

**课 程 实 验 报 告**

**课程名称： 汇编语言程序设计实验**

**实验名称： 实验七 跟踪与反跟踪程序设计**

**实验时间： 2016-5-3，14：00-17：30 实验地点： 南一楼804室73号实验台**

**指导教师： 张勇 专业班级：计算机科学与技术201409班**

**学 号： U201414813 姓 名： 唐礼威**

**同组学生： 无 报告日期： 2016年 5 月 7日**

**原创性声明**

  本人郑重声明：本报告的内容由本人独立完成，有关观点、方法、数据和文献等的引用已经在文中指出。除文中已经注明引用的内容外，本报告不包含任何其他个人或集体已经公开发表的作品或成果，不存在剽窃、抄袭行为。

特此声明！

学生签名：

日期：

成绩评定

|  |  |  |
| --- | --- | --- |
| 实验完成质量得分（70分）（实验步骤清晰详细深入，实验记录真实完整等） | 报告撰写质量得分（30分）（报告规范、完整、通顺、详实等） | 总成绩（100分） |
|  |  |  |

指导教师签字：

                    日期：

**目录**

[1 实验目的与要求 1](#_Toc451728003)

[2 实验内容 1](#_Toc451728004)

[3 实验过程 2](#_Toc451728005)

[3.1 任务1 2](#_Toc451728006)

[3.1.1 设计思想及存储单元分配 2](#_Toc451728007)

[3.1.2 流程图 2](#_Toc451728008)

[3.1.3 源程序 3](#_Toc451728009)

[3.1.4 实验步骤 8](#_Toc451728010)

[3.1.5 实验记录 8](#_Toc451728011)

[3.2 任务2 9](#_Toc451728012)

[3.2.1 设计思想及存储单元分配 9](#_Toc451728013)

[3.2.2 流程图 9](#_Toc451728014)

[3.2.3 源程序 9](#_Toc451728015)

[3.2.4 实验步骤 9](#_Toc451728016)

[4 体会 9](#_Toc451728017)

[参考文献 10](#_Toc451728018)

# 实验目的与要求

(1) 熟悉跟踪与反跟踪的技术；

(1) 提升对计算机系统的理解与分析能力。

# 实验内容

任务1：数据加密与反跟踪

在实验二的基础上，增加查询前输入密码的功能，密码不对则程序退出，只有密码正确之后才能完成后续的功能。密码采用密文的方式存放在数据段中。各科成绩也以密文方式存放在数据段中。加密方法自选。

可以采用计时、中断矢量表检查、堆栈检查、间接寻址等方式中的一种或多种方式反跟踪。

成绩表中要有自己的名字和各科成绩（密文存放）。

提示：为了使源程序的数据段中定义的密码、学生姓名、各科成绩能在汇编之后变成密文，可以使用数值运算符（参见教材P48）对变量的初始值进行变换。例如，如果想使语文成绩90分变成密文，加密算法是与密钥字符“W”做异或运算，则可写成：

YUWEN DB 90 XOR ‘W’

任务2：跟踪与数据解密

解密同组同学的加密程序，获取该同学的成绩。

注意：两人一组，每人实现一类加密与反跟踪方法，把执行程序交给对方解密。如何设计反跟踪程序以及如何跟踪破解的，是本次实验报告中重点需要突出的内容。

# 实验过程

## 任务1

### 设计思想及存储单元分配

此次实验主要是两部分内容：1.实现正常功能模块（即实验2所做的内容）2.加密模块：要求提供验证密码功能（加密算法设计：使用的是简单的算数逻辑运算，具体是将姓名与s异或，成绩与Bat异或，密码为Bat，采用函数(X-29H)\*3对保存的密码进行编码；反跟踪功能设计：在各个模块中穿插反跟踪代码，防止破解人员利用td破解）。

### 流程图



### 源程序

.386

STACK SEGMENT USE16 STACK

DB 200 DUP(0)

STACK ENDS

;

DATA SEGMENT USE16

NUM DD 3

RADX DD 10

BASE DB 10

D1 DB 0DH,0AH,'STUDENT NAME:$'

D2 DB 0DH,0AH,'GRADE:$'

PROMPT db 0dh, 0ah, 'please enter password: $'

MSG db 0dh, 0ah, 'please input target name : $'

BUF DB 'z' XOR 's','h'XOR 's','a'XOR 's', 7 DUP(0)

DB 100 XOR 'B' ,85 XOR 'a', 80 XOR 't', ?

