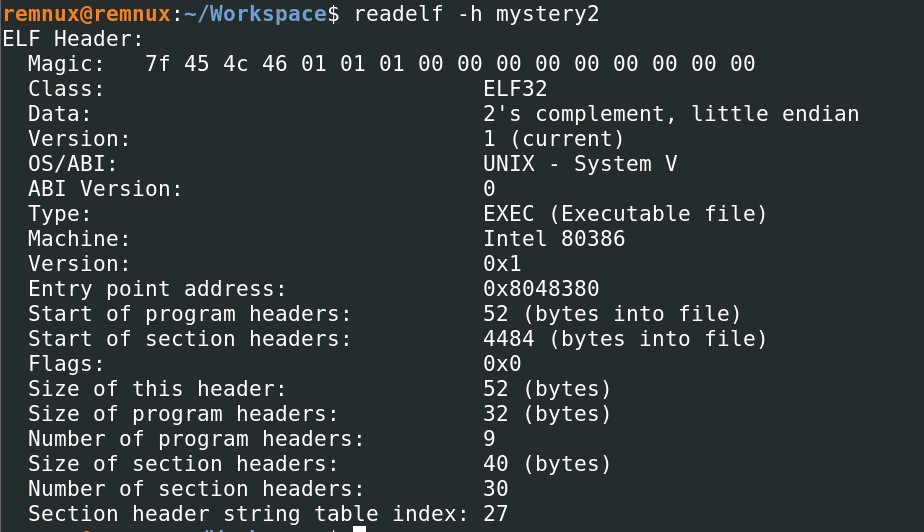
Name: Rithik Sarvesh Bharathiraja

UID: 120395246

Course: ENPM696

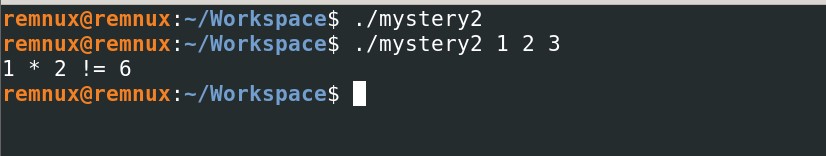
Task: In-class exercise 4

1. mystery2 (ELF)  
   A) It’s a 32-bit executable program



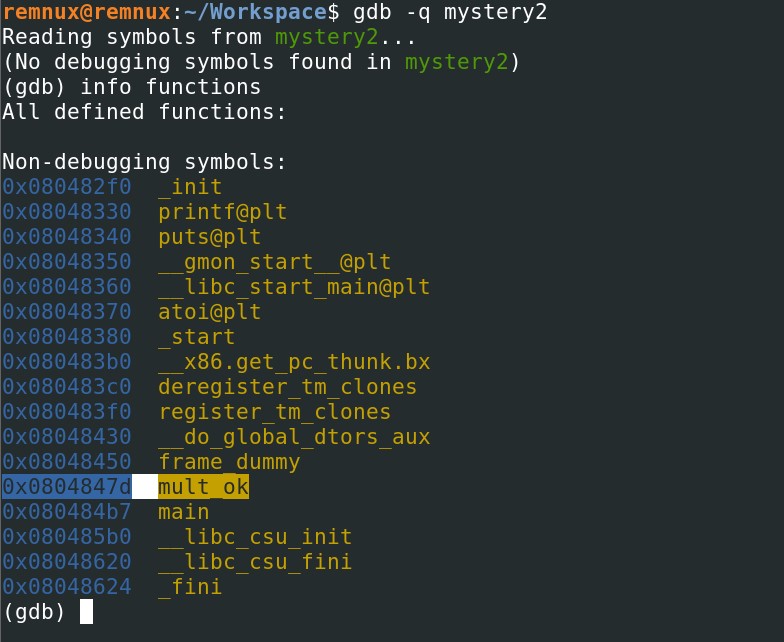
B) The file format is ELF .

C) No, The program doesn’t take input once they are started.

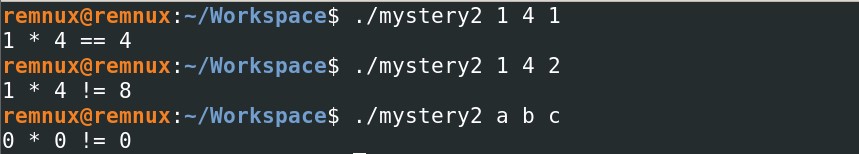


D) Yes, the program accepts input at startup on the command line.

