

rsa-math

一：简介

rsa加密算法是一种非对称加密算法。主要原理是利用大整数因式分解十分困难来确保加密的安全性。举一个简单的例子两个素数的乘积 $65537 * 65539 = 4295360521$ ，这样计算很容易，但是想把 4295360521 因式分解成 $65537 * 65539$ 却不太容易。更不用说因式分解以下实际使用的类似以下1024位数字：

```
1252658987214159054406445078393154097005635467245
28072091122281772620164539979309237727718945936762
358969294653557264794356653367016303596899076547
39462923702003832780170203995446888762126421711190
8402487768089808095965495841873677675609617642946
0052758887290894549679799500450956576042711988405
76401001170037
```

二：涉及数学

rsa主要涉及以下数学原理：欧拉函数,费马小定理,欧拉定理

三：数学原理详解

符号说明:

$\gcd(a,m)=x$ 代表a和m的最大公约数为x,假如x为1也代表a和m互质

$a \equiv b \pmod{n}$ 注意是 \equiv 不是 $=$,这就是同余式,表示a模n余数和b模n余数相等,即 $a \% n = b \% n$

3.1欧拉函数

给定一个正整数n，计算1和n之间与n互质的整数个数的计算方法就叫欧拉函数。

数学记号为 $\phi(n)$ ，比如 $\phi(8)=4$ ，因为1到8之间与8互质的有1, 3, 5, 7。

欧拉函数有下面几种情况和性质：

- 1.如果 $n=1$ ，则 $\phi(n)=1$ ，因为1和任何数都互质
- 2.如果 n 为质数则 $\phi(n)=n-1$ ，因为质数和比它小的数都互质
- 3.如果 n 为质数的幂次数，即：

$$n = p^k$$

则：

$$\varphi(n) = p^k - p^{k-1}$$

这是因为只有一个数不包括因数 p 才能和 n 互质，含有因数 p 的数有：

$$1p, 2p, 3p, 4p, \dots, p^{k-1} * p \quad (\text{一共是 } p^{k-1} \text{ 个数})$$

- 4.如果 $\gcd(m, n) = 1$ ，则 $\phi(mn) = \phi(m)\phi(n)$

证明之前假设有两个集合，第一个为小于 mn 且 mn 互质的整数 a 集合为下图左的集合，第二个为满足小于 m 且与 m 互质的整数 b 和满足小于 n 且与 n 互质的整数 c 的组合对集合为下图右边的集合。

$$\left\{ \begin{array}{l} a : 1 \leq a \leq mn \\ \gcd(a, mn) = 1 \end{array} \right\} \rightarrow \left\{ \begin{array}{l} (b, c) : 1 \leq b \leq m, \gcd(b, m) = 1 \\ 1 \leq c \leq n, \gcd(c, n) = 1 \end{array} \right\}$$

$$a \bmod mn \mapsto (a \bmod m, a \bmod n)$$

举一个更具体的例子，假设 $m=4, n=5$ ，则第一个集合有与20互质的数组成 $\{1, 3, 7, 9, 11, 13, 17, 19\}$ ，第二集合由序对 $\{(1, 1), (1, 2), (1, 3), (1, 4), (3, 1), (3, 2), (3, 3), (3, 4)\}$ 组成，刚好都是8个，即 $\phi(45) = \phi(4)\phi(5)$

要证明它只需要证明下面两点：

- (1)第一个集合的不同数对应第二个集合的不同序对
- (2)第二个集合的每个序对都对应第一个集合的某个数

下面先证明(1):取第一个集合的数 a_1, a_2 ,假设它们对应第二个集合相同的序对.则有 $a_1 \equiv a_2 \pmod{m}, a_1 \equiv a_2 \pmod{n}$.

因此 $a_1 - a_2$ 一定能被 m 和 n 整除,然而, m 与 n 互质,所有 $a_1 - a_2$ 一定能被整除 mn .因为 a_1, a_2 等小于 mn ,显然只有 $a_1 = a_2$ 才能满足 $a_1 - a_2 = 0$ 被 mn 整除.这表明 a_1 和 a_2 是第一个集合中相同的数.这就完成(1)的证明.

证明(2)的陈述需要用到"中国剩余定理"来证明.那么下面就说明以下中国剩余定理.

中国剩余定理定义: 设 m 与 n 是整数, $\gcd(m, n) = 1$, b 与 c 是任意整数.则对同余式组 $x \equiv b \pmod{m}$ 与 $x \equiv c \pmod{n}$ 求解,恰好有一个解 $0 \leq x < mn$.

