Appedix: X86 Cheatsheet

4.1 Registers

x86 registers are 8-bytes. Additionally, the lower order bytes of these registers can be independently accessed as 4-byte, 2-byte, or 1-byte register. The register names are:

8-byte register	Bytes 0-3	Bytes 0-1	Byte 0 (lowest order byte)
%rax	%eax	%ax	%al
%rbx	%ebx	%bx	%bl
%rcx	%ecx	%cx	%cl
%rsi	%esx	%si	%sil
%rdi	%edx	%di	%dil

...the rest is omitted...

4.2 Instructions

Instruction suffixes:

"byte" (`b`)	1-byte
"word" (`w`)	2-bytes
"doubleword" (`l`)	4-bytes
"quardword" (`q`)	8-bytes

Complete memory addressing mode: A memory operand of the form `D(Rb, Ri, S)` accesses memory at address `D + val(Rb) + val(Ri)*S`, where val(Rb) and val(Ri) refer to the value of registers Rb and Ri respectively, D is a constant, and S is a constant of value 1, 2, 4, or 8.

Sign extension and zero extension:

movzlq S, D	copy 4-byte-sized S to 8-byte-sized D and fill in the higher order 4 bytes of D with zero bytes.
movslq S, D	copy 4-byte-sized S to 8-byte-sized D and sign extend the higher order 4 bytes of D, i.e. fill with 0s if S's sign bit is zero and fill with 1s if S's sign bit is one.

Basic Arithmatic instructions that you might not remember:

sal / shl k, D	Left shift destination D by k bits
sar	Arithmatic right shift destination D by k bits
shr	Logical right shift destination D by k bits

Jump instructions:

Jump instruction following `cmp S, D`:

jmp	Unconditional jump
je	Jump if D is equal to S
jne	Jump if D is not equal to S
jg	Jump if D is greater than S (signed)
jge	Jump if D is greater or equal than S (signed)
jl	Jump if D is less than S (signed)
jle	Jump if D is less or equal than S (signed)
ja	Jump if D is above S (unsigned)
jae	Jump if D above or equal S(unsigned)
jb	Jump is D is below S (unsigned)
jbe	Jump if D is below or equal S (unsigned)

4.3 Calling convention

Argument Passing:

Which argument	Stored in register
1	%rdi
2	%rsi
3	%rdx
4	%rcx
5	%r8
6	%r9
7 and up	passed on stack

Return value (if any) is stored in %rax

Caller save registers: %rax, %rcx, %rdx, %rdi, %rsi, %r8-11

Callee save registers: %rbx, %rbp, %r12-15