DB 'l' XOR 's','i'XOR 's','s'XOR 's','i' XOR 's',6 DUP(0)

DB 80 XOR 'B', 98 XOR 'a', 70 XOR 't',?

PWD DB 3 XOR 'C' ;密码串的长度为3，采用与常数43H异或的方式编码成密文

DB ('B' -29H)\*3 ;真实密码为Bat。采用函数(X-29H)\*3对保存的密码进行编码。

DB ('a' -29H)\*3

DB ('t' -29H)\*3

DB 0A1H,5FH,0D3H ;用随机数填充密码区到6个字符，防止破解者猜到密码长度

;

IN\_PWD DB 7 ;输入密码，最大长度6个字符

DB ?

DB 7 DUP(0)

;

INPUT DB 11

DB ?

DB 11 DUP(0)

P1 DW PASS1 ;地址表

E1 DW OVER

P2 DW PASS2

P3 DW PASS3

DATA ENDS

;

CODE SEGMENT USE16

ASSUME CS:CODE,DS:DATA,SS:STACK

START: MOV AX,DATA

MOV DS,AX

LEA DX,PROMPT

MOV AH,9

INT 21H

LEA DX,IN\_PWD ;输入密码字符串

MOV AH,10

INT 21H

cli ;计时反跟踪开始

mov ah,2ch

int 21h

push dx ;保存获取的秒和百分秒

MOV CL,IN\_PWD+1 ;比较输入的串长与密码长度是否一样

XOR CL,'C'

SUB CL,PWD

MOVSX BX,CL

ADD BX,OFFSET P1

mov ah,2ch ;获取第二次秒与百分秒

int 21h

sti

cmp dx,[esp] ;计时是否相同

pop dx

jz OK1 ;如果计时相同，通过本次计时反跟踪

mov bx,offset E1 ;如果计时不同，则把转移地址偏离P1

OK1: mov bx,[bx]

cmp word ptr cs:[bx],0B60FH ;是否是PASS1处的指令，其实是用于判断前面比较的

;串长是否相同

jz OK2

jmp E1

OK2: jmp bx

db 'How to go' ;定义的冗余信息

PASS1: MOVZX CX,IN\_PWD+1

cli ;堆栈检查反跟踪

push P2 ;PASS2的地址压栈

MOV SI,0

MOV DL,3

pop ax

mov bx,[esp-2] ;把栈顶上面的字（PASS2的地址）取到

sti

jmp bx ;如果被跟踪，将不会转移到PASS2

db 'i donot know！'

PASS2: MOVZX AX,IN\_PWD+2[SI] ;比较密码是否相同。把输入的串变成密文，与保存的密文比较

SUB AX,29H

MUL DL

CMP AL,PWD+1[SI]

JNZ ERR2

INC SI

DEC CX

CMP CX,0

JNE PASS2

JMP PASS3

ERR2: MOV EBX,OFFSET P1

MOV EDX,1

JMP WORD PTR [EBX+EDX\*2] ;指向OVER

db 'YES,get it'

;

PASS3: ;　正常功能区

lea dx, msg ; 输出提示信息 - 请输入姓名

mov ah, 9h

int 21h

lea dx, input ; 读入学生姓名, 以 '$' 符号结尾

mov ah, 0ah

int 21h

lea esi, input+2

lea edi, buf

xor ebx, ebx

xor ecx, ecx

search\_loop:

cmp ecx, num

jge search\_finish

xor eax, eax

search\_inner:

cmp eax, radx

jge search\_finish

mov dl, [esi + eax]

xor dl, 's'

cmp [edi + ebx], dl

jnz search\_next

cmp byte ptr [edi + ebx + 1], 0

jz search\_finish

inc eax

inc ebx

jmp search\_inner

db 'the future will be better tomorrow'

search\_next:

inc ecx

imul ebx, ecx, 14

jmp search\_loop

db 'welcome to hust'

search\_finish:

xor ebx, ebx

output:

sub ebx,ecx

imul bx,14 ; 根据目标学生下标值, 找到分数缓冲区首地址

mov si,0

mov ax, 0

mov dx, 0

mov al,buf+10[bx+si]

