<参考答案见视频源码下载>

short plus(short x,short y,short z,short m)

{

return x+y+z+m;

}

void main() //入口程序 程序开始执行的地方

{

//调用函数

plus(1,2);

return; //执行结束

}

压栈参数,函数调用,外平栈

00401088 push 4

0040108A push 3

0040108C push 2

0040108E push 1

00401090 call @ILT+0(plus) (00401005)

00401095 add esp,10h

中转

00401005 jmp plus (00401020)

压栈ebp,提升ebp,提升esp,压栈ebx/esi/edi,循环填充ebp-40h

00401020 push ebp

00401021 mov ebp,esp

00401023 sub esp,40h

00401026 push ebx

00401027 push esi

00401028 push edi

00401029 lea edi,[ebp-40h]

0040102C mov ecx,10h

00401031 mov eax,0CCCCCCCCh

00401036 rep stos dword ptr [edi]

带符号加法

00401038 movsx eax,word ptr [ebp+8]

0040103C movsx ecx,word ptr [ebp+0Ch]

00401040 add eax,ecx

00401042 movsx edx,word ptr [ebp+10h]

00401046 add eax,edx

00401048 movsx ecx,word ptr [ebp+14h]

0040104C add eax,ecx

出栈,还原esp,还原ebp,函数返回

0040104E pop edi

0040104F pop esi

00401050 pop ebx

00401051 mov esp,ebp

00401053 pop ebp

00401054 ret

返回值在eax

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
|  |  |  | edi | esp:0018FE98 | | edi | esp:0018FE98 | |
|  |  |  | esi |  |  | esi |  |  |
|  |  |  | ebx |  |  | ebx |  |  |
|  |  |  |  | esp:0018FEA4 | | CCCCCCCC | esp:0018FEA4 | |
|  |  |  |  |  |  | CCCCCCCC |  |  |
|  |  |  |  |  |  | CCCCCCCC |  |  |
|  |  |  |  |  |  | CCCCCCCC |  |  |
|  |  |  |  |  |  | CCCCCCCC |  |  |
|  |  |  |  |  |  | CCCCCCCC |  |  |
|  |  |  |  |  |  | CCCCCCCC |  |  |
|  |  |  |  |  |  | CCCCCCCC |  |  |
|  |  |  |  |  |  | CCCCCCCC |  |  |
|  |  |  | 0018FF48 | ebp:0018FEE4 | | 0018FF48 | ebp:0018FEE4 | |
| 00401095 | esp:0018FEE8 | | 00401095 | esp:0018FEE8 | | 00401095 | esp:0018FEE8 | |
| 1 | esp:0018FEEC | | 1 | esp:0018FEEC | | 1 | esp:0018FEEC | |
| 2 |  |  | 2 |  |  | 2 |  |  |
| 3 |  |  | 3 |  |  | 3 |  |  |
| 4 |  |  | 4 |  |  | 4 |  |  |
|  | esp:0018FEFC | |  | esp:0018FEFC | |  | esp:0018FEFC | |
|  |  |  |  |  |  |  |  |  |
|  | ebp:0018FF48 | |  | ebp:0018FF48 | |  | ebp:0018FF48 | |
| 压栈参数,函数调用 | |  | 压栈ebp,提升ebp，提升esp, | | | 循环填充ebp-40h | |  |
|  |  |  | 压栈ebx，esi，edi | |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
| edi | esp:0018FE98 | | edi |  |  | edi |  |
| esi |  |  | esi |  |  | esi |  |
| ebx |  |  | ebx |  |  | ebx |  |
| CCCCCCCC | esp:0018FEA4 | | CCCCCCCC |  |  | CCCCCCCC |  |
| CCCCCCCC |  |  | CCCCCCCC |  |  | CCCCCCCC |  |
| CCCCCCCC |  |  | CCCCCCCC |  |  | CCCCCCCC |  |
| CCCCCCCC |  |  | CCCCCCCC |  |  | CCCCCCCC |  |
| CCCCCCCC |  |  | CCCCCCCC |  |  | CCCCCCCC |  |
| CCCCCCCC |  |  | CCCCCCCC |  |  | CCCCCCCC |  |
| CCCCCCCC |  |  | CCCCCCCC |  |  | CCCCCCCC |  |
| CCCCCCCC |  |  | CCCCCCCC |  |  | CCCCCCCC |  |
| CCCCCCCC |  |  | CCCCCCCC |  |  | CCCCCCCC |  |
| 0018FF48 | ebp:0018FEE4 | | 0018FF48 |  |  | 0018FF48 |  |
| 00401095 | esp:0018FEE8 | | 00401095 |  |  | 00401095 |  |
| 1 | esp:0018FEEC | | 1 | esp:0018FEEC | | 1 |  |
| 2 |  |  | 2 |  |  | 2 |  |
| 3 |  |  | 3 |  |  | 3 |  |
| 4 |  |  | 4 |  |  | 4 |  |
|  | esp:0018FEFC | |  |  |  |  | esp:0018FEEC |
|  |  |  |  |  |  |  |  |
|  | ebp:0018FF48 | |  | ebp:0018FF48 | |  | ebp:0018FF48 |
| 循环填充ebp-40h | |  | 出栈edi,esi,ebx,还原esp | | | 外平栈 |  |
|  |  |  | 还原ebp,函数返回 | |  |  |  |