RSA 加密算法的数学原理

Alvin 2019/01/23
idealvin@qq.com

RSA 是一种非对称加密算法，这里只介绍数学原理，不涉及任何其他细节。RSA 的数学基础是费马小定理及欧拉定理，可以参考另一篇文章《费马小定理及其欧拉推广》。

算法流程

1. 找两个大素数 p 与 q，计算乘积：

$$n = pq$$

2. 计算欧拉函数：

$$\varphi(n) = (p-1)(q-1)$$

3. 找一个与 $\varphi(n)$ 互素的正整数 e，然后找一个正整数 d，满足：

$$de \equiv 1 \pmod{\varphi(n)}$$

4. 加密。对于明文 $x < n$(保证解密结果唯一)，计算 x^e 除以 n 的余数，作为密文 y，即有：

$$x^e \equiv y \pmod{n}$$

5. 解密。计算 y^d 除以 n 的余数，即得到明文 x：

$$y^d \equiv x \pmod{n}$$

数学证明

现在对上述算法流程加以解释。第一个问题是，第 3 步中的 d 一定存在吗？令 $\varphi(n)=k$，由于 e 与 k 互素，由欧拉定理有：

$$e^{\varphi(k)} \equiv 1 \pmod{k}$$

容易看出 $d=e^{\varphi(k)-1}$ 即满足条件，因此 d 是一定存在的。

再来看为什么 y^d 除以 n 的余数是 x。由 $x^e \equiv y \pmod{n}$ 及同余性质，容易得到：

$$x^{de} \equiv y^d \pmod{n}$$

即有

$$y^d - x - (x^{de} - x) = kn$$

只需证明 n 整除 $x^{de}-x$，就能证明 n 也整除 y^d-x，即 $y^d \equiv x \pmod{n}$。

当 n 与 x 互素时，由欧拉定理有：

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

由同余性质得到，对任意正整数 k 成立：

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

由上式及 $de \equiv 1 \pmod{\varphi(n)}$, 立即得到：

$$x^{de-1} \equiv 1 \pmod{n}$$

表明 n 整除 $x^{de}-x$。

当 n 与 x 不互素时，由于 $x<n$，且 n 只有素因子 p 与 q，因此 n 与 x 恰好有一个共同的素因子，要么是 p，要么是 q。不妨设 n 与 x 的共同素因子是 p，现在只需要证明 q 整除 $x^{de-1}-1$。容易看出：

$$x^{de-1}-1 = x^{k\varphi(n)}-1 = x^{k(p-1)(q-1)}-1 = \lambda^{q-1}-1$$

其中 $\lambda = x^{k(p-1)}$。由于 q 与 x 互素，从而也与 λ 互素，由费马定理立即得到：

$$\lambda^{q-1} \equiv 1 \pmod{q}$$

这样就得到了完整的证明。

上面只证明了从 $x^e \equiv y \pmod{n}$ 可以推出 $y^d \equiv x \pmod{n}$。反过来也可以从 $y^d \equiv x \pmod{n}$ 推出 $x^e \equiv y \pmod{n}$，证明是类似的。上述 (e,n) 与 (d,n) 可以作为一对密钥，用其中任意一个加密后，都能用另一个解密。通常会公开其中的一个作为公钥，而另一个作为密钥。