CS 241: Computer Organization and Assembly Language
Midterm

Do not open until instructed to do so.

Name: _____

"C'est en forgeant qu'on devient forgeron."
("It is by smithing that one learns to become a smith.")
~French proverb

Every problem is marked with a ► . When you see this symbol, it means that's a question which you can — and should — answer.

For grader use:

Score: _____

Syscalls

0	sys_read
1	sys_write
60	sys_exit

Arguments in: rdi, rsi, rdx, r10, r8, r9

Return value in: rax

Callee-saved regs.: rcx, r11

C-style functions

```
func:
  push rbp
  mov rbp, rsp

  ...

  pop rbp
  ret
```

Arguments in: rdi, rsi, rdx, rcx, r8, r9

Return value in: rax

Callee-saved regs.: rbx, rbp, r12-r15

Caller-saved regs.: rax, r10, r11, arguments

Memory operands

size [*displacement* + *base* + m * *offset*]

size byte, word, dword, etc.

displacement Constant address of array

base Array base register

m 1, 2, 4, or 8

offset Array offset register

Instructions

mov rm, rmi	Move
xchng rm, rm	Swap
lea r, m	Load Effective Address
xor r, r	Set *r* to 0
add rm, rmi	Addition
sub rm, rmi	Subtraction
mul rmi	Unsigned multiply (by/into rax)
div rm	Unsigned divide (by/into rax, rdx)
imul rmi	Signed multiply
idiv rmi	Signed divide
cmp rm, rmi	Compare (subtract), update flags
text rm, rmi	Test, update flags
jmp target	Jump to target
j*CC* target	Jump if condition *CC*
loop target	Decrement rcx, jump if not 0
call func	Push rip, jump to func
ret	Pop rip and jump to it
push rmi	Push onto stack
pop rmi	Pop from stack

r: register, m: memory operand, i: immediate

Condition codes

CC	Meaning
a	Unsigned $>$
ae	Unsigned $\geq$
b	Unsigned $<$
be	Unsigned $\leq$
g	Signed $>$
ge	Signed $\geq$
l	Signed $<$
le	Signed $\leq$
e	$=$
ne	$\neq$
s,c,z,...	If flag is set

5 points each

► Perform the following binary addition:
`01110101 + 00111111`
Show your work (all carries).

► What is the decimal value of `10001111` when interpreted as two's complement-signed?

► What is the two's complement binary value of –17?

► Suppose a cache has a hit percentage of 98%. The latency for a hit is 1ns, while the latency for a miss is 300ns. What is the average latency of a memory access?

► Suppose a cache has a total size of 16kB and a line size of 256 bytes. How many sets, and how many lines/set does the cache have if it is:

	Set-associative?	Fully-associative?
Sets:		
Lines/Set:		

► Perform the addition `11100010 + 01101111`, show your work, write the final sum, as well as the state of the flags after the addition is complete.

`CF =`

`OF =`

`SF =`

`ZF =`

► For each of the following condition codes, write the state of the flags it will check:

- `a`
- `b`
- `s`
- `ne`

► When executing a `syscall`, which of the following is used for the **syscall code**, the **1st argument**, the **2nd argument**, and the **3rd argument**?

- `rdx`
- `rax`
- `rsi`
- `rdi`

► What registers are used when passing floating-point arguments to a C-ABI-compatible function?

► Write assembly code to perform the division `157 / 13` using the `div` instruction. When your code is complete, the quotient should be in `rax`.

25 points each

► Complete the following `syscall`-style function so that it will print out a rectangle made of # characters. E.g., if the function's parameter in `rdi` is 5, it should print out

```
#####
#####
#####
#####
#####
```

Do not modify the `.data` section.

```
section .data

newline:    db    10
star:       db    '*'

section .text

print_stars:
  ; Size in rdi
  ; Your code here...
```

► Complete the following function so that it returns 1 if the (qword) value in `rdi` is found within the array pointed to by `rsi`, with length (in bytes) in `rdx`.

```
section .text

contains:
  ; rdi = search target
  ; rsi = addr. of array
  ; rdx = length of array (bytes)
  ; Return 1 in rax if found, 0 if not
```