CS 591 G1—Formal Methods in Security and Privacy—Spring 2020

Assignment 1

Due by Wednesday, February 19, at 5pm

1 Hoare Logic Proofs

In this assignment, you will be writing proofs about programs in EasyCrypt's Hoare logic.

Begin by downloading the files

- `1-assigns-fill.ec`,
- `2-sort3-fill.ec`, and
- `3-expon-fill.ec`

from the course website, and renaming them to

- `1-assigns.ec`,
- `2-sort3.ec`, and
- `3-expon.ec`,

respectively.

For each of these files, your goal is to replace the occurrence or occurrences of the comment `(* fill in *)` by EasyCrypt proofs, in such a way that running EasyCrypt on your file succeeds. You may add supporting lemmas and your own comments, as needed or appropriate.

- The goal of `1-assigns.ec` is to write two simple proofs about a program consisting of assignments.
- The goal of `2-sort3.ec` is to prove the correctness of a program for sorting three integers.
- The goal of `3-expon.ec` is to prove the correctness of a program for ("slow") exponentiation, i.e., raising an integer to a non-negative power. (In the EasyCrypt Lab, Alley will talk about the proof of correctness for "fast" exponentiation.)

2 Assignment Submission by Email

You should submit your assignment by email, only. Create a zip or tar archive containing the three plain text files `1-assigns.ec`, `2-sort3.ec` and `3-expon.ec`, and email it to Alley (`stough@bu.edu`) and Marco (`gaboardi@bu.edu`), with a subject line including the text `[CS591SUB]`.