Name: Utkarsh Arora

Roll No: 2020143

Question 2

Run:

Run make in shell. Program outputs will be displayed on stdout.

Logic:

There are three files: A.c, B.asm, C.c; B.asm is a GAS Assembly file.

main() lies in A.

main() calls A()

A.c has a line extern void B(unsigned long long int); which indicated that B() is an external function from another source.

A() prints “Currently inside function A”

A() calls B(0x6969696969696969LL);

B() first prints “Currently inside function B”

it interprets the 64-bit number and prints it as 8 ascii characters using syscall write(). The 64-bit number is stored in memory (RAM) and its memory address is provided in write(). When a function is called, the return address is stored on top of the stack.

```
0x6969696969696969LL
translates to
iiiiiiii
```

To pass control to C(), we overwrite the return address with the address to function C().

C() then calls system call exit() to stop execution.

About System Calls

All system calls are done using syscall instruction

rax stores identifier for the system call being called (1 for write, 60 for exit). The arguments to the write system call are stored in rdi, rsi, rdx as it needs 3 arguments.