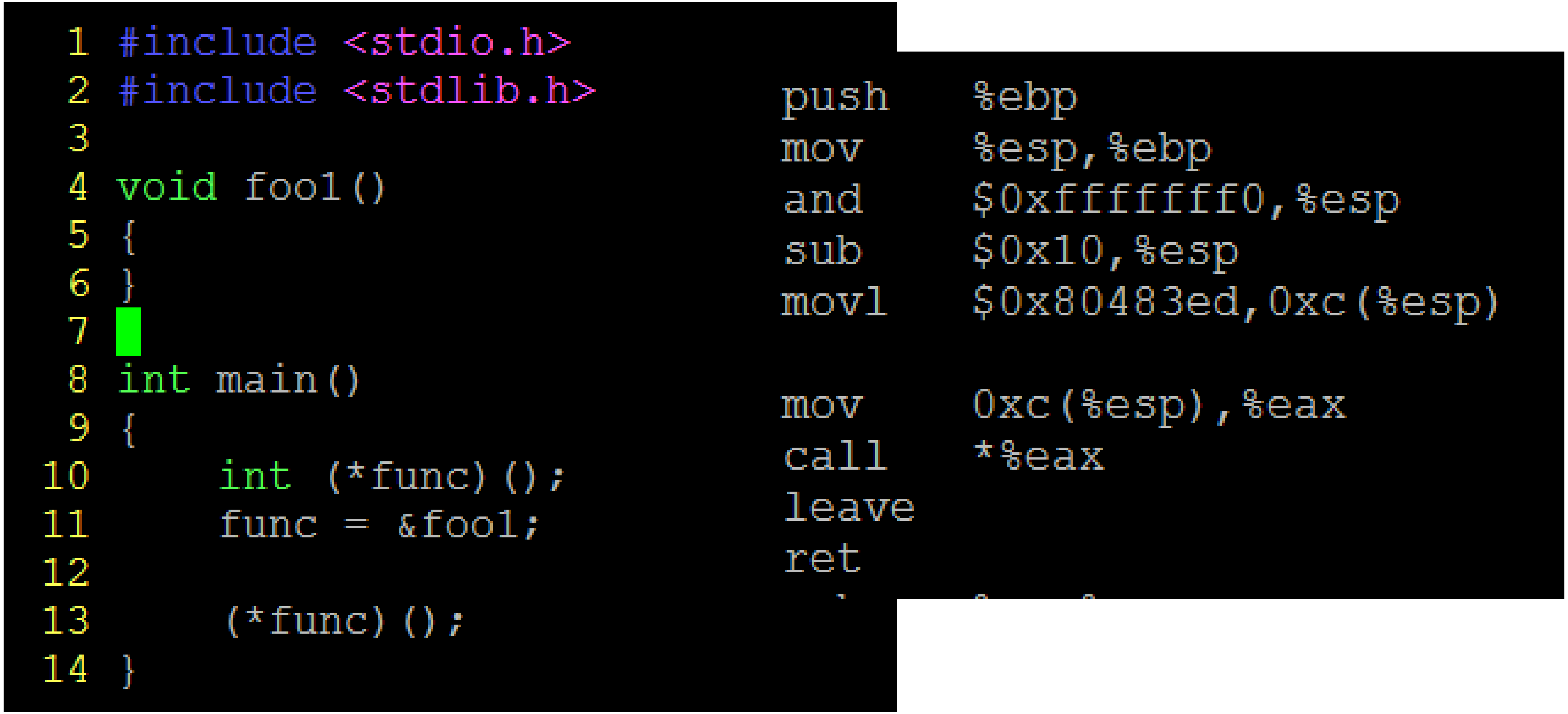
Homework 0x02 hint

ddaa

nphw1

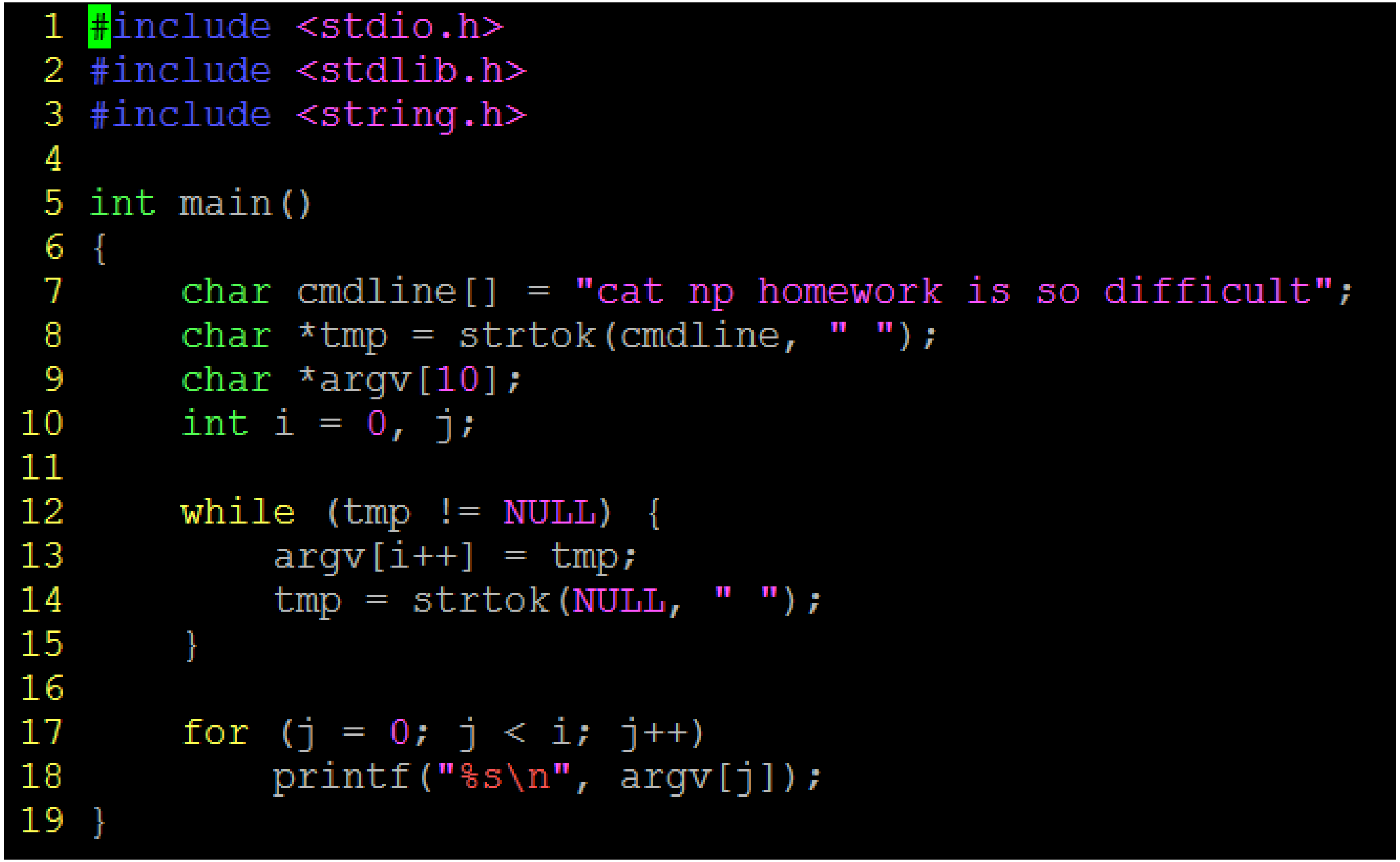
Control eax = control eip



```c
#include <stdio.h>
#include <stdlib.h>

void foo1()
{
}

int main()
{
        int (*func)();