证明:

由 $x \equiv b \pmod{m}$, 设 $x = my + b$ (y 为整数).
 代入第二个同余式得: $my \equiv c - b \pmod{n}$.
 已知 $\gcd(m, n) = 1$ 这里根据欧几里得扩展算法
 可以得到恰有一个解 $y_1, 0 \leq y_1 < n$.则可得一个解 $x_1 = m$
 假设 x_1 不在 0 到 mn 的范围内,
 那么通过 $x_1 + kmn$ 总能找到一个且唯一符合要求的解 x .
 (因为 $\gcd(m, n) = 1$, 那么 x 的解差总是 mn 的倍数)

下面讲讲欧几里得扩展算法是什么:

我们知道可以用欧几里得算法来计算两个数的最大公约数,比如60和22的最大公约数可以这样求:

$$60 = 2 * 22 + 16$$

$$22 = 1 * 16 + 6$$

$$16 = 2 * 6 + 4$$

$$6 = 1 * 4 + 2$$

$$4 = 2 * 2 + 0$$

最后一行余数为0, 所以 $\gcd(60, 22) = 2$

同时我们发现上面的每一行等式其实都可以通过60和22代入计算.设 $a=60, b=22$,那么可以如下代入计算:

代入第一行等式: $a = 2 * b + 16$, 则 $16 = a - 2b$,

以/为主/ 展开/公路上/的上/出/的/去/的/ 的/上/去/的/

4/8

$$3^6 \equiv 1 \pmod{7}$$

然而我们不是进行一般的证明。

首先根据上面的启发,我们证明以下引理:

设 p 是素数, a 是任何整数且 a 不被 p 整除,则
数 $a, 2a, 3a, \dots, (p-1)a \pmod{p}$ 与
数 $1, 2, 3, \dots, (p-1) \pmod{p}$ 相同, 尽管次序不同。

我们采用反证法证明.数列 $a, 2a, 3a, \dots, (p-1)a$ 包含 $p-1$ 个数,显然没有一个数被 p 整除.假设从数列中取两个数 ja 和 ka ,并假设它们同余, $ja \equiv ka \pmod{p}$. 则 $p \mid (j-a)a$, 因为假设 p 不整除 a ,所以 $p \mid j-a$.又因为 $1 \leq j, k \leq p-1$, 则 $|j-k| < p-1$. 所以仅当 $j=k$ 时 $p \mid j-a$.则推出 $a, 2a, 3a, \dots, (p-1)a$ 中的每个数都不同余,同时数列的个数为 $p-1$ 个,所以尽管次序不能不同, $a, 2a, 3a, \dots, (p-1)a$ 和 $1, 2, 3, \dots, (p-1)$ 包含相同的数 \pmod{p} .

利用该引理,很容易推导出费马小定理的证明.即:

$$\begin{aligned} &a, 2a, 3a, \dots, (p-1)a \pmod{p} \text{与数列 } 1, 2, 3, \dots, (p-1) \pmod{p} \\ &\text{所以它们的乘积也相同:} \\ &a * 2a * 3a * \dots * ((p-1)a) \equiv 1 * 2 * 3 * \dots * (p-1) \pmod{p} \\ &\text{简化得:} \\ &a^{p-1} * (p-1)! \equiv (p-1)! \pmod{p} \end{aligned}$$

3.3欧拉定理

$$\text{如果 } \gcd(a, m) = 1, \text{ 则 } a^{\varphi(m)} \equiv 1 \pmod{m}$$

欧拉定理相比费马小定理更一般化了.区别在于模 m 不需要是质数,而费马小定理里的模 p 得是质数.证明的过程其实和费马小定理类似.我们先证明以下引理:

如果 $\gcd(a, m) = 1$, 则数列 $b_1a, b_2a, b_3a, \dots, b_{\varphi(m)}a \pmod{m}$
数列 $b_1, b_2, b_3, \dots, b_{\varphi(m)} \pmod{m}$ 的数相同, 尽管次序不一致

我们采用和费马小定理类似的方式证明:

