<https://www.zhihu.com/question/20874499>

**RSA 1024和AES 256，这两种加密算法理论上哪种更安全？**

默认排序​

[坚果云](https://www.zhihu.com/org/jian-guo-yun-34)

[**坚果云**](https://www.zhihu.com/org/jian-guo-yun-34)

已认证的官方帐号

83 人赞同了该回答

回答这个问题，需要先了解下AES和RSA的区别，前者属于**对称加密**，后者属于**非对称加密**。

## 1、对称加密

对称加密就是加密和解密使用同一个密钥。

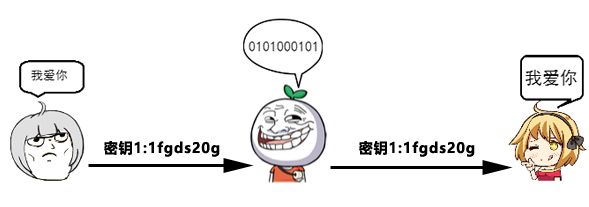
用数学公示表示就是：

▲加密：Ｅk(P) = C

▲解密：Ｄk(C) = P

这里E表示加密算法，D表示解密算法，P表示明文，C表示密文。

是不是看起来有点不太容易理解？看下图：



看过间谍局的知友们一定知道电台和密码本的功能。潜伏里面孙红雷通过电台收听到一堆数字，然后拿出密码本比对，找到数字对应的汉字，就明白上级传达的指令。而军统的监听台没有密码本，只看到一堆没有意义的数字，这就是对称算法的原理。

***AES就属于对称加密****，常见的对称加密方法还有DES、3DES、Blowfish、RC2以及国密的SM4。*

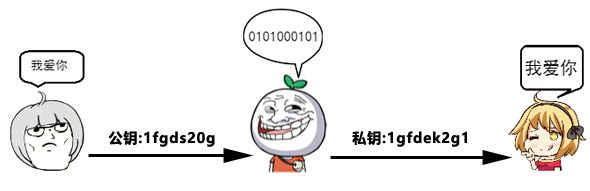
## 2、非对称加密

对称加密快而且方便，但是有个缺点——密钥容易被偷或被破解。非对称加密就可以很好的避免这个问题。

非对称算法**把密钥分成两个**，一个自己持有叫**私钥**，另一个发给对方，还可以公开，叫**公钥**，用公钥加密的数据只能用私钥解开。

▲加密： E公钥(P) = C

▲解密:：D私钥(C) = P



这下就不用担心密钥被对方窃取或被破解了，私钥由自己保管。

非对称加密算法核心原理其实就是设计一个数学难题，使得用公钥和明文推导密文很容易，但根据公钥、明文和密文推导私钥极其难。

***RSA****就属于非对称加密，非对称加密还有Elgamal、背包算法、Rabin、D-H、ECC（椭圆曲线加密算法）以及国家商用密码SM2算法。*

## 3、AES和RSA

AES和RSA都很安全，至少在目前的计算机体系结构下，没有任何有效的攻击方式。量子计算机时代，RSA有一定的破绽，因为利用shro's algorithm，量子计算机穷举计算质因子速度可以提高N个数量级，能够在有限的时间内破解RSA密钥。AES256至少目前并没有什么明显的漏洞。

**AES作为对称加密技术，加密速度很快。**现在高端一点的CPU都带有AES-NI指令，可以极快的完成加密和解密。

举例来说，坚果云存储系统采用了intel 的AES-NI加速，在采用AES加密和解密的时候，  
单核的性能可以超过 1GB Byte/秒，非常非常快，很适合对大量数据进行加解密。

***摘自：***[*坚果云团队版 - 办公云盘|文件管理|协同办公|企业网盘|安全备份*](https://link.zhihu.com/?target=http%3A//www.jianguoyun.com/s/team/security)

但是AES作为对称加密技术，如何安全的分发密钥是一个难题。通过任何方式传递密钥都有泄密的风险。当然，目前我国高大上的量子通信技术或许能很好的解决这个问题。

**RSA作为非对称加密技术的代表，**加解密的速度其实相当慢，只能对小块的数据进行加解密。但是其非对称的特点，满足公钥可以随处分发，只有公钥能解密私钥加密的数据，只有私钥能解密公钥加密的数据。所以很适合用来进行密钥分发和身份验证，这两个应用场景刚好相反。

1）用于对称秘钥分发的场景，其他人用公钥加密对称的秘钥，那么只有授权人才持有私钥，因此才能解密获得对应的秘钥，解决了AES密钥分发的难题；

2）对于身份验证的场景，授权人用私钥加密一段指令，其他人用公钥解密对应的数据，验证对应的指令与之前约定的某些特征一致（例如，这段话必须使用四川口音，像是坚果云CEO

[@韩竹](https://www.zhihu.com/people/21f55fcf7b9aace2b6fc46f097660f7e)

的标准四川口音==），如果一致，那么可以确认这个指令就是授权人发出的。

**相关趣闻轶事：**

RSA除了是一个伟大的发明，被免费开放给所有互联网用户使用。它的发明者还以此成立了一家名为[RSA Security](https://link.zhihu.com/?target=https%3A//en.wikipedia.org/wiki/RSA_Security)的网络安全公司，这家公司最后被EMC高价收购。这是德艺双馨的伟大证明， 是“又红又专”的典范。  
RSA的算法是以三个发明者的名字命名的，三位都是成功的数学家，科学家和企业家，其中的排名第一Ron Rivest，有非常多的杰出贡献。

