1. 假设数组 int b[2], %rdi 保存数组 b 的首地址，b[1]=2 **等价于**哪条汇编指令 D ?

   A、movl $0x02, (%rdi)　　B、movl $2, 2(%rdi)

   C、movl $2, 8(%rdi)　　D、movl $2, 4(%rdi)

2. 对于数组 int A[M][N]，需要将其元素 A[i][j]保存到 eax 中，数组起始地址在 rdi，i 保存在 rsi，j 保存在 rdx 中。相关的汇编代码如下：

   leaq (%rsi, %rsi, 2), %rax

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

   movl (%rax, %rdx, 4), %eax

   则 N 的值为： B

   A、2　　B、3　　C、4　　D、5

3. 以下关于 GCC 生成可执行文件过程的描述中，错误的是 D 。

   A、预处理的结果还是一个 C 语言源程序文件，属于人可阅读的文本文件；

   B、经过预处理、编译、和汇编处理的结果是一个可重定位目标文件；

   C、每个 C 语言源程序文件生成一个对应的可重定位目标文件；

   D、纯静态链接所生成的可执行文件中，需要用重定位标志出所需重定位的相关信息。

4、函数 P 与结构体 test 的定义如下，并请完成以下的问题：

```
struct test {
    char *a;
    char b;
    int c;
};
long P(long x, long y, struct test *s)
{
    long u = Q(y);
    long v = Q(x);
    return u+v+(s->c);
}
```

```
1   P:
2       pushq   %rbp
3       pushq   %rbx
4       pushq   %r12
5       subq    $8,         %rsp
6       movq    %rdx,       %r12

7       movq    %rdi        ,   %rbp

8       movq    %rsi    ,   %rdi
9       call    Q

10      movq    %rax    ,   %rbx

11      movq    %rbp    ,   %rdi
12      call    Q
13      addq    %rbx,   %rax

14      addq    16(%r12)    ,   %rax
15      addq    $8,   %rsp
16      popq    %r12
17      popq    %rbx
18      popq    %rbp
19      ret
```

补全 P 函数对应的汇编代码中的缺失部分；

5、考虑下面的结构声明、set_y函数主体及对应的汇编代码。其中，A, B，和C未知

```
typedef struct {
    int x[B];
    int y;
    int z[C];
} struct_a;
typedef struct{
    struct_a data[A];
    int idx;
} struct_b;
void set_y(struct_b *bp, int val)
{
    int idx = bp->idx;
    bp->data[idx].y = val;
}
```

GCC 为 set_y 函数产生了如下的代码片段：

```
set_y:
    movslq 168(%rdi),%rax
    leaq (%rax,%rax,2), %rax
    movl %esi, 12(%rdi,%rax,8)
    ret
```

请根据汇编代码，推理出 A、B 和 C 的值各是多少？

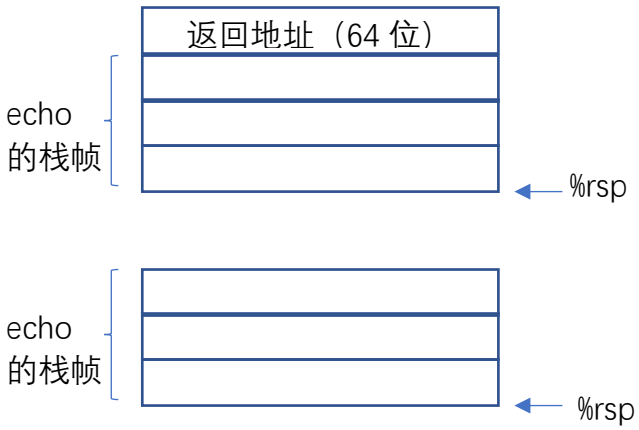
7 3 2

6、（堆栈破坏问题）函数 echo 定义如下：

```
void echo(){
    char buf[8];
    gets(buf);
    puts(buf);
}
```

对应的汇编代码如下：

```
echo:
        subq    $24,%rsp
        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
```



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？

02/03/04/05/06/07/08/09

输出 abcdefg 并正常退出

不能够正常退出，输出 123456789，并报告栈帧被破坏