5

1. movsx dword ptr [edx], al
2. mov [edx], al
3. mov [edx], eax
4. movsx dword ptr [edx], ax
5. movzx dword ptr [edx], al
6. movsx dword ptr [edx], al
7. mov [edx], eax

9

|  |  |
| --- | --- |
| movl 12(%ebp), %ecx | y送ecx |
| sall $8, %ecx | ecx左移8位 // y左移8位 |
| movl 8(%ebp), %eax | x送eax |
| movl 20(%ebp), %edx | k送edx |
| imull %edx, %eax | x\*k送eax |
| movl 16(%ebp), %edx | z送edx |
| andl $65520, %edx | z&65520送edx // z&0xFFF0 |
| addl %ecx, %edx | z&0xFFF0 + y\*256，送edx |
| subl %edx, %eax | x\*k-(z&0xFFF0+y\*256)，送eax |

int v = x \* k – (z&0xFFF0 + y \* 256);

15

…

4: while (x != 0) {

5: y ^= x;

6: x >> = 1;

7: }

8: return y & 1;

…

返回 (x ^ (x>>1) ^ (x>>2) ^ … 0) & 0x1。只看最后一位，最后一位为所有的位相异或。即检查x中1的个数，奇数个1返回1，偶数个1返回0。

18.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | 0xBBFFFFF0 |  |
|  | 0xBBFFFFF4 |  |
|  | 0xBBFFFFF8 |  |
|  | 0xBBFFFFFC |  |
|  | 0xBC000000 |  |
|  | 0xBC000004 |  |
|  | 0xBC000008 |  |
|  | 0xBC00000C |  |
|  | 0xBC000010 |  |
|  | 0xBC000014 |  |
|  | 0xBC000018 |  |
|  | 0xBC00001C |  |
|  | 0xBC000020 | SP |

执行3后：(EBP) = 0xBC00001C

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | 0xBBFFFFF0 |  |
|  | 0xBBFFFFF4 |  |
|  | 0xBBFFFFF8 |  |
|  | 0xBBFFFFFC |  |
|  | 0xBC000000 |  |
|  | 0xBC000004 |  |
|  | 0xBC000008 |  |
|  | 0xBC00000C |  |
|  | 0xBC000010 |  |
|  | 0xBC000014 |  |
|  | 0xBC000018 |  |
| 0xBC000030 | 0xBC00001C | SP |
|  | 0xBC000020 |  |

执行4后：

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | 0xBBFFFFF0 |  |
|  | 0xBBFFFFF4 | SP |
|  | 0xBBFFFFF8 |  |
|  | 0xBBFFFFFC |  |
|  | 0xBC000000 |  |
|  | 0xBC000004 |  |
|  | 0xBC000008 |  |
|  | 0xBC00000C |  |
|  | 0xBC000010 |  |
|  | 0xBC000014 |  |
|  | 0xBC000018 |  |
| 0xBC000030 | 0xBC00001C |  |
|  | 0xBC000020 |  |

执行6后：EAX = (EBP) – 8 = 0xBC000014

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | 0xBBFFFFF0 |  |
|  | 0xBBFFFFF4 | SP |
|  | 0xBBFFFFF8 |  |
| 0xBC000014 | 0xBBFFFFFC |  |
|  | 0xBC000000 |  |
|  | 0xBC000004 |  |
|  | 0xBC000008 |  |
|  | 0xBC00000C |  |
|  | 0xBC000010 |  |
|  | 0xBC000014 |  |
|  | 0xBC000018 |  |
| 0xBC000030 | 0xBC00001C |  |
|  | 0xBC000020 |  |

执行8后：EAX = (EBP) – 4 = 0xBC000018

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | 0xBBFFFFF0 |  |
|  | 0xBBFFFFF4 | SP |
| 0xBC000018 | 0xBBFFFFF8 |  |
| 0xBC000014 | 0xBBFFFFFC |  |
|  | 0xBC000000 |  |
|  | 0xBC000004 |  |
|  | 0xBC000008 |  |
|  | 0xBC00000C |  |
|  | 0xBC000010 |  |
|  | 0xBC000014 |  |
|  | 0xBC000018 |  |
| 0xBC000030 | 0xBC00001C |  |
|  | 0xBC000020 |  |

执行9后：

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | 0xBBFFFFF0 |  |
| 0x804C000 // 格式串地址 | 0xBBFFFFF4 | SP |
| 0xBC000018 | 0xBBFFFFF8 |  |
| 0xBC000014 | 0xBBFFFFFC |  |
|  | 0xBC000000 |  |
|  | 0xBC000004 |  |
|  | 0xBC000008 |  |
|  | 0xBC00000C |  |
|  | 0xBC000010 |  |
|  | 0xBC000014 |  |
|  | 0xBC000018 |  |
| 0xBC000030 | 0xBC00001C |  |
|  | 0xBC000020 |  |

开始执行到10中：

|  |  |  |
| --- | --- | --- |
|  |  |  |
| 11行指令地址 | 0xBBFFFFF0 | SP |
| 0x804C000 // 格式串地址 | 0xBBFFFFF4 |  |
| 0xBC000018 | 0xBBFFFFF8 |  |
| 0xBC000014 | 0xBBFFFFFC |  |
|  | 0xBC000000 |  |
|  | 0xBC000004 |  |
|  | 0xBC000008 |  |
|  | 0xBC00000C |  |
|  | 0xBC000010 |  |
|  | 0xBC000014 |  |
|  | 0xBC000018 |  |
| 0xBC000030 | 0xBC00001C |  |
|  | 0xBC000020 |  |

执行10后：

|  |  |  |
| --- | --- | --- |
|  |  |  |
| 11行指令地址 | 0xBBFFFFF0 |  |
| 0x804C000 // 格式串地址 | 0xBBFFFFF4 | SP |
| 0xBC000018 | 0xBBFFFFF8 |  |
| 0xBC000014 | 0xBBFFFFFC |  |
|  | 0xBC000000 |  |
|  | 0xBC000004 |  |
|  | 0xBC000008 |  |
|  | 0xBC00000C |  |
|  | 0xBC000010 |  |
| 0x100 | 0xBC000014 |  |
| 0x16 | 0xBC000018 |  |
| 0xBC000030 | 0xBC00001C |  |
|  | 0xBC000020 |  |

执行10后，若按10行注释：

|  |  |  |
| --- | --- | --- |
|  |  |  |
| 11行指令地址 | 0xBBFFFFF0 |  |
| 0x804C000 // 格式串地址 | 0xBBFFFFF4 | SP |
| 0xBC000018 | 0xBBFFFFF8 |  |
| 0xBC000014 | 0xBBFFFFFC |  |
|  | 0xBC000000 |  |
|  | 0xBC000004 |  |
|  | 0xBC000008 |  |
|  | 0xBC00000C |  |
|  | 0xBC000010 |  |
| 20 | 0xBC000014 |  |
| 15 | 0xBC000018 |  |
| 0xBC000030 | 0xBC00001C |  |
|  | 0xBC000020 |  |

（1）执行3、10、13行后，BP的值依次为0xBC00001C、0xBC00001C、0xBC000030H。第13行leave还原BP

（2）执行3、10、13行后，SP的值依次为0xBC00001C、0xBBFFFFF0、0xBC000020H。

第13行leave还原SP

（3）x、y的地址为 0xBC000018、0xBC000014

（4）见上图