如果 b 与 m 互质, 则 ab 也与 m 互质. 从而 $b_1a, b_2a, b_3a, \dots, b_{\varphi(m)}a$ 同余于数列 $b_1, b_2, b_3, \dots, b_{\varphi(m)} \pmod{m}$ 中的某个数. 从第一个数列取两个数 b_ja, b_ka , 假设它们同余, 即 $b_ja \equiv b_ka \pmod{m}$. 则 $m \mid (b_j - b_k)a$. 但是 m 和 a 互质, 因此 $m \mid b_j - b_k$. 然而 b_j, b_k 在 1 到 $m-1$ 之间, 因此 $|b_j - b_k| \leq m-1$. 只有 0 能满足 $m \mid (b_j - b_k)$. 从而 $b_j = b_k$. 这说明 $b_1a, b_2a, b_3a, \dots, b_{\varphi(m)}a \pmod{m}$ 中每个数模 m 都不相同. 因此完成了上述引理的证明

以此类推:

$$b_1a * b_2a * b_3a * \dots * b_{\varphi(m)}a \equiv b_1 * b_2 * b_3 * \dots * b_{\varphi(m)} \pmod{m}$$

从而完成欧拉定理的证明.

四：rsa加密算法

4.1 公私钥生成步骤

1. 选择两个不同的质数 p 和 q
2. 计算 p 和 q 的乘积 n
3. 计算 n 的欧拉函数 $\phi(n)$
4. 随机选择一个整数 e , 条件是 $1 < e < \phi(n)$, 且 e 与 $\phi(n)$ 互质。
5. 计算一个和 e 相乘然后模 $\phi(n)$ 为 1 的数 d , 即 $ed \equiv 1 \pmod{\phi(n)}$
6. 把上面生成的 n 和 e 作为公钥, n 和 d 作为私钥.

4.2 加密和解密步骤

首先需要把需要发送的消息转换成数字形式, 假设转化后数字格式消息为 m , 则加密公式为:

$$m^e \pmod{n} \equiv c \pmod{n}, \text{ 即求 } m^e \text{ 模 } n \text{ 余数, 假设结果为 } c$$

解密公式为:

$$c^d \pmod n \equiv m \pmod n, \text{即求 } c^d \text{ 模 } n \text{ 得原消息 } m$$

举一个简单的例子来验证下:(实际位数会比下面的例子大的多)

公私钥等相关数:

```
1 p=61
2 q=53
3 n=p*q=61*53=3233
4 e=17
5 d=2753
```

假设消息m为65,则加密计算结果为

$$m^e \pmod n \equiv 65^{17} \pmod{3233} \equiv 2790 \pmod{3233}, \text{即 } c = 2790$$

解密结果为:

$$c^d \pmod n = 2790^{2753} \pmod{3233} \equiv 65 \pmod{3233}, \text{即 } m = 65$$

五: rsa的正确性

加密公式 $m^e \equiv c \pmod n$, 则c可以写成以下形式:

$$c = m^e - kn$$

将c代入解密公式, 则

$$(m^e - kn)^d \equiv m \pmod n$$

等同于证明 $m^{ed} \equiv m \pmod n$

由于 $ed \equiv 1 \pmod{\varphi(n)}$

所以 $ed = h(\varphi(n)) + 1$

所以 $m^{h\varphi(n)+1} \equiv m \pmod n$

①假设m与n互质, 根据欧拉定理, 则

$$m^{\varphi(n)} \equiv 1 \pmod n$$

那么 $(m^\varphi(n))^h m \equiv m \pmod{n}$, 原式得到证明.

②假设 m 与 n 不互质, 由于 n 等于 pq , 所以 m 要么等于 kp 或 kq
假设 $m = kp$, 那么 kp 与 q 也必然互质, 根据欧拉定理:

$$(kp)^{q-1} \equiv 1 \pmod{q}$$

进一步得到:

$$((kp)^{q-1})^{h(p-1)} kp \equiv kp \pmod{q}$$

进一步整理得:

$$(kp)^{h(q-1)(p-1)} kp \equiv kp \pmod{q}$$

因为 $\varphi(n) = (q-1) * (p-1)$, 所以:

$(kp)^e d = tq + kp$, 此时 t 必然能被 p 整除, 设 $t = t'p$, 则:

$(kp)^e d = t'pq + kp$, 又因为 $m = kp, n = pq$, 所以:

$m^e d \equiv m \pmod{n}$ 成立, 证毕.

参考资料:

[1]阮一峰_RSA算法原理

https://www.ruanyifeng.com/blog/2013/06/rsa_algorithm_part_one.html

https://www.ruanyifeng.com/blog/2013/07/rsa_algorithm_part_two.html