

Cryptol: working with files, commands, basic built-in functions

Description	Illustrate how to use Cryptol to load cry files, express properties, prove properties, find all models, etc.
Purpose	Knowledge of cryptol directives and commands is necessary to write effective specifications and prove properties.
Audience	This module is intended for: <ol style="list-style-type: none">1 The general public2 K-12 and college classes on Cyber Defense and Math Logic3 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 You will know how to use Cryptol to load files, set some system parameters2 You will know some important commands, directives, and built-in functions
Keywords	Math Logic, SMT Solver, SAT solver, ITP Solver, ATP solver, Propositional Logic, First Order Logic, Cryptol, Yices, ABC, Z3, CVC4, Boolector
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.