Exam 2 Cheatsheet DRAFT

Syscall

rax	System Call	rdi	rsi	rdx
0	read	file descriptor	buffer	number of bytes
1	write	file descriptor	buffer	number of bytes
60	exit	exit code	—	—

Calling C library functions

- Parameters are stored in registers in the following order: rdi, rsi, rdx, rcx, r8, r9. (If there are more parameters, they are pushed onto the stack)
- Most C functions return an integer or a pointer (which is just an integer). The return value is placed in the rax register
- The called functions may use or destroy the content of the following registers: rax, rcx, rdx, rsi, rdi, r8, r9, r10, r11
- Other registers may be used, but the called function is responsible for saving them.

General Purpose Registers

64-bit	32-bit	16-bit	8-bit low	8-bit high	Calling Convention	May be destroyed by called function?
rax	eax	ax	al	ah	Return Val/Accum	Yes
rbx	ebx	bx	bl	bh	—	No
rcx	ecx	cx	cl	ch	4th argument	Yes
rdx	edx	dx	dl	dh	3rd argument	Yes
rsi	esi	si	sil	–	2nd argument	Yes
rdi	edi	di	dil	–	1st argument	Yes
r8	r8d	r8w	r8b	–	5th argument	Yes
r9	r9d	r9w	r9b	–	—	Yes
r10	r10d	r10w	r10b	–	—	Yes
r11	r11d	r11w	r11b	–	—	Yes
r12	r12d	r12w	r12b	–	—	No
r13	r13d	r13w	r14b	–	—	No
r14	r14d	r14w	r14b	–	—	No
r15	r15d	r15w	r15b	–	—	Yes

Special Purpose Registers

Register	64-bit	32-bit	16-bit	8-bit low	May be destroyed by called function?
Stack Pointer	rsp	esp	sp	spl	No
Base Pointer	rbp	ebp	bp	bpl	No
Instruction Pointer	rip	eip	ip	–	
Flags and Conditions	rflags	eflags	flags	–	Yes

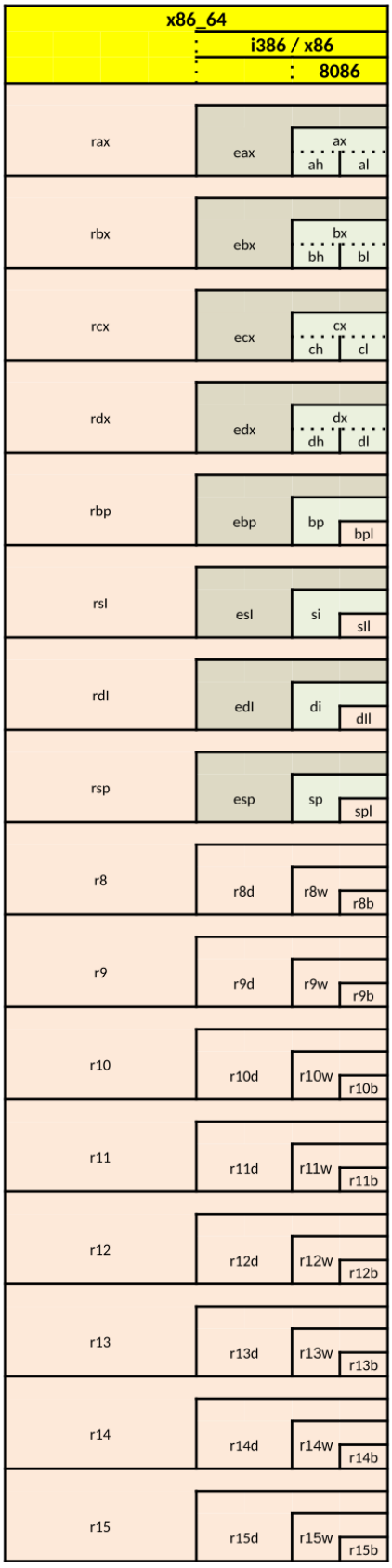
This is the cheatsheet from the first exam. It probably will not be on the second exam.

n	2^n	Other
0	1	8^0 and 16^0
1	2	
2	4	
3	8	
4	16	16^1
5	32	
6	64	
7	128	
8	256	16^2
9	512	
10	1024	1 Kilobyte
11	2048	
12	4096	16^3
13	8092	
14	16,384	
15	$32,768$	
16	65,536	16^4
17	131,082	
18	262,144	
19	524,288	
20	1,048,576	16^5 1 Megabyte

The counting in hex and binary is going to be on the exam itself

Multiplication	Result
$16 \cdot 0$	0
$16 \cdot 1$	16
$16 \cdot 2$	32
$16 \cdot 3$	48
$16 \cdot 4$	64
$16 \cdot 5$	80
$16 \cdot 6$	96
$16 \cdot 7$	112
$16 \cdot 8$	128
$16 \cdot 9$	144
$16 \cdot 10(a)$	160
$16 \cdot 11(b)$	176
$16 \cdot 12$ (c)	192
$16 \cdot 13$ (d)	208
$16 \cdot 14$ (e)	224
$16 \cdot 15$ (f)	240
$16 \cdot 16$	256

x86_64 Registers Map



The following is probably a placeholder, and it won't show up on the exam version.

function	arguments	return value	notes
puts	char *s	size_t length	does not count null byte
strcpy	char *dest, char *src	char *dest	dest must be big enough
strncmp	char *s1, char *s2, size_t n	int	0 if equal, $<$0 if s1<s2, $>$0 if s1>s2
strncpy	char *dest, char *src, size_t n	char *dest	dest must be big enough
strcat	char *dest, char *src	char *dest	dest must be big enough
strncat	char *dest, char *src, size_t n	char *dest	dest must be big enough
strcmp	char *s1, char *s2	int	0 if equal, $<$0 if s1<s2, $>$0 if s1>s2