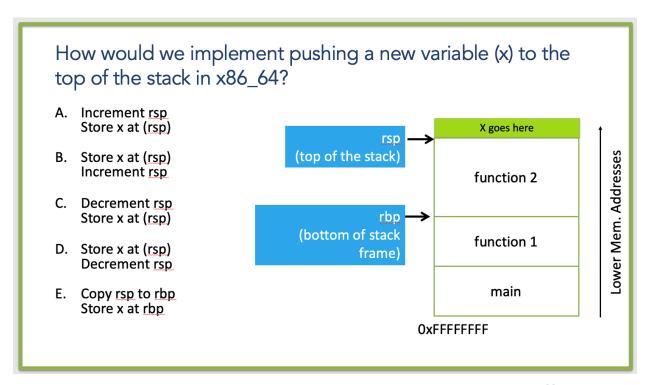
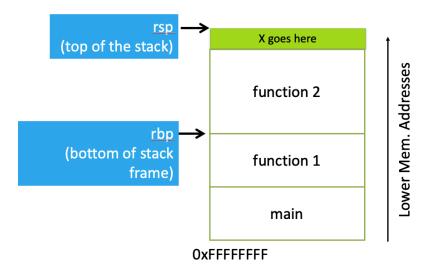
CS31 Worksheet: Week 6: Functions and the Stack



How would we implement popping a new variable (x) off the top of the stack in x86_64?



x86 Calling Conventions: Function Call callee caller's %rbp value rsp caller stack frame caller stack frame rbp Initial state push %rbp (store caller's base pointer) callee callee stack frame rsp caller's %rbp value rsp caller's %rbp value caller stack frame rbp caller stack frame mov %rsp, %rbp sub \$SIZE, %rsp (allocate space for callee's locals) (establish callee's frame pointer)

Given the figure above, can you describe in figures, and words the sequence of instructions to return from a function call?