Cryptol: Sequence Comprehensions with Examples

Description One of the basic computational structures in Cryptol is presented with examples to show how comprehensions are used to support computation without side effects.

Purpose Proofs in Cryptol rely on side-effects free specifications.

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 Understand the significance of comprehensions in supporting computation
2 Know how to write a comprehension from a specification
3 Witness the strong typing in Cryptol and its exploitation

Keywords comprehension, side-effects, sequence

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.