

Statistical Tests for Randomness

Chandrika Lanka
Harini Vasudevan
Swetha Manne

Objective

Study and test the existing Pseudorandom Number Generators using public domain implementation of NIST Statistical Test Suite and integrate the results with KRYPTOS Educational Software.

Abstract:

The need for random and pseudorandom numbers arises in many cryptographic applications like generation of session keys, initialization vectors and creation of public keys. The security of cryptographic systems depends on the generation of unpredictable numbers.

Although several tests exist to evaluate the Pseudorandom Number Generators (RNGs), such as the 16 tests in the NIST Statistical Test Suite, correct interpretation of probabilistic results is critical for final assessment of RNGs. Apart from testing and evaluation of existing PRNGs, our major goal would be good interpretation of test results and integration with KRYPTOS for educational purposes.

Language Platform, and Compiler

NIST Statistical Test Suite package Specification:

Language: ANSI C

Operating System: SunOS

Compiler: ANSI C Compiler

Portability: Platform independent, but minor modifications to be incorporated when ported to other platforms. Successfully ported to SGI Origins and onto IBM PC under Windows 98 and Microsoft C++ 6.0.

We plan to modify the code to work under Windows XP with Microsoft C++.

Input/Output Specification

Input: file of arbitrary length containing binary sequences to be tested for randomness.

Output: Assessment (Pass/Fail) made from results of an output file.

(The output file has results in the form of logs of empirical results that correspond to the computational information)

Functionality

The package performs the selected tests on the user prescribed input and produces a file with proportion of passing sequences for each test and a pass/fail assignment.

Procedures

- The initial step is to download the source code and test it for portability.
- Learn about the working of Random number Generators and Pseudorandom generators. (This test suite has implementations of nine PRNGs)
- Apply Strategy of statistical analysis of RNGs specific to the NIST Test Suite and present an assessment.
- Integrate the test source code with KRYPTOS with input as file of binary sequences and selection of tests, and output in the form of an assessment report of random sequence.

Testing

The results of tests can be compared with sample data of test results of existing RNGs to prove the validity of the tests results.

Schedule

<i>March 5, 2005</i>	<i>Submission of first draft of specification.</i>
<i>March 12, 2005</i>	<i>Submission of final project specification</i>
<i>March 19, 2005</i>	<i>Testing the code for portability on the intended platform complete. Study working of PRNGs and relation of statistical tests to cryptography.</i>
<i>March 26, 2005</i>	<i>Initial run of the code with existing PRNGs and inspection of sample results</i>
<i>March 29, 2005</i>	<i>First Progress Report</i> Detailed presentation of format of input and output functions Results of statistical analysis of half of the existing PRNGs.
<i>April 19, 2005</i>	<i>Second Progress Report</i> Detailed presentation of validity of results of statistical analysis of all the remaining PRNGs. Initiate work on integration with KRYPTOS.
<i>April 26, 2005</i>	Integration with KRYPTOS complete.
<i>May 3, 2005</i>	<i>Third Progress Report</i> Draft version of Final Presentation
<i>May 9, 2005</i>	<i>Draft version of the final written report</i>
<i>May 12, 2005</i>	<i>Review of a draft report of another team due</i>
<i>May 13, 2005</i>	<i>Discussion of the project reports and viewgraphs with the instructor; the instructor's recommendations for revisions.</i>
<i>May 17, 2005</i>	<i>Final oral presentations, final project reports submitted through WebCT.</i>

Possible Changes in Specification

- Platform and Compiler: this may change depending on portability test results.
- Testing of all the pseudorandom generators may not be included due to time constraints.
- References

References

Introduction and Surveys

- [1] "Random number generation," in *The Handbook of Simulation*, pp. 93-137. Wiley, New York, 1998.
- [2] J. E. Gentle, W. Haerdle, and Y. Mori, "Random Number Generation" in the draft for a chapter of the forthcoming *Handbook of Computational Statistics*, Ed. Springer-Verlag, 2004.
- [3] P. Hellekalek, "Good random number generators are (not so) easy to find," *Mathematics and Computers in Simulation*, 46: 485--505, 1998.
- [4] S. Wegenkittl, "On Empirical Testing of Pseudorandom Numbers and Generators," in editor(s), *G. De Pietro, A. Giordano, M. Vajtersic, P. Zinterhof Proceedings of the international workshop Parallel Numerics '95*. CEI-PACT Project, WP5.1.2.1.2. , 1995.
- [5] G. Marsaglia, "A current view of random number generators," in *Billard, L., editor(s), Computer Science and Statistics: The Interface*, pp. 3--10. Elsevier Science Publishers B.V., Amsterdam, 1985.
- [6] S. L. Anderson, *Random number generators on vector supercomputers and other advanced architectures*. SIAM pp. 221-251, 1990.
- [7] B. D. Ripley, *Thoughts on pseudorandom number generators*. J. Comput. Appl. Math. , 31: 153--163, 1990.

Mathematical Foundations and Philosophy

- [1] T. Ritter, *Randomness Links*. Available: <http://www.ciphersbyritter.com/NETLINKS.HTM>
- [2] G. J. Chaitin, *Randomness and mathematical proof*. Sci. Amer., 232: 47--52, 1975.
- [3] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions*, Applied

Mathematics Series. Vol. 55, Washington: National Bureau of Standards, 1964; reprinted 1968 by Dover Publications, New York.

Cryptographical Generators

- [1] J. C. Lagarias, *Pseudorandom Numbers*. Statistical Science, 8: 31--39, 1993
- [2] M. Blum and S. Micali, "How to generate cryptographically strong sequences of pseudo-random bits," SIAM Journal of Computing, 13: 850--864, 1984
- [3] M. Luby, *Pseudorandomness and Cryptographic Applications*. Princeton Computer Science Notes, 1996.
- [5] A. Menezes van P. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, Boca Raton, 1997.
- [6] Schneier, B.: Applied Cryptography. Wiley, New York, Second edition, 1996.
- [7] Revised NIST Special Publication 800-22, "A Statistical Test Suite for the validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications". Available: <http://csrc.nist.gov/rng/rng2.html>
- [8] "Statistical testing of Random Number Generators". *Proceedings of the 22nd National Information Systems Security Conference, 10/99*.