

Zad 7.

piątek, 31 marca 2023 17:38

Zadanie 7 (2). Poniższy kod w asemblerze otrzymano w wyniku deasemblacji funkcji zadeklarowanej jako «long switch_prob(long x, long n)». Zapisz w języku C kod odpowiadający tej funkcji.

case 0,1

case 4

case 2

case 5

default

```

1 400590 <switch_prob>:
2 400590: 48 83 ef 3c
3 400594: 48 83 fe 05
4 400598: 77 29
5 40059a: ff 24 f5 f8 06 40 00
6 4005a1: 48 8d 04 fd 00 00 00
7 4005a9: c3
8 4005aa: 48 89 f8
9 4005ad: 48 c1 f8 03
10 4005b1: c3
11 4005b2: 48 89 f8
12 4005b5: 48 c1 e0 04
13 4005b9: 48 29 f8
14 4005bc: 48 89 c7
15 4005bf: 48 0f af ff
16 4005c3: 48 8d 47 4b
17 4005c7: c3
    
```

```

subq $0x3c,%rsi
cmpq $0x5,%rsi
ja *0x4005c3
jmpq *0x4006f8(,%rsi,8)
lea 0x0(,%rdi,8),%rax
retq
movq %rdi,%rax
sarq $0x3,%rax
retq
movq %rdi,%rax
shlq $0x4,%rax
subq %rdi,%rax
movq %rax,%rdi
imulq %rdi,%rdi
leaq 0x4b(%rdi),%rax
retq
    
```

$n = n - 60$

$n > 5 \rightarrow \text{default}$

Zrzut pamięci przechowującej tablicę skoków:

```

18 (gdb) x/6gx 0x4006f8
19 0x4006f8: 0x4005a1
20 0x400700: 0x4005a1
21 0x400708: 0x4005b2
22 0x400710: 0x4005c3
23 0x400718: 0x4005aa
24 0x400720: 0x4005bf
    
```

$x \gg 3$

$x = (x \ll 4) - x$

x^2

$x + 0x4b$

$0x4006f8 + 8(n-60)$
jump table

fallthrough

```

37 long switch_prob(long x, long n) {
38     n = n - 60;
39     switch(n) {
40         case 0:
41             case 1: x = 8 * x;
42                 break;
43             case 4: x = x >> 3;
44                 break;
45             case 2: x = (x << 4) - x;
46             case 5: x = x * x;
47             default: x = x + 0x4B;
48         }
49     return x;
50 }
    
```