DEBUG 下修改内存空间

【实验目的】

1．学会在 window 系统下启动 DEBUG 程序。
2．掌握 DEBUG 程序的常用命令。
3．学习如何用 DEBUG 程序跟踪调试。

【实验内容】

调试实验一中的 hello.exe 程序，并修改字符串，输出自己的学号。

【需求分析】

修改内存中的内容，并输出。

【概要设计】

本次实验用到的主要命令有 T、D、E、G、R。
-T: 单步调试
-R: 查看寄存器的内容
-D: 查看内存区域的内容 [起始地址][L 长度]
-E: 修改内存区域的内容 [起始地址]
-G: 执行汇编命令直到断点

【详细设计】

```
DATAS SEGMENT
    STRING    DB "Hello World!",13,10,'$'
DATAS ENDS


CODES SEGMENT
    ASSUME CS:CODES,DS:DATAS
START:
    MOV AX,DATAS
    MOV DS,AX
    LEA DX,STRING
    MOV AH,9
    INT 21H
    MOV AH,4CH
    INT 21H
CODES ENDS
    END START
```

【实验结果】

```
D:\>DEBUG HELLO.EXE
-T

AX=076A  BX=0000  CX=0021  DX=0000  SP=0000  BP=0000  SI=0000  DI=0000
DS=075A  ES=075A  SS=0769  CS=076B  IP=0003   NV UP EI PL NZ NA PO NC
076B:0003 8ED8          MOV     DS,AX
-T

AX=076A  BX=0000  CX=0021  DX=0000  SP=0000  BP=0000  SI=0000  DI=0000
DS=076A  ES=075A  SS=0769  CS=076B  IP=0005   NV UP EI PL NZ NA PO NC
076B:0005 8D160000      LEA     DX,[0000]                       DS:0000=6548
-T

AX=076A  BX=0000  CX=0021  DX=0000  SP=0000  BP=0000  SI=0000  DI=0000
DS=076A  ES=075A  SS=0769  CS=076B  IP=0009   NV UP EI PL NZ NA PO NC
076B:0009 B409          MOV     AH,09
-E 076A:0000
076A:0000  48.53   65.41   6C.31   6C.38   6F.32   20.32   57.35   6F.35
076A:0008  72.33   6C.38   64.24

-G
SA18225538
```

【问题讨论】

1、 实验结论：成功修改内存中的内存并输出到屏幕上；
2、 实验改进：上图中的 T 连续执行了 3 次，或许可以使用-T=3 一步完成。
3、 理解思考：既然只要知道内存地址就可以修改内存中的内容，那么我是不是可以根据操作系统内核的地址用汇编语言修改它的代码区和数据区？我猜测内核应该有保护机制。