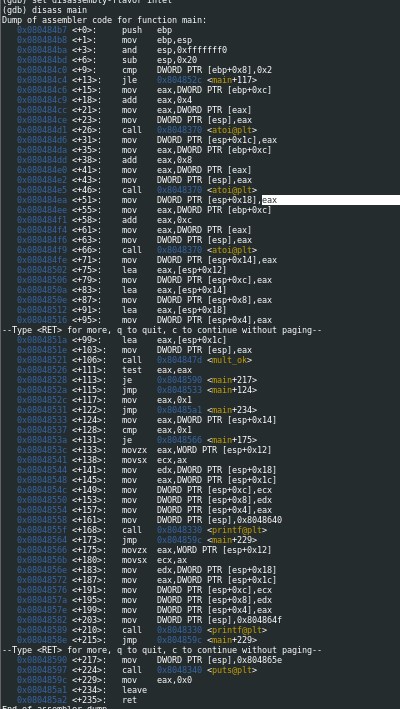
E) Yes, there is a function called “mult\_ok”. It appeared to be created by humans(Maybe aliens too !? But not a standard function)



F) The program requires three inputs. Either integer or string. It converts the string into an integer at the end. The output varies depending on the inputs. But, there are only two possible outputs.

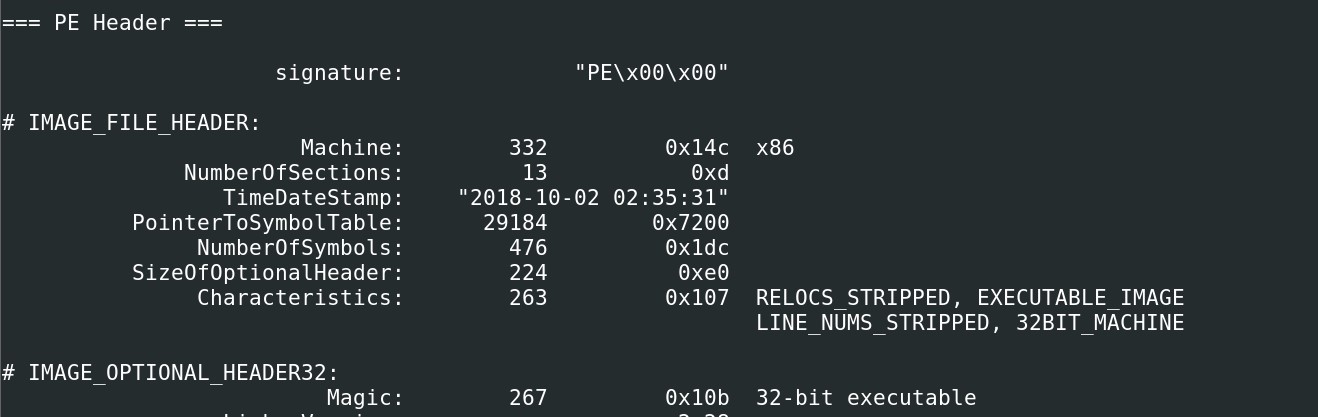


G) atoi, printf and puts are the functions called by the program.



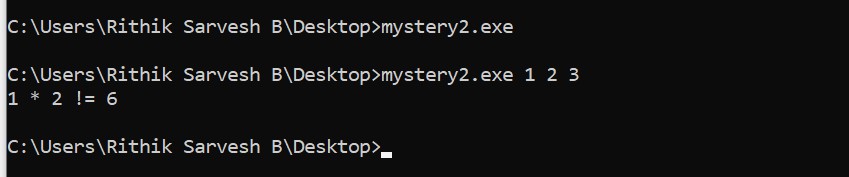
H) The caller clean-up convention or cdecl is the calling convention being used. As the function ends with ret operand, EAX receives the return value and PUSH EBP, MOV EBP, ESP is being done by the callee before the function execution.

