

汇编语言与逆向技术实验报告

Lab2- dec2hex

学号：2112514 姓名：辛浩然 专业：信息安全、法学

一、 实验内容

编写汇编程序 dec2hex.asm，编译成 dec2hex.exe。dec2hex.exe 的功能是将 Windows 命令行输入的十进制无符号整数，转换成对应的十六进制整数，输出在 Windows 命令行中，如图 1 所示。

输入的十进制无符号整数的范围是 0 到 4294967295 ($2^{32}-1$)。

输出对应的十六进制整数，对应的范围是 00000000h 到 FFFFFFFFh。

二、 实验步骤

- 1.使用 StdIn 函数获得用户输入的十进制整数。
- 2.用户输入的十进制数对应的 ASCII 编码字符串存储在内存中，编写过程 dec2dw，将 ASCII 字符串转换成 DWORD 数据。
- 3.编写过程 dw2hex，将 DWORD 数据转换成十六进制数的 ASCII 字符串。
- 4.使用 StdOut 函数在 Windows 命令函中输出十六进制整数的 ASCII 字符串。
- 5.使用 ml 将 dec2hex.asm 文件汇编到 dec2hex.obj 目标文件。
- 6.使用 link 将目标文件 dec2hex.obj 链接成 dec2hex.exe 可执行文件。

三、 实验代码

```
.386
.model flat, stdcall
option casemap:none
include D:\masm32\include\windows.inc
include D:\masm32\include\kernel32.inc
include D:\masm32\include\masm32.inc
includelib D:\masm32\lib\kernel32.lib
includelib D:\masm32\lib\masm32.lib
```

```
.data
    decstr      db 20 DUP(0)
    res         db 8 DUP(48)
    ten         dd 10
    decnum      dd 0
    str_input   db "Please input a decimal number(0~4294967295): ", 0
    str_output  db "The hexadecimal number is : ", 0
```

```
.code
dec2dw PROC
    invoke StdOut, addr str_input
    invoke StdIn, addr decstr, 20
    mov     edx, 0
    mov     ecx, 0
    mov     eax, 0
L1:
    mov     dl, [decstr+ecx]
    sub     dl, 48
    mov     ebx, eax
    shl     ebx, 3
    shl     eax, 1
    add     eax, ebx
    add     eax, edx
    inc     ecx
    mov     dl, [decstr+ecx]
    cmp     dl, 0
    jnz     L1
    mov     decnum, eax
    ret
```

```
dec2dw ENDP
```

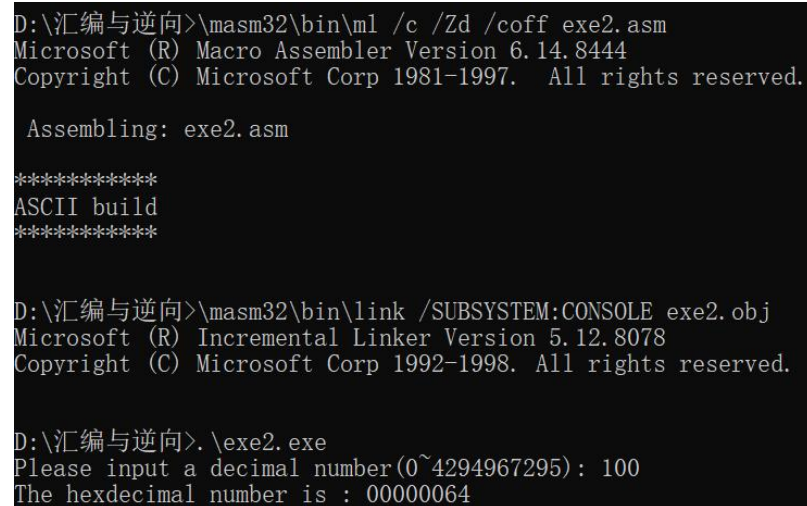
```
d2hex PROC
    call    dec2dw
    mov     edx, 7
    mov     ecx, 0
L2:
    mov     eax, decnum
    mov     ebx, ecx
    shl     ebx, 2
L3:
    cmp     ebx, 0
    je      L4
    shr     eax, 1
    dec     ebx
```

```

        jmp     L3
L4:
        and     eax,15
        cmp     eax,9
        jle     L5
        add     eax,87
        jmp     L6
L5:
        add     eax,48
L6:
        mov     [res+edx],al
        inc     ecx
        cmp     edx,0
        je      L7
        dec     edx
        jmp     L2
L7:
        invoke StdOut, addr str_output
        invoke StdOut, addr res
        invoke ExitProcess,0
d2hex ENDP
end d2hex

