Assignment #4

Name: _____ ID: _____

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

Question 1: **Formalising Address Space Layout Randomisation (ASLR)** . . . . . 25 marks

Add ASLR to the target language. To do so, read these at least the first (if needed also the second) of these two papers, which formalise ASLR in the context of a lambda calculus:[1]

- Martin Abadi and Gordon D. Plotkin. 2012. On protection by layout randomization. ACM Trans. Info. Syst. Secur. 15, Article 8 (July 2012).
- Radha Jagadeesan, Corin Pitcher, Julian Rathke, and James Riely. 2011. Local memory via layout randomization. In Proceedings of the 2011 IEEE 24th Computer Security Foundations Symposium (CSF'11). IEEE Computer Society, 161âĂŞ174

In our setting, the language models are simpler, since the functions (and the heap) are not higher order. However, the complications are the same, locations in the target are guessable with a certain (negligible) probability, and this is captured by the additional constructions in the target language.

[1] They also devise a compiler and prove it fully abstract, you can safely only focus on the ASLR modelling for now, skipping details about probabilistic contextual equivalence and probabilistic fully abstract compilation.