mystery2.exe (PE)  
A) It’s a 32-bit executable program



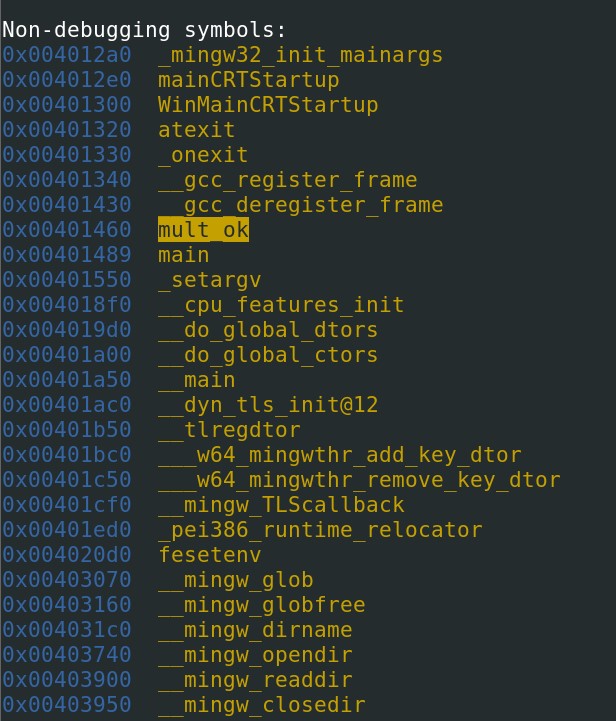
B) The file format is PE .

C) No, The program doesn’t take input once they are started.

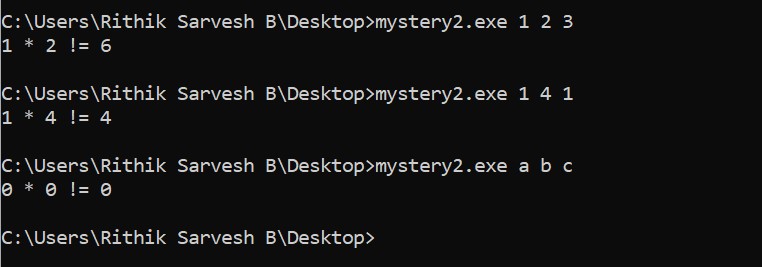


D) Yes, the program accepts input at startup on the command line.

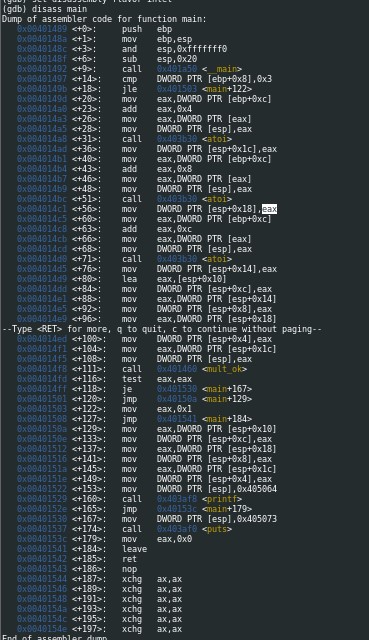
E) Yes, there is a function called “mult\_ok”. It appeared to be created by humans(Maybe aliens too !? But not a standard function)



F) The program requires three inputs. Either integer or string. It converts the string into an integer at the end. The output varies depending on the inputs. But, there are only two possible outputs.



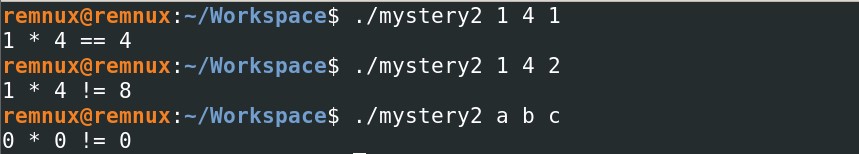
G) atoi, printf and puts are the functions called by the program.



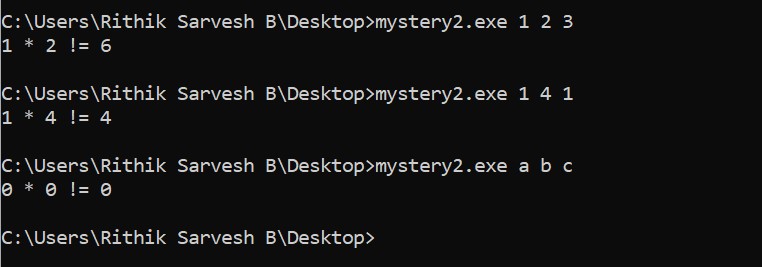
H) The caller clean-up convention or cdecl is the calling convention being used. As the function ends with ret operand, EAX receives the return value and PUSH EBP, MOV EBP, ESP is being done by the callee before the function execution.

1. The file size of mystery2 is 8kb whereas the file size of the mystery2.exe is 41 kb.The difference in size is due to the difference in the standard c library required by the program because of the file format. The another difference between the files is the result. The ELF file produces two types of output whereas the PE file produces the same output irrespective of the result. Because, there was not an another print case in the PE file which was present in the ELF file.

The output of the ELF file



The output of the PE file



strings command shows the difference between the two files.

