MD5工作原理

MD5的功能是：

1. 输入任意长度的信息，经过处理，输出为128位的信息（数字指纹）
2. 不同的输入得到的不同的结果（唯一性）
3. 根据128位的输出结果不可能反推出输入的信息（不可逆）

MD5的算法过程：

对MD5算法简要的叙述可以为：MD5以512位分组来处理输入的信息，且每一分组又被划分为16个32位子分组，经过了一系列的处理后，算法的输出由四个32位分组组成，将这四个32位分组级联后将生成一个128位散列值。

1. 填充：如果输入信息的长度(bit)对512求余的结果不等于448，就需要填充使得对512求余的结果等于448。填充的方法是填充一个1和n个0。填充完后，信息的长度就为N*512+448(bit)
2. 记录信息长度：用64位来存储填充前信息长度。这64位加在第一步结果的后面，这样信息长度就变为N*512+448+64=(N+1)*512位。
3. 装入标准的幻数（四个整数）：标准的幻数（物理顺序）是（A=(01234567)16，B=(89ABCDEF)16，C=(FEDCBA98)16，D=(76543210)16）。如果在程序中定义应该是（A=0X67452301L，B=0XEFCDAB89L，C=0X98BADCFEL，D=0X10325476L）
4. 四轮循环运算：循环的次数是分组的个数（N+1）