        func = &foo1;

        (*func)();
}
```

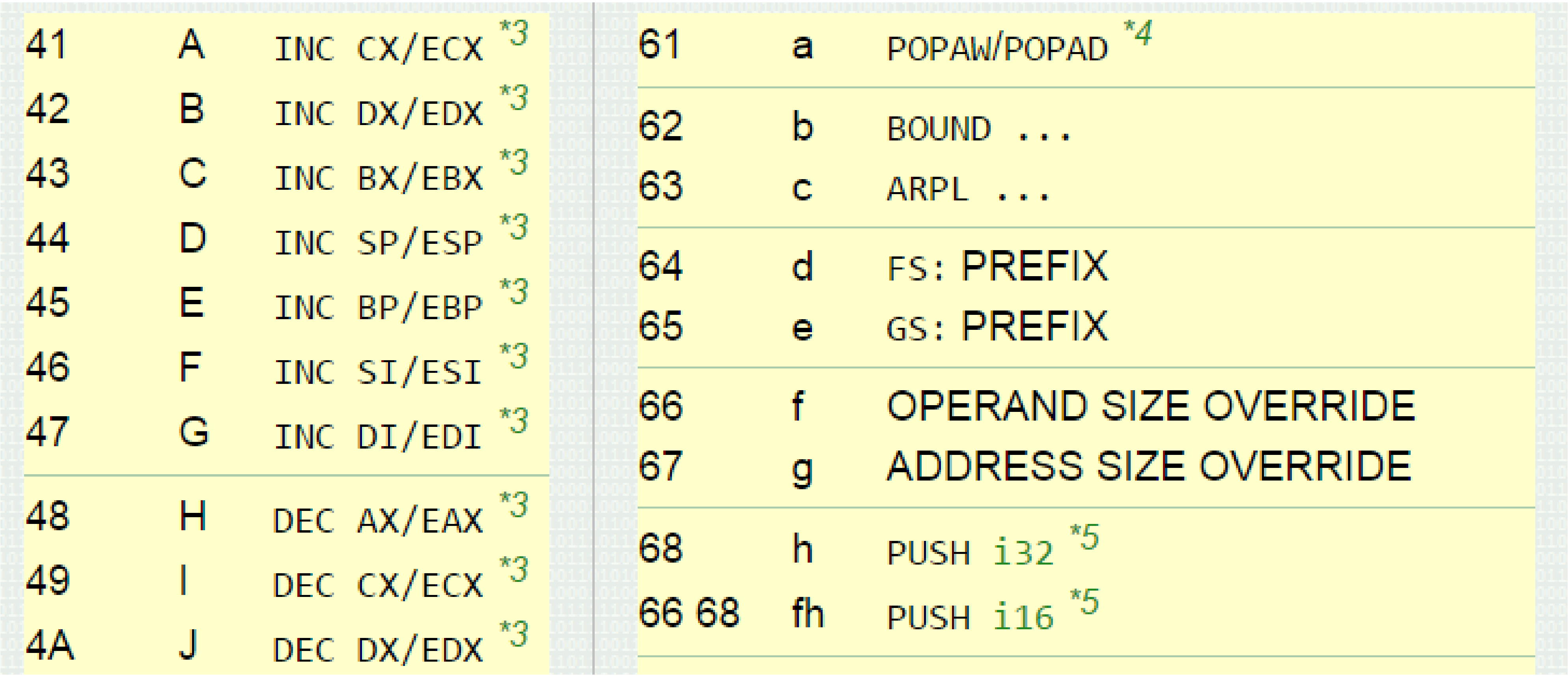
```
push    %ebp
mov     %esp,%ebp
and     $0xfffffff0,%esp
sub     $0x10,%esp
movl    $0x80483ed,0xc(%esp)

mov     0xc(%esp),%eax
call    *%eax
leave
ret
```

