

Cryptol: Functions

Description	Create a specification for an assembly program snippet that purports to multiply two 8 bit numbers. Show that the specification is verified to multiply two input numbers.
Purpose	Shows some features of Cryptol that do not exist in most other languages and shows how to set up a specification for low-level programs.
Audience	This module is intended for: <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> 1 setup of a line of code as part of a code specification is understood 2 the value of some Cryptol features, obscure before, now can be appreciated 3 writing access code for a specification, setting up for properties, is revealed
Keywords	multiplier, assembly code, State, tuple
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.