

姓名: 210923

学号: 2019091013

分数:

1 第三章 控制

写出下面函数Func1汇编代码对应的C程序, 其中参数1为x, 参数2为y:

Func1:

cmpq %rsi, %rdi

jge .L2

leaq 3(%rsi), %rdi

jmp .L3

.L2:

leaq(%rdi,%rdi,4), %rsi

addq %rsi, %rsi

.L3:

leaq(%rdi,%rsi), %rax

ret

if($x \geq y$)

{ $y = 10x$

}

else

{ $x = y + 3$

}

return $x + y$

2 第三章 多重数组+lea指令

对于数组int

保存在rsi, j保存在rdx中, 请完成以下代码中的空缺

leaq (, %rsi,), %rax

leaq (, ,), %rax

movl (, ,), %eax

$x_A = rdi$

$i = rsi$

$j = rdx$

$x_A + 4(5i + j)$

$x_A + 20i + 4j$

B[8][5], 需要将B[i][j]保存到eax中, 数组起始地址在rdi, i

(%rsi, %rsi, 4), %rax

(%rdi, %rax, 4), %rax

(%rax, %rdx, 4), %rax

5i

$x_A + 20i$

$x_A + 20i + 4j$

3 第三章 数组+函数+乘法的移位实现

已知int P[M][N]和int Q[N][M]

有以下函数 int addfun(int i, int j){

对应汇编代码如下, 请问M N各自是多少?

addfun:

movl %edi, %edx

shl \$2, %edx

addl %esi, %edx

movl %esi, %eax

shll \$2, %eax

addl %eax, %edi

movl Q(%rdi,4), %eax

addl P(%rdx,4), %eax

ret

return P[i][j]+Q[j][i];

rdi = i

rsi = j

$edx = 4i + j$

$eax = j \times 4$

$edi = j \times 4 + i$

int

↓

$eax = Q + 4(4j + i)$

$Q[1][4]$

$eax = P + 4(4i + j)$

$P[4][1]$

$M = 4, N = 1$

4 第三章 union+结构体

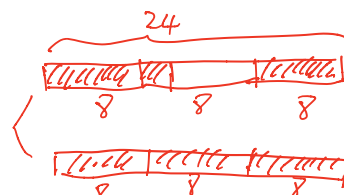
union a1{

struct { int * b1; char c1; long d1 } str1;

double data[3];

}

请问按照默认的对齐方式, 上述a1占用多少字节空间?



union, $3 \times 8 = 24$ 字节

5 第三章 结构体+函数+控制

已知node 结构体定义如下struct node{ long a; struct node *next;}

请对以下init函数进行逆向分析, 写出其C代码

Init:

movl \$12, %eax

jmp .TestExprStat

.Loop:

addq (%rdi), %rax

movq 8(%rdi), %rdi

.TestExprStat:

testq %rdi, %rdi

jne .Loop

ret

$rdi = node$

struct: 16

$eax = 12$

$rdi = 16[rdi + 8]$

$rdi = *node$

$rax += *(node)$

$rdi = 16(node + 8)$
 $= *node - next$

int sum = 12

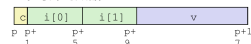
struct node * p

where (p != 0)

{ sum += p -> a

p = p -> next

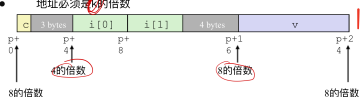
- 未对齐的数据



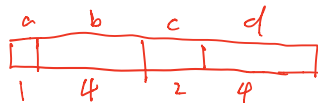
```
struct S1 {
    char c;
    int i[2];
    double v;
} *p;
```

· 对齐数据

- 原始数据类型占k字节
- 地址必须是2的位数的倍数



11. 湊布局



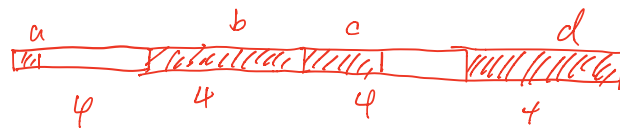
a: 1
b: 5
c: 7
d: 11

6 第三章 结构体

```
struct{
```

```
1 char a;;
8 char *b;;
2 short c;
4 int d;
```

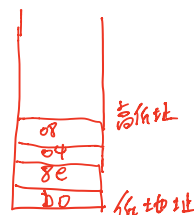
对齐布局



a: 1
b: 8
c: 10
d: 16

请问在紧凑布局和对齐布局中a/b/c/d字段的偏移量各是多少？

子端



高位 低位
08048e60
b78e0408

7 第三章. 堆栈破坏问题

对于函数void echo(){ char buf[8]; gets(buf);puts(buf); }对应的汇编代码如下:

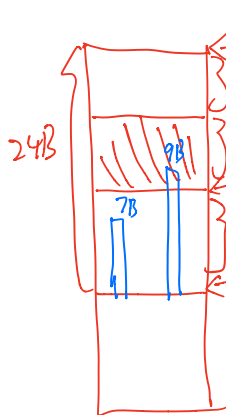
小端

echo:

```

subq    $24,%rsp    24 5#
movq    %fs:40,%rax
movq    %rax,8(%rsp)
xorl    %eax,%eax
movq    %rsp,%rdi
call    gets
movq    %rsp,%rdi
call    puts
movq    8(%rsp),%rax
xorq    %fs:40,%rax
je       .L9
call    __stack_chk_fail
addq    $24,%rsp
ret

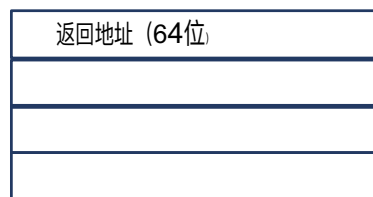
```



echo
的栈帧



的栈帧



```
%rsp
```



%rsp

观察代码, 判定该函数是否具有堆栈破坏的检测能力? 如果%fs:38地址开始存放了0x00/01/02/03/04/05/06/07/08/09/0a/0b/0c/0d/0e/0f。请问刚进入echo函数时, echo栈帧中%rsp+8位置存放的8字节数值是? 如果此时输入按键abcdefg并回车, 程序将如何执行? 如果此时输入按键123456789并回车, 程序能否正常返回? 如果不能将执行什么处理? 7Byte

8 第三章 函数参数+浮点

对于一下汇编代码，请写出对应的C函数代码（整数参数请使用a/b，浮点参数请使用c）

~~myfun:~~

```
movsbl    %dil, %edi
imull     $30, %edi, %edi
addl      (%rsi), %edi
movl      %edi, (%rsi)
cvtsi2ss  %edi, %xmm1
addss     %xmm1, %xmm0
ret
```

附加题