RSA是整个互联网数据安全的基础，与光纤处于同样基础和重要的方式。**大部分的加密和解密的应用都是同时应用RSA和AES。**

## 总结

1. 破解加密的难度除了跟**加密方法**有关，还跟**密钥长度**以及**加密模式**有很大的关系，就拿AES来说，有AES128和AES256（**代表密钥长度**），显然AES256的安全性能比AES128更高，而AES又要四种模式：ECB、CBC、CFB、OFB（**代表加密模式**）。
2. RSA1024是属于非对称加密，是基于大整数因式分解难度，也就是两个质数相乘很容易，但是找一个大数的质因子非常困难。量子计算机时代，RSA有一定的风险，具体可以参考：[超链接](https://link.zhihu.com/?target=https%3A//en.wikipedia.org/wiki/Shor%2527s_algorithm)
3. AES256目前没有明显的漏洞，唯一的问题就是如何安全的分发密钥。
4. 现在大部分的加密解密都是同时应用RSA和AES，发挥各自的优势，使用RSA进行密钥分发、协商，使用AES进行业务数据的加解密。

[编辑于 2017-07-31](https://www.zhihu.com/question/20874499/answer/205039590)

83​添加评论

​分享

​收藏​感谢收起

[姜政伟](https://www.zhihu.com/people/prcjzw)

[**姜政伟**](https://www.zhihu.com/people/prcjzw)

网络安全，人文历史。

7 人赞同了该回答

各有所长。前者是非对称加密，是PKI/CA的基础，是业内普遍使用的，加密效率较后者低，存在一些破解的报道，虽然在成本的限制下可行性不高。AES256是美国NIST在几种加密算法竞赛中选出来的对称加密算法，是用于取代(3)DES的，原名为Rijndael加密法，破解的报道相对少些。

[编辑于 2014-05-12](https://www.zhihu.com/question/20874499/answer/16571340)

7​添加评论

​分享

​收藏​感谢

知乎用户

**知乎用户**

不务正业...

6 人赞同了该回答

如果单纯从密码学上讲，要实现与AES256相当的加密强度，RSA加密算法长度要达到16384位，另外RSA1024目前已经不被认为是安全的加密算法了。

[发布于 2014-05-12](https://www.zhihu.com/question/20874499/answer/25502664)

6​2 条评论

​分享

​收藏​感谢

[李天天](https://www.zhihu.com/people/li-tian-tian-13)

[**李天天**](https://www.zhihu.com/people/li-tian-tian-13)

一个蛋疼的处女座文艺理工单身直男

1 人赞同了该回答

其实我觉得这样的比较意义不大。RSA和AES分别为非对称加密和对称加密的代表，各有各的用途。  
纵然，如前几位知友所述，RSA1024的安全性和效率较AES256低，但对称加密算法再好，其能被使用的前提也是双方握有相同的秘钥。而非对称加密是业界普遍采用的交换秘钥的方式。  
所以更多的情况下，两者是协同工作的，不存在谁好谁坏的问题。

[发布于 2017-03-13](https://www.zhihu.com/question/20874499/answer/151426998)

1​4 条评论

​分享

​收藏​感谢

匿名用户

**匿名用户**

1 人赞同了该回答

从安全强度来说，1024rsa只有80bit等效密钥强度。而且目前大数分解的能力已经迫近，1024已经不可靠了

256bit的aes还是靠谱的，安全使用的话没问题。（当然那些作死的用法另当别论）

[发布于 2015-02-16](https://www.zhihu.com/question/20874499/answer/39909015)

1​1 条评论

​分享

​收藏​感谢

[吴龙](https://www.zhihu.com/people/wu-long-57-98)

[**吴龙**](https://www.zhihu.com/people/wu-long-57-98)

AES算法更安全，但是二者使用场景不同

[发布于 2017-07-02](https://www.zhihu.com/question/20874499/answer/192328091)

0​添加评论

​分享

​收藏​感谢

知乎用户

**知乎用户**

低端人口

加密后的数据膨胀让人很是烦恼。。

[发布于 2017-03-22](https://www.zhihu.com/question/20874499/answer/152921215)

0​1 条评论

​分享

​收藏​感谢

知乎用户

**知乎用户**

U2，网络安全从业者

7 人赞同了该回答

这两种加密算法所适用的业务场景不同，没有可比性。

RSA是非对称加密算法，一般用于密钥交换、数字签名，或者保护动态随机对称加密密钥。  
RSA效率低下，只能用于对少量内容的加密（如动态随机对称加密密钥、HASH摘要）。  
就RSA本身的安全性而言，RSA 768已于2009年被破解，RSA 1024理论上只是略高于RSA 768，因此也被认为不适合使用了，业务场景中推荐RSA 2048或以上。

AES是对称加密算法，包含三种密钥长度（128、192、256），目前都是安全的，商业用途使用AES 128目前是足够的，AES 256更好。  
AES主要的业务场景是对内容进行加密，效率高。

把RSA和AES进行比较，好比锤子和斧头那个更好一样。

利用好各自的特点，组合使用，效果更佳。  
比如数字证书（密钥协商时用RSA来传递，确定密钥后用AES或其它对称加密来传输）、比如微软的RMS系统（随机AES密钥对内容加密，然后用RSA传递到服务器保护起来），都是组合使用这两种算法的。

===========广告时间==========  
本人运营维护微信公众号：网络安全生命周期 （Security\_SDL），欢迎关注~  
共同探讨网络安全体系建设~

[编辑于 2015-12-31](https://www.zhihu.com/question/20874499/answer/79406499)

7​添加评论

​分享

​收藏​感谢

[find goo](https://www.zhihu.com/people/find-goo)

[**find goo**](https://www.zhihu.com/people/find-goo)

MOV AX, BX

2 人赞同了该回答

都不安全。

如果我用1pb的硬盘，存储了世界基于正态分布的密码库，通过存储来换时间。

撒1kb盐才是王道。

[编辑于 2016-10-21](https://www.zhihu.com/question/20874499/answer/127744881)