Y86-64 Cheat Sheet

Y86-64 Instructions

- `halt`
- `nop`
- Move Data [xxmovq src, dest]
  - `rrmovq %rax, %rbx`
  - `irmovq $1, %rbx`
    - `irmovq label, %rbx`
  - `rmmovq %rax, 8(%rsi)`
    - `rmmovq %rax, (%rsi)`
  - `mrmovq 1(%rsi), %rbx`
  - `cmov__ %rax, %rbx`
- ALU Opq [%rbx = %rbx OP %rax]
  - `addq %rax, %rbx`
  - `subq %rax, %rbx`
  - `andq %rax, %rbx`
  - `xorq %rax, %rbx`
- Jumps
  - `jmp label`
  - `j__ label`

- Stack
  - `pushq %rax`
  - `popq %rbx`
- Functions
  - `call label`
  - `ret`

Y86-64 Simulator Commands

- `.pos 0x100`
  - move to position `0x100` in memory
- `label:`
  - Assign label to current position / next memory address
  - Can be used in `irmovq`, `jmp`, and `call` instructions
- `.quad 0xabcdef123`
  - place the quadword `0xabcdef123` in memory at current position