汇编语言与逆向技术实验报告

Lab2-dex2hex

学号：1911406

姓名：丁彦添

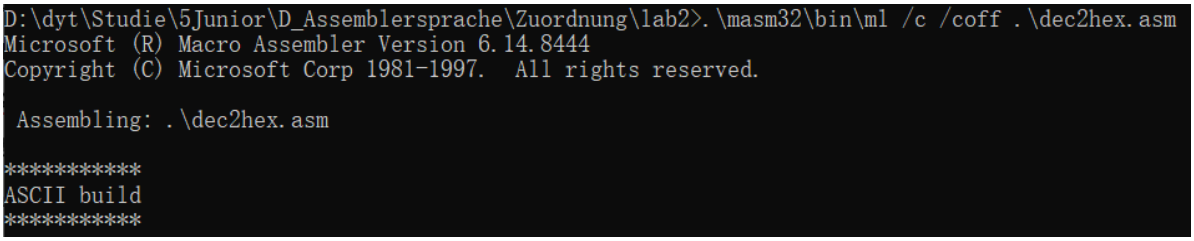
dec2hex.asm源代码

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

.data
    str1 BYTE "Please input a decimal number(0~429496725): ", 0
    str2 BYTE "The hexdecimal number is: ", 0
    str3 BYTE "0123456789ABCDEF", 0
    num1 BYTE 10 DUP(0), 0
    num2 DWORD 0
    d1 DWORD 0
    tmp1 BYTE 10h
    tmp2 DWORD 0Ah
    tmp3 DWORD 1
    tmp4 BYTE 0, 0
    oneAH BYTE 0
    oneECX DWORD 0
    oneESI PDWORD 0
.code
start:
main PROC
    invoke StdOut, addr str1
    invoke StdIn, addr num1, 10;input a decimal number
    call dec2dw; decimal number transmit into DWORD
    invoke StdOut, addr str2; output string str2
    call Dw2hex; transmit DWORD into hexdecimal number
    invoke ExitProcess, 0;end
main ENDP

;ax是eax的低16位。
;ah是ax的高8位
;al是ax的低8位
dec2dw PROC; decimal number -> DWORD
    mov esi, OFFSET num1
L1:
    inc d1;calculate num of bits, store in d1
    inc esi
    mov eax, [esi];store addr of esi into eax
```

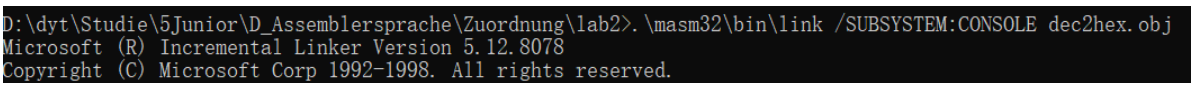
```
    cmp al, 0;if al==0, jump to L2, else jump to L1
    je L2
    jmp L1
L2:
    mov ecx, d1;store d1 into ecx as loop times of L3
L3:
    sub num1[ecx-1], '0'
    mov eax, 0;init eax
    mov al, byte ptr num1[ecx-1]
    mul tmp3; eax = tmp3 multiplies eax
    add num2, eax
    xchg eax, tmp3;exchange eax and tmp3
    mul tmp2
    xchg tmp3, eax
    loop L3
    ret
dec2dw ENDP


Dw2hex PROC; DWORD to hexdecimal
    mov esi, offset num2+3
    mov ecx, 4
L4:
    mov ax, 0
    mov al, byte ptr[esi];store data esi point to into al
    div tmp1
    mov oneAH, ah
    mov oneECX, ecx
    xchg esi, oneESI
    mov esi, offset str3
    mov tmp4, al
    movzx ebx, tmp4
    add esi, ebx
    mov bl, byte ptr[esi]
    mov tmp4, bl
    invoke StdOut, addr tmp4
    mov esi, offset str3
    mov ah, oneAH
    mov tmp4, ah
    movzx ebx, tmp4
    add esi, ebx
    mov bl, byte ptr[esi]
    mov tmp4, bl
    invoke StdOut, addr tmp4
    xchg oneESI, esi
    mov ecx, oneECX
    dec esi
    loop L4
    ret
Dw2hex ENDP


end start
end main
```

编译和链接过程说明

使用命令`.\masm32\bin\ml /c  /coff  .\dec2hex.asm`可以对编写好的汇编代码进行编译成 obj 文件。（如下图）

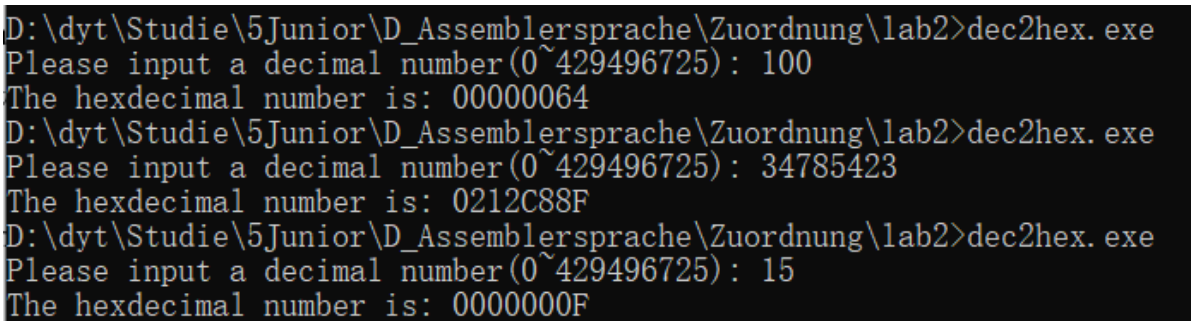


编译成 obj 文件后，使用命令`.\masm32\bin\link /SUBSYSTEM:CONSOLE .\dec2hex.obj`将 obj 文件链接成 exe 可执行文件。（如下图）



测试说明

使用命令`.\dec2hex.exe`运行可执行程序，测试发现结果符合预期。（如下图）



实验中踩过的坑

- 原本在 DWORD 转十六进制过程我写的 dw2hex，结果报编译错误：`error A2111: conflicting parameter definition`，结果将其改成 Dw2hex 编译才能通过，说明 dw2hex 这是 x86 系统保留的关键字。
- 在连接时直接赋值实验指导书上的命令，导致出现错误`LINK : fatal error LNK1146: no argument specified with option "/SUBSYSTEM:"`。经检查，原因是SUBSYSTEM:CONSOLE`中间不能有空格，将空格删去即可链接成功。