December 2000

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

A STATISTICAL TEST SUITE FOR RANDOM AND PSEUDORANDOM NUMBER GENERATORS FOR CRYPTOGRAPHIC APPLICATIONS

By Elaine B. Barker, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology

Introduction

Random and pseudorandom numbers are needed for many cryptographic applications. For example, common cryptosystems employ keys that must be generated in a random fashion. Many cryptographic protocols also require random or pseudorandom inputs at various points, e.g., for auxiliary quantities used in generating digital signatures or for generating challenges in authentication protocols.

NIST Special Publication (SP) 800-22, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, discusses the randomness testing of random number and pseudorandom number generators (RNGs and PRNGs) that may be used for many purposes including cryptographic, modeling, and simulation applications. Co-authors of the document from ITL's Computer Security and Statistical Engineering Divisions include Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, and San Vo. The publication and the associated tests are intended for individuals who are responsible for the testing and evaluation of random and pseudorandom number generators, including (P)RNG developers and testers.

The document focuses on those applications where randomness is required for cryptographic purposes such as the generation of keying material. A set of statistical tests for randomness is described; the statistical tests and NIST SP 800-22 are available at http://csrc.nist.gov/rng/.

General Discussion

There are two basic types of generators used to produce random sequences: random number generators and pseudorandom number generators. A random number generator uses a non-deterministic source (i.e., some unpredictable physical source) to produce random bits. A pseudorandom number generator produces a sequence of bits from an initial value called a seed using a known algorithm.

Various statistical tests can be applied to a sequence produced by such generators to compare and evaluate the sequence for randomness. The distribution of outcomes of statistical tests, when applied to a truly random sequence, is known *a priori* and can be described in probabilistic terms. However, no set of statistical tests, including these tests, is sufficient to certify the randomness of a generator; the analysis of the generator's design (e.g., cryptanalysis) is also required.

The Statistical Tests

The NIST Statistical Test Suite is a package of 16 tests that were developed to test the randomness of (arbitrarily long) binary sequences produced by random or pseudorandom number generators. The tests focus on a variety of different types of non-randomness that could exist in a sequence.

Each test is based on a calculated test statistic value, which is a function of the tested sequence. The test statistic is used to calculate a P-value that summarizes the strength of the evidence for randomness. Each P-value can be interpreted as the probability that a perfect random number generator would have produced a sequence less random than the sequence that

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8901, Gaithersburg, MD 20899-8901, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since May 1999

was tested, given the kind of non-randomness assessed by the test. The use of P-values is intended to allow an individual testing a generator to easily and objectively interpret the test results and assess the quality of the generator.

NIST SP 800-22 provides a high-level description and examples for each of the 16 tests in the test suite, along with the mathematical background for each test. In addition, the document provides guidance for specifying the parameters required for the tests and for interpreting the test results, both on a single sequence for a given test and for multiple sequences for that test.

The 16 statistical tests contained in the test suite are:

