ELEC 334 - Homework #3

Reminders:

- Please read carefully, and answer accordingly.
- Submit your solutions in a PDF file and any additional files asked from you.

Problem 1 `[20 pts]`. **Function calls.**
For Cortex M0+, what registers are used when a C function is called with

A. 1 parameter (e.g. `void func(int a)`)
B. 2 parameters
C. 3 parameters
D. 4 parameters
E. 5 parameters
F. 6 parameters

Explain each case with a simple example (both C and Assembly).

Problem 2 `[5 pts]`. **Return values.**
How does the returned value from a function is handled in Assembly? Explain your answer with an example (e.g. `int func(int a) {... return x; }`)

Problem 3 [`40 pts`]. **Reverse me if you can.**
Our engineers found a hardware wallet, and after long hours of playing with the device, they discovered that it has an STM32G031 based processor that handles all the operations, and they even managed to extract the binary from the device. It uses some mechanism to conceal the password. Reverse the binary to find the password that will get you access to the possible crypto coins. The link to the binary will be shared soon.

Problem 4 [`10 pts`]. **Reading.**
Read "*Reading Faults, Injection Methods, and Fault Attacks*" paper and write a half page summary about different fault injection techniques. Do not copy paste from the article. Try to elaborate the use cases.

Problem 5 [`25 pts`]. **Reading.**
Read Controlling PC on ARM Using Fault Injection paper and write a one page summary about the objective of the paper, their execution, and the implications of these attacks. Then elaborate on the prevention mechanisms.