**作业 汇编实现MD5类核心函数**

**一、背景：**

MD5即Message-Digest Algorithm 5,是广泛使用的的哈希算法。MD5可以生成任意一个输入字串（甚至可以是一个文件）的“数字指纹”，对输入的微小改动都会直接导致数字指纹的巨大变化。

二、要求

在MD5类中，存在4个偏重算数逻辑运算的函数

static void FRound(DWORD& a, DWORD& b, DWORD& c, DWORD& d, DWORD mj, DWORD s, DWORD ti);

static void GRound(DWORD& a, DWORD& b, DWORD& c, DWORD& d, DWORD mj, DWORD s, DWORD ti);

static void HRound(DWORD& a, DWORD& b, DWORD& c, DWORD& d, DWORD mj, DWORD s, DWORD ti);

static void RRound(DWORD& a, DWORD& b, DWORD& c, DWORD& d, DWORD mj, DWORD s, DWORD ti);

1、使用在线编译器<https://godbolt.org> ，对上述4个函数的内部实现用内嵌汇编实现，目标：尽可能减少内存操作，尽可能使用简洁的汇编指令序列，函数功能不变。

2、文件命名：学号\_MD5.cpp和 学号\_MD5.h

使用线编译器的建议步骤：

1、调整在线编译器源代码类型为C++

2、拷贝MD5.hpp文件内容到源代码区

3、拷贝MD5.cpp文件内容到源代码区

4、在线编译器会报错，这时，在源代码区找到并删除#include "MD5.hpp"

5、在源代码区最下面，增加main函数。至此，在线编译器不在报错

6、调整汇编显示区的编译器为“x86-64 gcc 12.2”

7、用asm()和AT&T汇编修改源代码，编译测试

8、拷贝源代码区类声明部分代码到 学号\_MD5.hpp文件

9、拷贝源代码区类实现部分代码到 学号\_MD5.cpp文件，并在适当位置加入对 学号\_MD5.hpp 的include语句