

1. 如上图

2.

|  |  |  |
| --- | --- | --- |
| Operation | Destination | Value |
| Subq (%rbx),%rax | %rax | 0x108 |
| Incq -8(%rax) | 0x100 | 0x201a |
| Decq %rdx | %rdx | 0x8 |
| Imulq $4, 0x100(%rdx,%rcx,4) | 0x110 | 0x48 48 48 48 48 48 48 48 |
| Shrq $4,%rax | %rax | 0x10 |
| Imulq 0x10 | %rax,%rdx | 0x100, 0x0 |
| notw(%rax,%rdx) | 0x100 | 0xdfe5  小心！此时根据上一步，rdx已经变成0x0了，连锁反应 |
| Andq 0x10 (%rax,%rcx,4),%rax | %rax | 0x100 |
| Leaq 9(%rax,%rcx,8),%rdx | %rdx | 0x119 |

3.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| instruction | OF | CF | ZF | SF |
| Addq %rbx,%rax | 0 | 0 | 0 | 1 |
| Subq %rax,%rbx | 0 | 0 | 0 | 1 |
| Leaq (%rax,%rax,2), %rax | --- | --- | --- | --- |
| Xorq %rax,%rax | 0 | 0 | 1 | 0 |
| Salq $2,%rbx | 0 | 1 | 0 | 1 |
| Cmpq %rax,%rbx | 0 | 0 | 0 | 1 |
| Testq %rax,%rbx | 0 | 0 | 1 | 0 |