Validation Testing and NIST Statistical Test Suite

July 22, 2004

Larry Bassham
Computer Security Division
National Institute of Standards and Technology

Cryptographic Module Validation Program (CMVP)

- Joint effort between National Institute of Standards and Technology (NIST) and Communications Security Establishment (CSE) of Canada
- National Voluntary Laboratory Accreditation Program (NVLAP)
- http://csrc.nist.gov/cryptval/

Deterministic Generators

- Variable Seed Tests
  - Single seeds of various lengths supported
  - Verify produced bits are as expected
- Monte Carlo Tests
  - Single seed input
  - Produced bits used as subsequent seeds
  - Used to identify implementation flaws

Non-Deterministic Generators

- NIST Statistical Test Suite (needs CSE buy-in)
- Other requirements?

NIST Statistical Test Suite (STS)

- First published in October 2000
- A set of 16 individual tests
- Generally well received, with a few exceptions
  - Lempel-Ziv Compression Test
  - Spectral Test

Enhancements to STS

- Remove Lempel-Ziv Test
- Modify Spectral Test
  - Change constant from 3 to 2.995732274
- Correlation between test
- Combining P-values
- Power of Tests study

- How to adapt for operational testing?