xor al,in\_pwd+2[si]

add ax, ax

inc si

mov dl, buf+10[bx+si]

xor dl,in\_pwd+2[si]

add ax, dx ; al = zh \* 2 + ma

inc si

mov dl, buf+10[bx+si]

xor dl,in\_pwd+2[si]

sar dl, 1

add ax, dx ; al = zh \* 2 + ma + en / 2

sal ax, 1 ; al = 2 \* al

mov dx, 7

idiv dl ; al = al / 7

inc si

mov buf+10[bx+si], al ; avg = al ( al / 3.5)

push ax

mov dl, 0ah

mov ah, 2h

int 21h

mov dl, 0dh

mov ah, 2h

int 21h

pop ax

cmp al, 90 ; switch 语句

jge gradea

cmp al, 80

jge gradeb

cmp al, 70

jge gradec

cmp al, 60

jge graded

jmp gradee

db 'my sunshine'

gradea: mov dl, 41h

mov ah, 2h

int 21h

jmp pass3

gradeb: mov dl, 42h

mov ah, 2h

int 21h

jmp pass3

gradec: mov dl, 43h

mov ah, 2h

int 21h

jmp pass3

graded: mov dl, 44h

mov ah, 2h

int 21h

jmp pass3

gradee: mov dl, 45h

mov ah, 2h

int 21h

jmp pass3

OVER:

MOV AH,4CH

INT 21H

CODE ENDS

END START

### 实验步骤

1. 绘制程序流程图；

2. 根据程序流程图，编写shiyan7.asm；

3. 编译、链接源程序，生成可执行目标文件shiyan7.exe;

4. 运行shiyan7.exe，检查程序具有正常功能;

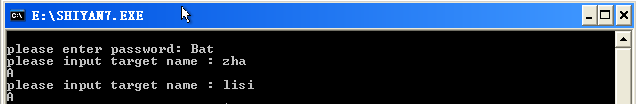
5. 输入正确密码后，键入学生姓名，可以正常查询出成绩；

6. 输入错误密码后，程序直接终止运行；。

### 实验记录

（包括实验条件、输入/输出、错误和修改等信息的记录）

1. 实验环境条件：P3 1GHz，256M内存；WINDOWS XP命令行窗口；EDIT.EXE 2.0；MASM.EXE 6.0； LINK.EXE 5.2; TD.EXE 5.0。
2. 输入密码Bat后程序运行如下



当输入错误的密码时程序直接停止运行，当破解人员在td里调试时，由于执行两条指令的时间远大于执行程序的时长，通过检测这一时差，若两次计时调用间时长过长，直接结束程序，阻止了破解人员进一步破解；当破解人员利用反汇编工具运行程序时，栈顶数据的值被修改，可通过此检测程序是否是在反汇编环境下执行；若程序在异常环境下运行，则立即终止程序。

## 任务2

### 设计思想及存储单元分配

在td里单步执行待破解的程序，可以很直观地获得程序的执行流程和完成的操作。若碰到反跟踪程序段，配合设置断点的方法，绕过反跟踪程序段设置的陷阱。

### 流程图

无

### 源程序

无

### 实验步骤

1. 运行TD，开始破解密码；

2. 当遇到疑似反跟踪代码时，若其中含有功能代码，则在其尾部设置断点，直接运行过去；

3. 当遇到疑似反跟踪代码时，若其中不含功能代码，纯粹为反跟踪代码，则直接修改IP寄存器的值，跳过此段代码的执行;

4. 在验证密码与计算成绩处，找出加密手段；在相关数据段，找出暗文数据;

5. 利用暴力破解法,编写破解脚本，结合加密手段与暗文，得到明文数据;

6. 记录明文数据，并利用源代码进行验证，查看是否成功破密;

# 体会

这次实验初步熟悉了一些跟踪与反跟踪手段：中断向量检测、计时检测、堆栈检测。提升了自己对计算机系统的理解与分析能力，懂得如何进行简单的数据加密。这次实验收获很大，相信对今后的编程有很大的帮助。

# 参考文献

[1] 王元珍等.80x86汇编语言程序设计.版本(第1版)

[2] 王晓虹等.汇编语言程序设计教程.版本(第1版)