CS – Information Security (FALL 2022)
Masood Habib

Submission Guidelines:

- A single violation of guidelines will lead to zero mark in your assignment.
- You are required to make a Microsoft Word file, containing all your codes along with screenshots of every question next to it. Any question without the screenshots will not be accepted. PDF or other format files will not be accepted
- Keep the questions in order. Not following the proper order will result in marks deduction
- Word file format should be "Roll-Number_Section_AssignmentNo", for example *19F0123_A_ assignment02*. Marks will be deducted for not following the correct format.
- Plagiarism will not be tolerated, either done from the internet or from any fellow classmate (of same/different section) and **will lead to zero or negative marks in the assignment.**
- **No late submissions will be accepted.**
- **Assignment evaluation will be viva based**

Question#01 (Format String)

Consider the above code and draw the stack memory layout of the stack of the give function with format String. (2)

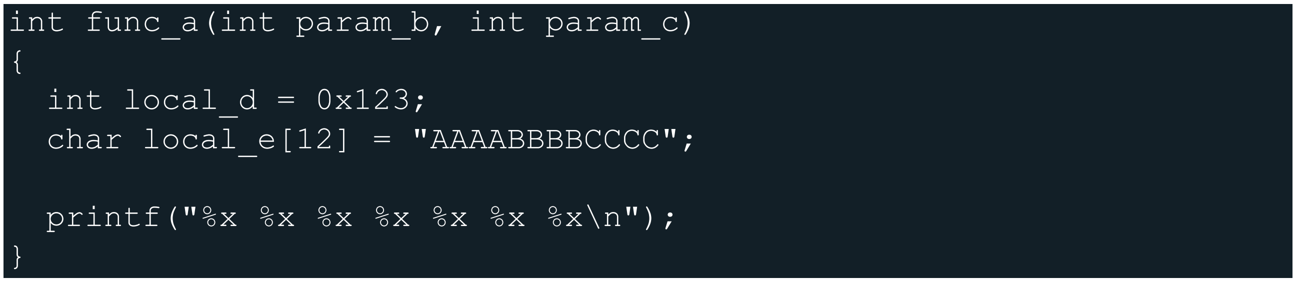
Hint: Param_b = 1000 and Param_c = 10 and draw memory stack when prinf is called

Question#02 (Format String)

Write a C program to read anything on the stack using format String, compile the code and show your output. Discuss your observations?

HINT: DON'T" pass arguments in the Printf function

Question#03 (Buffer overflow)



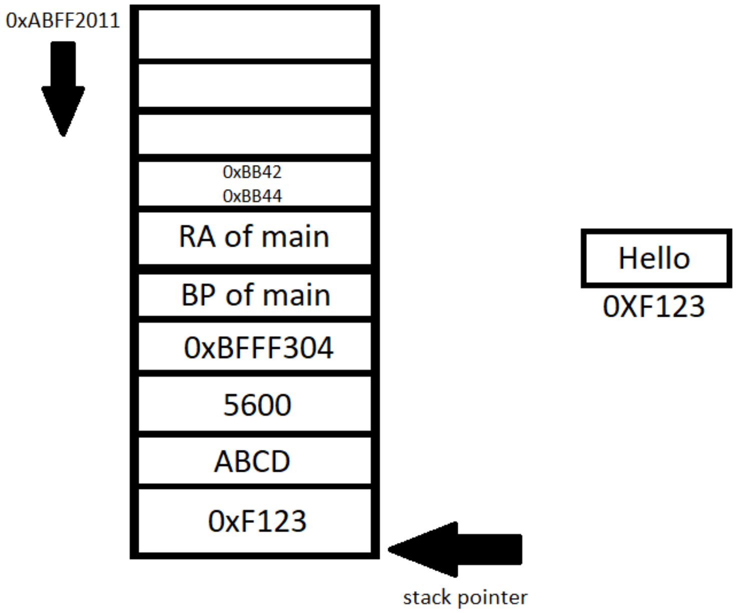
```
int func_a(int param_b, int param_c)
{
  int local_d = 0x123;
  char local_e[12] = "AAAABBBBCCCC";

  printf("%x %x %x %x %x %x %x\n");
}
```

Consider the above code and draw the stack memory layout of the stack of the give function. (3)

Hint: Param_b = 1000 and Param_c = 10

Question#04 (Format String)

Provide the input string which can change help you write "0xA551" at the place of 0xBB42 on the stack:



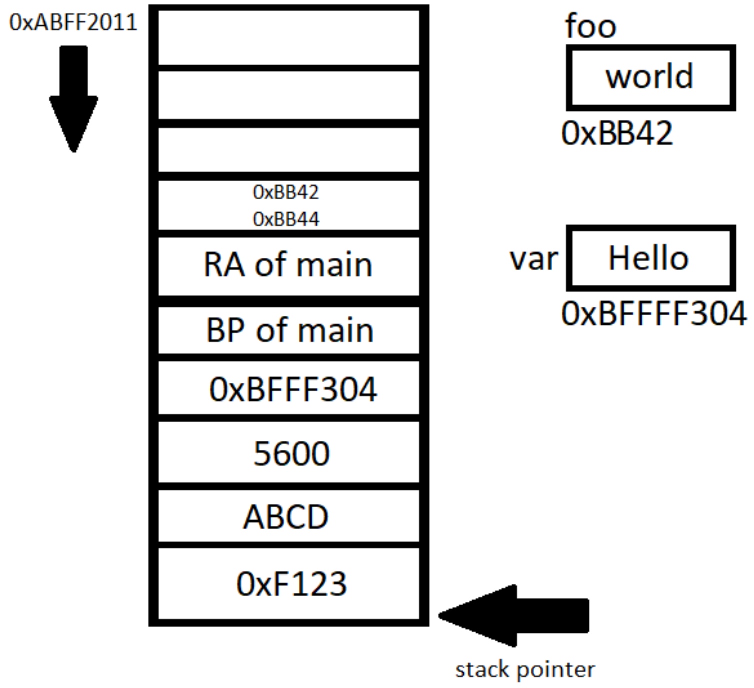
Note: these are half addresses, each having 2 bytes.

Input string:

Explanation:

Question#05 (Format String)

Provide the input string which can display the string stored in var in the memory block and then change it with foo:



Input string for display:

Terminal Output:

Input string for changing the var with foo: