RSA 算法原理

作者：whitespur
原文链接：https://ld246.com/article/1537456182047
来源网站：链滴
许可协议：署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

讲的最好的文章

RSA算法原理 (http://)http://www.ruanyifeng.com/blog/2013/06/rsa_algorithm_part_one.html

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

简单来说RSA加密的前提是：大整数的因数分解，是一件非常困难的事情。目前，除了暴力破解，还有发现别的有效方法。

维基百科这样写道：

"对极大整数做因数分解的难度决定了RSA算法的可靠性。换言之，对一极大整数做因数分解愈困难，SA算法愈可靠。

假如有人找到一种快速因数分解的算法，那么RSA的可靠性就会极度下降。但找到这样的算法的能性是非常小的。今天只有短的RSA密钥才可能被暴力破解。到2008年为止，世界上还没有任何可靠攻击RSA算法的方式。

只要密钥长度足够长，用RSA加密的信息实际上是不能被解破的。"

公私钥产生过程：

https://blog.csdn.net/q376420785/article/details/8557266

假设Alice想要通过一个不可靠的媒体接收Bob的一条私人讯息。她可以用以下的方式来产生一个**公钥**一个**私钥**：

1. 随意选择两个大的 质数p_和_q，p_不等于_q，计算_N_=pq。
2. 根据 欧拉函数，求得r = (p-1)(q-1)
3. 选择一个小于 r 的整数_ e_，求得 e 关于模 r 的 模反元素，命名为d。（模反元素存在，当且仅当与r互质）
4. 将_ p 和 q _的记录销毁。

_(N,e)是公钥，(N,d)_是私钥。Alice将她的公钥(N,e)传给Bob，而将她的私钥(N,d)藏起来。