```

四、实验截图



```

D:\汇编与逆向>\masm32\bin\ml /c /Zd /coff exe2.asm
Microsoft (R) Macro Assembler Version 6.14.8444
Copyright (C) Microsoft Corp 1981-1997. All rights reserved.

Assembling: exe2.asm

*****
ASCII build
*****

D:\汇编与逆向>\masm32\bin\link /SUBSYSTEM:CONSOLE exe2.obj
Microsoft (R) Incremental Linker Version 5.12.8078
Copyright (C) Microsoft Corp 1992-1998. All rights reserved.

D:\汇编与逆向>.\exe2.exe
Please input a decimal number(0~4294967295): 100
The hexadecimal number is : 00000064

```

五、实验分析

1. dec2dw 过程

该过程将 ASCII 字符串转换成 DWORD 数据，代码注释逐行解释如下：

```
dec2dw PROC
```

```

        invoke StdOut, addr str_input
        invoke StdIn,addr decstr,20
        mov     edx,0
        mov     ecx,0
;ecx 是处理的位数，从最高位开始处理
        mov     eax,0
;eax 用来存放每轮计算结束后的结果（包括最终结果）
L1:
        mov     dl,[decstr+ecx]
;处理第 ecx 位，将第 ecx 位赋值给 dl，即 edx 的低位
        sub     dl,48
;dl=dl-48，将 ASCII 码变成数字
        mov     ebx,eax
        shl     ebx,3
        shl     eax,1
        add     eax,ebx
;向左三位相当于乘 8，向左一位相当于乘 2，二者加起来就实现了乘 10。这些步相当于是
        eax=eax*8+eax*2=eax*10
        add     eax,edx
;加上提取出来的个位
        inc     ecx
;取下一个字符
        mov     dl,[decstr+ecx]
        cmp     dl,0
;如果到字符串末尾，那程序结束；如果未到末尾，循环 L1
        jnz     L1
        mov     decnum,eax
        ret

```

dec2dw ENDP

;该过程的思路，举一例子，输入 1234，第一轮处理第 0 位，转换成数字后 dl=1，eax=0*10+1；第二轮处理第 1 位，dl=2，eax=1*10+2；第三轮，eax=12*10+3；...以此类推

2.dw2hex 过程

该过程将 DWORD 数据转换成十六进制数的 ASCII 字符串，代码逐行解释如下：

d2hex PROC

```

        call    dec2dw
        mov     edx,7
;除了正在处理的位，还要处理的位数
        mov     ecx,0
;正在处理的位的序号
L2:

