<参考答案见视频源码下载>

画出下面函数的堆栈图：

int plus(int p1,int p2,int p3)

{

int a;

int b;

int c;

a = p1+p2+p3;

b = p1-p2-p3;

c = p1-p2+p3;

return a+b+c;

}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
| edi |  |  | edi |  |
| esi |  |  | esi |  |
| ebx | 压栈寄存器 | | ebx |  |
| CCCCCCCC | 提升esp |  | CCCCCCCC |  |
| CCCCCCCC |  |  | CCCCCCCC |  |
| CCCCCCCC |  |  | CCCCCCCC |  |
| CCCCCCCC |  |  | CCCCCCCC |  |
| CCCCCCCC |  |  | CCCCCCCC |  |
| 2 | c = p1-p2+p3; | | 2 |  |
| FFFFFFFC | b = p1-p2-p3; | | FFFFFFFC |  |
| 6 | a = p1+p2+p3; | | 6 |  |
| 0018FF48 | 原EBP |  | 0018FF48 |  |
| 004010A3 | 函数返回地址 | | 004010A3 |  |
| 1 |  |  | 1 |  |
| 2 |  |  | 2 |  |
| 3 | 参数 |  | 3 |  |
|  |  |  | 出栈edi,esi,ebx | |
|  |  |  | 还原esp,还原ebp | |
|  |  |  | 函数返回,外平栈 | |

Return a+b+c;是eax里的值4