1. The Frequency (Monobit) test determines whether the number of ones and zeros in a tested sequence are approximately ½, as is expected for a truly random fair binary sequence. All subsequent tests depend on the passing of this test.
2. The Test for Frequency within a Block determines whether the frequency of ones in an M-bit block of the tested sequence is approximately M/2, as would be expected under an assumption of randomness.
3. The Runs test is used to determine whether the total numbers of runs of ones and zeros of various lengths is as expected for a random sequence. The runs test can be thought of as determining whether the oscillation between zeros and ones is too fast or too slow.
4. The Test for the Longest-Run-of-Ones in a Block determines whether the longest run of ones within an M-bit block of the tested sequence is consistent with the length of the longest run of ones that would be expected in a random sequence of M bits.
5. The Random Binary Matrix test uses disjoint submatrices formed from the entire sequence to check for linear dependence among fixed length substrings of the tested sequence.
6. The Discrete Fourier Transform (Spectral) test uses the peak heights of the Discrete Fast Fourier Transform of the tested sequence to detect periodic features (i.e., repetitive patterns) that would indicate a deviation from the assumption of randomness.
7. The Non-overlapping Template Matching test determines whether there are too many occurrences of predefined aperiodic patterns.
8. The Overlapping Template Matching test also determines whether there are too many occurrences of predefined patterns. Note that for both the overlapping and non-overlapping matching template tests, if the pattern is not found, the match window slides one bit position. If the pattern is found, the match window slides one bit position before resuming the overlapping test, whereas the match window slides m bit positions for the non-overlapping test, where m is the length of the pattern.
9. Maurer's "Universal Statistical" test determines whether or not the tested sequence can be significantly compressed without loss of information. It achieves this by evaluating the distribution of the average distances between patterns occurring in the sequence. The averaging is performed over the numbers of digits in the binary expansions of those distances.
10. The Lempel-Ziv Compression test examines the number of cumulatively distinct patterns in the test sequence in order to determine how far the sequence can be compressed. A truly random sequence will have a characteristic number of distinct patterns.
11. The Linear Complexity test determines whether or not the sequence is complex enough to be considered random. This is accomplished by examining the sequence to determine the length of a linear feedback shift register (LFSR) that would produce the sequence. A short feedback register implies non-randomness.
12. The Serial test checks for the uniformity of the distribution(s) of overlapping m-bit patterns for varying pattern lengths, m. Random sequences exhibit uniformity: every m-bit pattern should appear as frequently as every other m-bit pattern, on average.
13. The Approximate Entropy test compares the frequency of overlapping blocks of two consecutive lengths (m and m+1) against the expected result for a random sequence.
14. The Cumulative Sums (Cusums) test determines whether the maximum absolute value of the cumulative sum of the partial sequences occurring in the tested sequence is too large or too small relative to the expected behavior of such a cumulative sum for random sequences. The cumulative sum may be considered as a random walk. For a random sequence, the random walk should oscillate around zero. Large values of the walk indicate too many zeros or ones near the start of the sequence. Small values indicate that the zeros and ones are intermixed too evenly.
15. The Random Excursions test determines if the numbers of visits of the cumulative sum random walk to integer levels ("states") between successive zero level crossings distribute as expected for a truly random sequence.
16. The Random Excursions Variant test extends the Random Excursions test by examining level crossing distributions across multiple excursions between zero level crossings.

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our Web site is http://www.itl.nist.gov/.

The Test Code

The source code for the tests was developed in ANSI C on a SUN™ workstation running under the Solaris™ operating system. Other systems may require modifications to the source code to run properly.

Instructions are provided in NIST SP 800-22 for installing, modifying, and operating the test code and interpreting the results. Sample generators are provided along with the test code that can be used to run with the tests and compare against the expected results that are provided in the document.

Empirical Studies

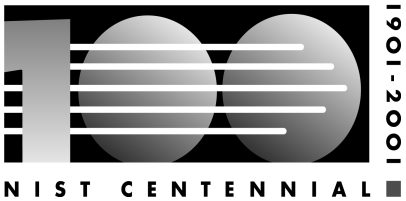
Over the course of this project, several empirical studies were conducted to ascertain whether the statistical tests were properly developed and implemented. These studies were employed to demonstrate the usefulness of each of the statistical tests. Both "good" and "bad" generators were used to assess the quality of the tests. Codes for these generators have been made available with the test code. In addition, the tests were used to ascertain the randomness of the algorithm candidates for the Advanced Encryption Standard (AES). An appendix to NIST SP 800-22 describes results for the generators provided with the test code, while NISTIR 6390 and NISTIR 6483 describe the results of testing algorithm candidates for the AES. All documents are available at http://csrc.nist.gov/rng.

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.

Sun™ and Solaris™ are trademarks of Sun Microsystems, Inc. in the United States and other countries.

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.



U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8901
Gaithersburg, MD 20899-8901