<https://mp.weixin.qq.com/s/OTFFG0qL6KVDTZgALN30sA>

# MD5 到底是不是加密算法？

在回答这个问题之前，我们先分别来了解一下两个知识点：

什么是 MD5 算法？

什么是加密算法？

## 一、MD5算法

MD5 即 Message-Digest Algorithm 5（信息-摘要算法5），用于确保信息传输完整一致。是计算机广泛使用的杂凑算法之一，主流编程语言普遍已有 MD5 实现。

将数据（如汉字）运算为另一固定长度值，是杂凑算法的基础原理，MD5 的前身有 MD2 、MD3 和 MD4 。

MD5 是输入不定长度信息，输出固定长度 128-bits 的算法。经过程序流程，生成四个32位数据，最后联合起来成为一个 128-bits 散列。

基本方式为，求余、取余、调整长度、与链接变量进行循环运算，得出结果。

MD5 计算广泛应用于错误检查。在一些 BitTorrent 下载中，软件通过计算 MD5 来检验下载到的碎片的完整性。

## 二、加密算法

百度百科：加密，是以某种特殊的算法改变原有的信息数据，使得未授权的用户即使获得了已加密的信息，但因不知解密的方法，仍然无法了解信息的内容。

维基百科：在密码学中，加密（英语：Encryption）是将明文信息改变为难以读取的密文内容，使之不可读的过程。只有拥有解密方法的对象，经由解密过程，才能将密文还原为正常可读的内容。

## 三、对比

也就是说，MD5 算法和加密算法都可以将信息转换为另外一种内容。

但是，MD5 算法对比 加密算法 缺少了解密过程。

事实上，使用 加密算法 加密后的消息是完整的，并且基于解密算法后，可以恢复原始数据。

而 MD5 算法 得到的消息是不完整的，并且通过摘要的数据也无法得到原始数据。

所以，**MD5 算法不是加密算法！**