> 面试题：

1. > Q：MD5加密是对称还是非对称加密？

> A：MD5严格上不能算是加密算法，因为能加密就能解密，而经过MD5后的消息是不能再解密的，不可逆，因此MD5不算是加密算法。

MD5算法

> MD5计算，对原始消息（Message）做有损压缩计算，无论消息（输入值）的长度字节是多少，是一亿字节、1个字节、还是0个字节，都会生成一个固定长度（128位/16字节）的消息摘要（输出值）。

- > 不可逆
- > 单项性
- > 恒定性
- > 不可预测性

> 作用：密码的保存等。

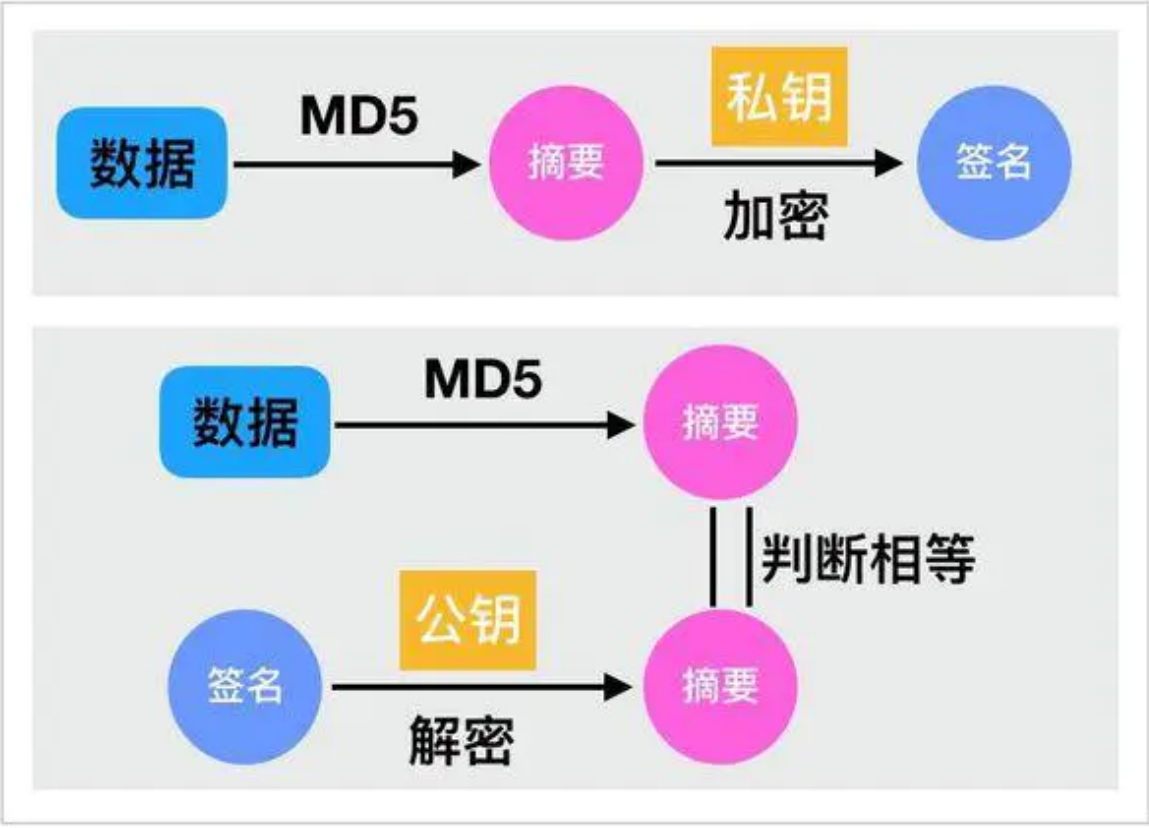
非对称加密和对称加密在加密和解密过程、加密解密速度、传输的安全性上都有所不同，具体介绍如下：

1、加密和解密过程不同

对称加密过程和解密过程使用的同一个密钥，加密过程相当于用原文+密钥可以传输出密文，同时解密过程用密文-密钥可以推导出原文。但非对称加密采用了两个密钥，一般使用公钥进行加密，使用私钥进行解密。

2、加密解密速度不同

对称加密解密的速度比较快，适合数据比较长时的使用。非对称加密和解密花费的时间长、速度相对较慢，只适合对少量数据的使用。



3、传输的安全性不同

对称加密的过程中无法确保密钥被安全传递，密文在传输过程中是可能被第三方截获的，如果密码本也被第三方截获，则传输的密码信息将被第三方破获，安全性相对较低。

非对称加密算法中私钥是基于不同的算法生成不同的随机数，私钥通过一定的加密算法推导出公钥，但私钥到公钥的推导过程是单向的，也就是说公钥无法反推导出私钥。所以安全性较高。

非对称加密和对称加密的区别：

1、加密算法不同

在非对称加密中使用的主要算法有：RSA、Elgamal、背包算法、Rabin、D-H、ECC（椭圆曲线加密算法）等。

在对称加密中使用的主要算法有：DES（Data Encryption Standard）、3DES（Triple DES）、AES（Advanced Encryption Standard）、Blowfish等。

2、加密安全性不同

对称加密的通信双方使用相同的秘钥，如果一方的秘钥遭泄露，那么整个通信就会被破解。

而非对称加密使用一对秘钥，一个用来加密，一个用来解密，而且公钥是公开的，秘钥是自己保存的，不需要像对称加密那样在通信之前要先同步秘钥。非对称加密与，其安全性更好。

4、流程图不同

非对称加密流程图：

对称加密流程图：

4、加密耗时不同

非对称加密使用一对秘钥，一个用来加密，一个用来解密，这样加密和解密花费时间就会更长长。

对称加密中加密方和解密方使用同一个密钥，加密解密的速度比较快，耗时短，适合数据比较长时的使用。

https://www.jianshu.com/p/de50d1489359