

WHAT is Cryptol?

Cryptol (www.cryptol.net) is a domain specific language designed in collaboration with the NSA as a standard for specifying cryptographic algorithms. The Cryptol Workbench facilitates the deployment of cryptographic modules across the entire development process, from specification and implementation to verification and certification.

The Cryptol Workbench can significantly reduce the overall lifecycle costs for cryptographic modules by addressing the key cost drivers:

Rapid design cycle

Cryptol specifications are fully executable, allowing designers to experiment incrementally with their designs.

Reusable specification

The Cryptol Workbench can generate software implementations, hardware implementations, and formal models for verification from a single specification.

Accelerated certification

A Cryptol reference specification becomes the formal documentation for the cryptographic module, eliminating the need for separate and voluminous English descriptions. Cryptol verification tools show functional equivalence between the specification and the implementation at each stage of the tool chain.

Galois is offering a four-day Cryptol course for those interested in exploring the capabilities of the Cryptol Workbench. The course is highly participatory: after each topic is introduced, the class will solve a collection of problems.

Prospective participants should have experience writing programs and some knowledge of cryptography. Those who complete the course will have the skills necessary to develop high assurance, high performance cryptographic modules in Cryptol.

DAY 1	DAY 2	DAY 3	DAY 4
<i>Cryptol interpreter</i>	<i>High assurance programming</i>	<i>AES</i>	<i>Q&A session</i>
<i>Basic types</i>	<i>Safety checking</i>	<i>Generating FPGA cores</i>	<i>Your algorithms</i>
<i>Arithmetic</i>	<i>Theorems</i>	<i>Proving hardware correct</i>	<i>Your domain explorations</i>
<i>Functions</i>	<i>Substitution ciphers</i>		<i>Team challenge problem</i>
<i>Recurrences</i>	<i>Verification</i>		

WHO should take the course?

- Cryptographers who want to specify algorithms clearly and unambiguously
- Crypto developers who want a high assurance, high performance path to solutions
- Crypto evaluators who want assurance that a crypto device correctly implements the chosen algorithm

WHEN can I take the course?

- Offered several times a year at Galois headquarters - request a course schedule
- Tuition: \$4000
- Class size: 6-10 students
- Ask for a quote for training at your site.

HOW do I register?

- Contact:
Dr. Sally A. Browning
sally@galois.com
503•808•7151

WHO is teaching the course?

- Galois' mission is to ensure trustworthiness in critical systems. For more than a decade, Galois has applied cutting-edge research to develop new approaches to security and information assurance.
- Dr. John Launchbury is Chief Scientist of Galois, Inc. Prior to founding Galois, John was a full professor in Computer Science and Engineering at the Oregon Graduate Institute School of Science and Engineering at OHSU. His instruction style earned him several awards for outstanding teaching, and he is internationally recognized for his work on the analysis and semantics of programming languages. John holds a Ph.D. in Computing Science from University of Glasgow. In 2010, he was inducted as a Fellow of the Association for Computing Machinery (ACM).

Galois, Inc.

421 SW 6th Ave, Suite 300
Portland, OR 97204
503•626•6616
www.galois.com

