Writing and Proving Theorems

Description Some of the principles of writing and proving theorems are presented. Due to the strong typing of Cryptol sometimes subtle errors can be caught that would otherwise not be noticed. Such an example is presented. But sometimes the strong typing requires creativity to work around. Such an example is presented. Exercises provided are intermediate level and should help familiarize the learner with the meaning of verification in Cryptol. In particular, one exercise has Cryptol proving the equivalence of two functions although they are not equivalent – but this is perfectly OK in that case.

Purpose Get some practice with theorems and see a few things while working around the strong typing restrictions of Cryptol.

Audience This module is intended for:

1 The general public
2 K-12 and college classes on cyber defense
3 preparation for proficiency in the use of tools and a computing environment suitable for the study of cyber defense

Objectives After completing the module:

1 learner sees that a “golden” standard spec can be applied to many implementations – hence more time can be assigned to specs
2 learner sees that specifications/proofs may be faster with certain provers, depending on the problem, and by using comprehensions instead of recursion
3 learner see that user-defined type signatures are sometimes needed

Keywords property, theorem, proof, monomorphic, polymorphic, type signature, function

Category cybersecurity > education

Delivery java applets and written documentation in pdf format

Team John Franco and Ethan Link

Assessment The applets provide the means for experimentation. Questions are asked in the documentation that help with the set up of experiments. The ideas that learners come up with is evidence that the module was successful.

Workflow No particular schedule was established

Environment All materials are contained in a single jar file. The jar file can be run on any computer where java version 14 or higher and some pdf reader such as acroread or evince are available. The jar file may be executed in the cyber range or learners may download the jar file (which is considered to be an executable file) and run it on their personal computers.