```

```

        mov     eax,decnum
;恢复 eax 的值
        mov     ebx,ecx
        shl     ebx,2
;正在处理的位的序号左移两位，相当于乘 4
L3:
        cmp     ebx,0
        je      L4
;ebx 为 0 的时候跳转 L4
;ebx=0，跳转 L4。ebx 乘 4 后的数值是 4 的整数倍。
        shr     eax,1
        dec     ebx
;ebx 乘 4 后的数值是 4 的整数倍，要减到 0，那么 eax 需要向右移动 4 的整数倍。
        jmp     L3
;ebx=0，eax 不动；ebx=1，eax 向右移动 4 位；ebx=2，eax 向右移动 8 位...每轮删掉
16 进制最后的一个数
L4:
        and     eax,15
;按位与操作 只保留了最后一个十六进制位
        cmp     eax,9
;判断是数字还是字母
        jle     L5
;如果小于等于 9，是数字，跳转 L5
        add     eax,87
;是字母，加 87 转为 ASCII 码
        jmp     L6
L5:
        add     eax,48
;数字减 48 转为 ASCII 码
L6:
        mov     [res+edx],al
;把转换成的 ASCII 码存到 res 中
        inc     ecx
;处理下一位
        cmp     edx,0
        je      L7
;还剩 0 位要处理时结束，跳转 L7
        dec     edx
;要处理的位数减一
        jmp     L2
L7:
        invoke  StdOut, addr str_output
        invoke  StdOut, addr res
        invoke  ExitProcess,0

```

d2hex **ENDP**

3.源代码的编译和链接过程说明

①编译：

```
\masm32\bin\ml /c /Zd /coff exe2.asm
```

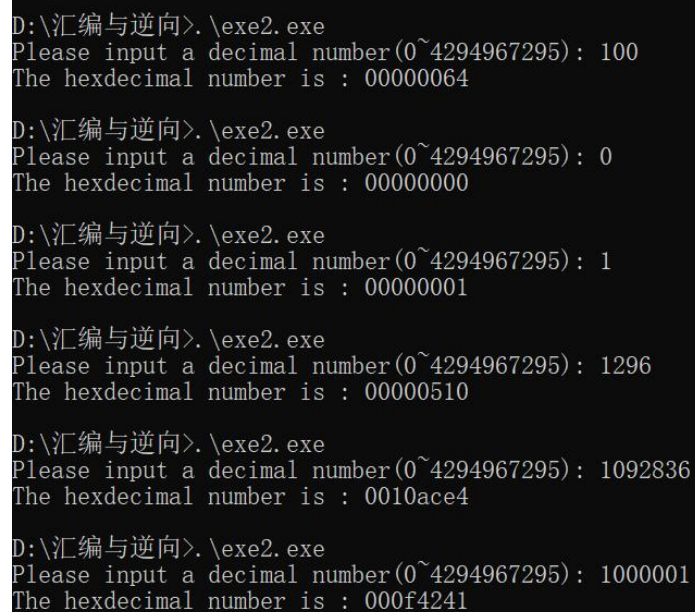
；用汇编程序（\masm32\bin\ml.exe）对 exe2.asm 进行汇编，形成目标文件（.obj）。其中：
/c 是只汇编、不链接的指令，/Zd 是在目标文件中生成行号信息，即目标文件指令与源代码中代码行的对应关系，/coff 是生成 microsoft 公共目标文件格式的文件。

②链接：

```
\masm32\bin\link /SUBSYSTEM:CONSOLE exe2.obj
```

；用链接程序（\masm32\bin\link.exe）对 exe2.obj 进行链接，形成可执行文件（.exe）。
/SUBSYSTEM:CONSOLE 是生成命令程序的指令。

4.测试说明



```
D:\汇编与逆向>.\exe2.exe
Please input a decimal number(0~4294967295): 100
The hexadecimal number is : 00000064

D:\汇编与逆向>.\exe2.exe
Please input a decimal number(0~4294967295): 0
The hexadecimal number is : 00000000

D:\汇编与逆向>.\exe2.exe
Please input a decimal number(0~4294967295): 1
The hexadecimal number is : 00000001

D:\汇编与逆向>.\exe2.exe
Please input a decimal number(0~4294967295): 1296
The hexadecimal number is : 00000510

D:\汇编与逆向>.\exe2.exe
Please input a decimal number(0~4294967295): 1092836
The hexadecimal number is : 0010ace4

D:\汇编与逆向>.\exe2.exe
Please input a decimal number(0~4294967295): 1000001
The hexadecimal number is : 000f4241
```

经测试，能够正常输出输入的十六进制整数的 ASCII 字符串。