Code Jam 4

Names: Caesar Dai Tung

Complete the following exercises in 40 minutes. This activity is open book, open computer. All work should be your own group.

Question 1

Short answer

1) How is machine code generated from source code? What is the relationship between machine code and assembly?

The caupiler compiles the source code to machine-specific assembly code. Assembly code is the same as machine code, which is a human readable form of the binary machine code instructions that a caupiter can execute

2) What is a register?

Register is a unit of storage that hold program data and the instructions that are being executed by the ALU (small, fast)

3) What two steps occur when the CPU executes the instruction `push %rbp` ?

sub $0x8, %rsp

mov %rbp, (%rsp)

4) What two steps occur when the CPU executes the instruction `pop %rbp` ?

mov (%rsp), %rbp

add $0x8, %rsp

5) What does `callq` do?

Switches active frame to callee function

push %rip

What is the value 0x10 as a base 10 integer?

16

2) What is the value 0xfffffff7 as a base 10 *signed* integer (two's complement)?

-9

3) Draw the contents of the registers and stack after executing the instruction `sub $0x10,%rsp` (0x0000555555555151)

Register	Value
%eax	0x202
%edx	0xe148
%rbp	0x040
%rsp	0x030
%esi	0xe138
%edi	0x1
%rip	0x0000555555555151

"Stack top"

Address	Stack value	
0x030		← Stack top
0x038		
0x040	0x0	
0x048		← Stack bottom

4) What is the translation of the memory form `-0x8(%rbp)` ?

M[%rbp - 0x8]

5) What is the `shl` instruction?

left bit shift (logical shift). filling the lowest bit with 0

6) What are the contents of %eax after executing instruction 0x000055555555515c?

0xffffff7

7) What are the contents of %eax after executing instruction 0x000055555555515f?

0x3fffffdc

8) What are the contents of %rsi after executing instruction 0x000055555555516b?

%esi = 0xffffff7

9) What are the contents of %rdi after executing instruction 0x000055555555516d?

0x00005555555556004

Question 3

In this question use GDB and objdump to reverse engineer to binary executable `secret`

```
$ ./secret
Guess the mysterious number: 39
You are wrong!
```

1) What functions does `main` call (please list in execution order)?

mystery. foo. printf. scanf. puts

2) What are the values of %esi and %edi before the first function call in main?

value at %esi = 87

value at %edi = 62

3) What is the return value from the first function?

74

4) What is the value of %edi before the second function call in main?

74

5) What is the secret number? 174