Assignment #3

Name: _____ ID: _____

This assignment has **1** questions, for a total of **25** marks.

Question 1: **Formalising Isolation à la Intel SGX** ..... 25 marks

Security architectures are necessary to provide secure compilation. Intel SGX provides (roughly speaking) isolation for both code and data at the assembly level so that some memory region is accessible only when the program counter is in a certain memory segment. Fortunately we do not have assembly languages (nor explicit program counters), and fortunately, our languages already provide the kind of code isolation that SGX provides, but the coarse-grained memory isolation is not there.

Remedy this and take the target language (without capabilities but with the contexts that do multiple calls) and add coarse-grained memory isolation. There needs to be a memory that can only be addressed by the function of the program (when it is executing), and not by the context. Define any addition to the syntax and to the semantics that will attain this and argue why the context cannot access this memory.