

RSA 加密算法

Ron Rivest, Adi Shemir, Len Adleman

可厉害的土豆

加密过程

步骤	说明	描述
1	选择一对不相等且足够大的质数	p, q
2	计算 p, q 的乘积	$n = p * q$
3	计算 n 的欧拉函数	$\varphi(n) = (p-1) * (q-1)$
4	选一个与 $\varphi(n)$ 互质的整数 e	$1 < e < \varphi(n)$
5	计算出 e 对于 $\varphi(n)$ 的模反元素 d	$de \bmod \varphi(n) = 1$
6	公钥	$KU = (e, n)$
7	私钥	$KR = (d, n)$

明文 M

加密 $M^e \bmod n = C$

密文 C

解密 $C^d \bmod n = M$

3. 计算 n 的欧拉函数

- **欧拉函数**是小于 n 的正整数中与 n 互质的数的数目。
- **互质**是公约数只有1的两个整数，叫做互质整数。
- **质数**是指在大于1的自然数中，除了1和它本身以外不再有其他因数的自然数。

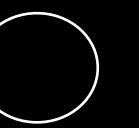
3. 计算n的欧拉函数

- 如果n可以分解成2个互质的整数之积，那么n的欧拉函数等于这两个因子的欧拉函数之积。
- 即若 $n=p*q$ ，且p,q互质，则 $\varphi(n)=\varphi(p*q)=\varphi(p)*\varphi(q)$ 。

4. 计算模反元素d

如果两个正整数 e 和 $\varphi(n)$ 互质，那么一定可以找到一个整数 d ，使得 $ed-1$ 被 $\varphi(n)$ 整除，或者说 ed 除以 $\varphi(n)$ 所得余数为1。

此时， d 就叫做 e 的模反元素。



加密 $M^e \bmod n = C$

解密 $C^d \bmod n = M$

谢谢

可厉害的土豆