| galois |

DES SPECIFICATION

01.12.2023

Cryptol: Data Encryption Standard and Weak Keys

Description From a human readable specification of DES, produce a formal specification of DES using Cryptol constructs.

Purpose Provides and refines practice in using Cryptol constructs to formally represent a functional description of the DES encryption and decryption scheme, particularly designing comprehensions and functions.

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 know the DES encryption and decryption scheme
2 know what are weak keys and how to find them using Cryptol constructs on functions defined for the formal specification of DES
3 Understand the design of solutions using comprehensions and functions

Keywords DES, Triple DES, permutation, comprehension, 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.