

5 Машин програм

1. Дараах санах ой болон регистрын утгууд өгөгдсөн.

Хаяг	Утга	Регистр	Утга
0x100	0xFF	%rax	0x100
0x104	0xAB	%rcx	0x1
0x108	0x13	%rdx	0x3
0x10C	0x11		

Тэгвэл дараах хүснэгтэд заагдсан операндуудын утгыг нөхнө үү.

Операнд	Утга
%rax	...
0x104	...
\$0x108	...
(%rax)	...
4(%rax)	...
9(%rax, %rdx)	...
0xFC(%rcx, 4)	...
(%rax,%rdx,4)	...

2. Дараах мөр бүрийн хувьд тохирох mov командыг бич. Энд movb, movw, movl, movq нарын аль нэгийг бичнэ.

```
mov_      %eax, (%rsp)
mov_      (%rax), %dx
mov_      $0xFF, %b1
mov_      (%rsp,%rdx,4), %d1
mov_      (%rdx), %rax
mov_      %dx, (%rax)
```

3. Дараах машин кодын мөр бүрийг ажиллуулах гэвэл алдаа өгнө. Тухайн мөрд ямар алдаа өгөхийг ол.

```
movb $0xF, (%ebx)
movl %rax, (%rsp)
movw (%rax), 4(%rsp)
movb %al, %sl
movq %rax, $0x123
movl %eax, %rdx
movl %si, 8(%rbp)
```

4. objdump команд ашиглах дараах си кодын машин кодыг харуул.

```
#include <stdio.h>
int fact(int n)
{
    if (n == 0)
        return 1;
    int x = fact(n - 1);
    return x * n;
}
int main()
{
    int y = fact(5);
    printf("%d\n", y);
    return 0;
}
```

5. Функцийн зарлалт нь дараах хэлбэртэй.

```
void decode1(long *xp, long *yp, long *zp);
```

Тэгвэл хөрвүүлэгдсэн машин кодоос уг функцийн Си кодыг бич.

```
decode1:
    movq (%rdi), %r8
    movq (%rsi), %rcx
    movq (%rdx), %rax
    movq %r8, (%rsi)
    movq %rcx, (%rdx)
    movq %rax, (%rdi)
    ret
```

xp, yp, zp параметрууд харгалзан *%rdi*, *%rsi*, *%rdx* региструудэд хадгалагдсан.