RSA加密算法

- 视频: 彻底搞懂“公钥加密算法RSA”的工作原理
- **记号表**
  - m : message, 原始数据
  - e : encrypt, 加密
  - c : cipher, 原始数据加密后得到的密文
  - d : decrypt, 解密
- **欧拉定理**

$$m^{\varphi(n)} \equiv 1 \pmod{n} \tag{Euler's Theorem}$$

  其中, m 与 n 互质, $\phi(n)$ 是欧拉函数,

  表示在 $\leq n$ 的正整数中, 有多少个数与 n 互质.

  比如 $\phi(6) = 2$, 因为 1 和 5 这 2 个数与 6 互质. (注意, 1 和任何数都互质)

- **欧拉定理的性质**:
  1. 对任何质数 p, 有 $\phi(p) = p - 1$

     这是显然的, 比如质数 7 和 1,2,3,4,5,6 均互质.
  2. $\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$

     其中 $p_1, \cdots, p_k$ 是 n 的全体素因子.

     证明见这里.
  3. 对于互质的 p 和 q ,

     有 $\varphi(p * q) = \varphi(p) * \varphi(q)$

     这是上一条性质的直接推论.

     > 比如令 $p = 17, q = 23$
     >
     > 则 $\varphi(391) = \varphi(17 * 23) = \varphi(17) * \varphi(23) = 16 * 22 = 352$

- **对欧拉定理进行变形**:

  首先, 两端同时取 $k \in \mathbb{N}^+$ 次幂:

$$m^{k\varphi(n)} \equiv 1^k \pmod{n} \tag{同时取k次幂}$$

然后, 两端同时乘以 m:

$$m^{k\varphi(n)+1} \equiv m \pmod n \tag{同时乘以m}$$

换成计算机的模运算写法, 即:

$$m^{k\varphi(n)+1} \mod n = m \tag{对任意的正整数k均成立}$$

上面的式子可以形象理解为:

$$m\text{经过一番折腾之后, 又回到}m.$$

于是, 如果有两个正整数 e 和 d 满足:

$$ed = k\varphi(n) + 1 \tag{1}$$

记密文 c

$$m^e \mod N \triangleq c \tag{2}$$

则有解密过程

$$\begin{aligned} c^d \mod N &= m^{ed} \mod n \\ &= m \end{aligned} \tag{3}$$

也就是说, (1)式把原始数据 m 加密为密文 c ,

而(2)式可以通过私钥 d 把密文 c 还原为原始数据 m .

事实上, 把(1)式写成

$$d = \frac{k\varphi(n) + 1}{e} \tag{4}$$

容易看出, 只要固定了 n 和公钥 e , 我们就可适当选取 k 来让私钥 d 是一个整数.

- 回到加密算法本身, 我们把上述的 e 和 n 作为加密用的公钥(public key),

  而计算出的 d 作为解密用的私钥(private key)

  例:

  比如我们取 $n = 391 (= 17 * 23), e = 3$ 作为公钥,

  (这里 n 是一个我们已知其质因数分解的大数)

  (而 e 应该是一个比较小的数, 且与 $\varphi(n)$ 互质, 因为如果不互质的话, 无论 k 取什么, d 都不可能是整数)

  则可以计算出私钥 $d = \dfrac{k\varphi(n)+1}{e} = \dfrac{5*352+1}{3} = 587$ (这里k可以取2,5,8,... 因此d并不唯一. 我们这里取k=5)

  注意, 对于自己而言, 因为我们知道 $391 = 17 * 23$,

  所以利用欧拉函数的性质, 可以快速求解 $\varphi(391) = 16 * 22$

  然而对于其它人而言, 由于他们不知道这个大数的质因数分解, 因此无法在短时间内求解欧拉函数值.

  而这个信息不对等正是算法的关键.

  对于我们需要加密的数据 m, 比如令 $m = 233 < n$

  则为了加密数据 m , 我们需要用到公钥 n 和 e 来对其加密, 进而得到密文 c (cipher):

$$
\begin{aligned}
c &= m^e \mod n \\
&= 233^3 \mod 391 \\
&= 96
\end{aligned}
$$

  为了得到原文 m, 我们需要用到私钥 d , 进而还原出原文 m :

$$
\begin{aligned}
m &= c^d \mod 391 \\
&= 96^{587} \mod 391 \\
&= 233
\end{aligned}
$$