strtok – what will it happen?



```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int main()
{
    char cmdline[] = "cat np homework is so difficult";
    char *tmp = strtok(cmdline, " ");
    char *argv[10];
    int i = 0, j;

    while (tmp != NULL) {
        argv[i++] = tmp;
        tmp = strtok(NULL, " ");
    }

    for (j = 0; j < i; j++)
        printf("%s\n", argv[j]);
}
```

alnum

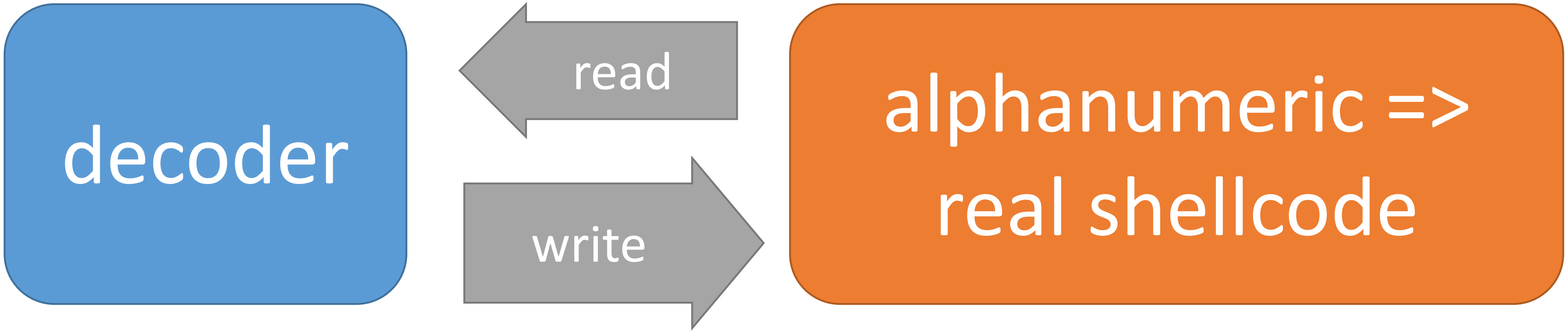


41	A	INC CX/ECX	*3
42	B	INC DX/EDX	*3
43	C	INC BX/EBX	*3
44	D	INC SP/ESP	*3
45	E	INC BP/EBP	*3
46	F	INC SI/ESI	*3
47	G	INC DI/EDI	*3
48	H	DEC AX/EAX	*3
49	I	DEC CX/ECX	*3
4A	J	DEC DX/EDX	*3

61	a	POPAW/POPAD	*4
62	b	BOUND ...	
63	c	ARPL ...	
64	d	FS: PREFIX	
65	e	GS: PREFIX	
66	f	OPERAND SIZE OVERRIDE	
67	g	ADDRESS SIZE OVERRIDE	
68	h	PUSH i32	*5
66 68	fh	PUSH i16	*5

Make a decoder

- Allowed characters only [A-Za-z0-9] – [BINSHbinsh].
- We must run a segment of legal shellcode to decode legal data to illegal shellcode.


decoder
read
write
alphanumeric =>
real shellcode