Cryptol: Operators, Functions, Comprehensions, Data Types

Description Introduction to aspects of Cryptol including operators, built-in functions, computation structures, data structures, writing functions, recursive functions, working with infinite sequences. Cryptol is very strongly typed and the typing is a bit different from classical typing. However, the typing regime may be exploited for surprising capability and some examples of this are given, especially in the section on Functions.

Purpose A basic introduction to Cryptol before learning how to use Cryptol and SAW to formally verify properties of hardware, software, and protocols

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 Familiarity with the Cryptol language
2 Understand how to use Cryptol to advantage
3 Some small notion of verifying with Cryptol

Keywords function, comprehension, recursion, type signature, sequence, infinite 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 11 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.