 代表明文数据，c 代表加密后的数据，e 代表用于加密的公钥，d 代表用于加密的私钥，n 是一个不可公开的因子，加密解密中都需要这个因子。

预备知识:

1. 互质数（互素数）：
   这两个数之间的公因数只有 1，就称这两个数互质（互素）
2. 模运算之同余：
   例如整数 a,b，若 a 与 b 同除 m 所得余数相等，则称 a 与 b 对于 m 同余。记为

$$a \equiv b \pmod{m}$$

计算公钥和私钥的方法(暂不涉及原理和思想，仅方法)

step 1.

选择两个位数很大的素数，记为 p 和 q 。同时计算 p 和 q 的乘积，记为 n。 即 $n = p \times q$ 。

ps: 注意这些字母和字母的性质，后面都用得着的！！！！

step 2.

选择一个小的奇数 e. 这个 e 必须满足与(p-1)(q-1)互素的关系。这个 e 将成为用于加密的公钥的一部分。

step 3.

利用前面的 p、q、e 我们可以计算出我们来求一个 d，这个 d 将成为用于解密的私钥的一

部分。

$$\mathrm{d} = e^{-1} \bmod (p-1)(q-1) \tag{0}$$

至于这个 d 为什么是这么求得，我待会说。

P = (e,n) 是公钥，S = (d,n) 是私钥，私钥中得 d 必须要保密，p 和 q 也要保密（通常算法执行完就销毁 p 和 q）

公钥加密，私钥解密方法（暂不涉及原理和思想，仅方法）

我们想对明文 m 进行加密（m 是一长串数字，我们也可以对 m 进行分组，分组加密，这里不具体讨论，就当 m 是一长串数字。如果一开始 m 是字符，那你自己也想办法弄成数字）

对明文 m 加密后得到密文 c。具体操作如下：

$$c = m^e \bmod n \tag{1}$$

对密文 c 解密后得到明文 m。具体操作如下

$$m = c^d \bmod n \tag{2}$$

对于只想知道怎么使用 RSA 的人，阅读到这里就算完了，反正 RSA 就是贼安全，还想继续深入了解下去的，就往下看。

公钥加密和私钥解密的原理和思想

计算公钥 P 和私钥 S 的思想源于**欧拉函数**中的一些有趣的性质。特别是，这些性质允许对模幂运算做一些有用的操作。

我们记欧拉函数位 $\varphi(n)$，其定义为所有小于 n 的正整数里和 n 互素的整数的个数。例如 n=8 时，$\varphi(8)=4$。因为比 8 小的且与 8 互素的整数有 1，3，5，7。

我们现在给出支撑 RSA 算法的有关欧拉函数的三条重要性质（其中性质 3 我们先不讨论它有什么作用，就是先给出来）：

性质 1. 当 x 是素数时

$$\varphi(\mathrm{x}) = x-1$$

性质 2. 欧拉函数是乘法性质（这个我还暂时没整明白，好像是数论里的）的，这意味着如果 p 和 q 是互素的（假如 p 和 q 都是素数，那两个数肯定是互素的了啊），就有 $\varphi(p\times q)=\varphi(p)\times\varphi(q)$。

性质 3. 对于任意小于 n 且与 n 互素的正整数 a，都存在一个关系即

$$a^{\varphi(n)+1} \bmod \ n = a \tag{3}$$

由上面性质 1 和性质 2，我们可以推出一个结论，如果有两个素数 p 和 q，且 $n = p \times q$，则有

$$\varphi(\mathrm{n}) = (p-1)(q-1) \qquad (4)$$

注意：这里的 p-1 和 q-1 是性质 1 推来的。而(p-1)×(q-1)这个乘法操作是由性质 2 推出来的这个公式(3)在后面推导中还会用到。

我们现在知道加密是用公式(1)进行加密，解密是用公式(2)进行解密，那 RSA 算法的核心问题来了，为什么使用公式(2)可以原原本本的将密文还原成明文 m？为什么这个 d 就有用？下面我们给出公式(2)，即解密过程的推导:
我们先给出下面这个式子，注意下面这个式子我没说它等于 m

$$c^d \bmod n$$

我们用公式(1) 替换上面公式的字母 c 得到

$$m^{ed} \bmod n \qquad (5)$$

由公式(0)：

$$\mathrm{d} = e^{-1} \bmod (p-1)(q-1) \ = \ e^{-1} \bmod \varphi(n)$$

我们知道 d 其实和 e 就是模的乘法逆元关系 即：

$$de \equiv 1 (\bmod \varphi(n))$$

所以我们可以很轻易的想到

$$\varphi(n) + 1 = de \qquad (6)$$

然后我们把公式(6)丢进公式(5)里边儿（把公式(5)的 de 替换掉)可以推出：

$$m^{\varphi(n)+1} \bmod n$$

现在关键就是这个 m 怎么判断它和欧拉函数的关系。想要 m 比 n 小很简单，但让 m 与 n 互素，这个怎么搞？如果能判断出 m 与 n 互素且 m 比 n 小，那就可以证明出：
我是不是可以这么认为，我选取 p 和 q 的时候一定要满足 m 与 p×q 互素？？ 这里我存疑

$$m = m^{\varphi(n)+1} \bmod n$$

从而证明出

$$\mathrm{m} = c^d \bmod n$$

Conclusion

攻击者知道了 e 和 n，但是不知道 d，想求出 d 只能通过公式 $\mathrm{d} = e^{-1} \bmod (p-1)(q-1)$ 推出，但是即寻找到 p 和 q，且 p 和 q 是素数，且满足 p×q=n 这个条件。这个寻找的过程极其苦难，原因是 p 和 q 都是几百位的数字，要遍历到猴年马月才能找到这么个 p 和 q 啊。

由 p 和 q 获得 n 简单，由 n 推出 p 和 q 就很难了，就好比把针丢进大海里和从大海里捞

针是一个道理！！！！！

参考文献

https://www.cnblogs.com/idreamo/p/9411265.html
https://blog.csdn.net/q376420785/article/details/8557266