NIST

National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-22
Revision 1a

A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications

Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, San Vo

Revised: April 2010
Lawrence E Bassham III

NIST Special Publication 800-22
Revision 1a

A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications

Andrew Rukhin[1], Juan Soto[2], James Nechvatal[2], Miles Smid[2], Elaine Barker[2], Stefan Leigh[1], Mark Levenson[1], Mark Vangel[1], David Banks[1], Alan Heckert[1], James Dray[2], San Vo[2]

Revised: April 2010
Lawrence E Bassham III[2]

C O M P U T E R   S E C U R I T Y

[1]Statistical Engineering Division
[2]Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

Revised: April 2010

U.S. Department of Commerce

Gary Locke, Secretary

National Institute of Standards and Technology

Patrick Gallagher, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-22 revision 1a
Natl. Inst. Stand. Technol. Spec. Publ. 800-22rev1a, 131 pages (April 2010)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Table of Contents

Abstract **1**

1. Introduction to Random Number Testing **1-1**

1.1 General Discussion 1-1
1.1.1 Randomness 1-1
1.1.2 Unpredictability 1-1
1.1.3 Random Number Generators (RNGs) 1-2
1.1.4 Pseudorandom Number Generators (PRNGs) 1-2
1.1.5 Testing 1-2
1.1.6 Considerations for Randomness, Unpredictability and Testing 1-5
1.2 Definitions 1-5
1.3 Abbreviations 1-8
1.4 Mathematical Symbols 1-8

2. Random Number Generation Tests **2-1**

2.1 Frequency (Monobit) Test 2-2
2.1.1 Test Purpose 2-2
2.1.2 Function Call 2-2
2.1.3 Test Statistic and Reference Distribution 2-2
2.1.4 Test Description 2-2
2.1.5 Decision Rule (at the 1% Level) 2-3
2.1.6 Conclusion and Interpretation of Results 2-3
2.1.7 Input Size Recommendation 2-3
2.1.8 Example 2-3
2.2 Frequency Test within a Block 2-4
2.2.1 Test Purpose 2-4
2.2.2 Function Call 2-4
2.2.3 Test Statistic and Reference Distribution 2-4
2.2.4 Test Description 2-4
2.2.5 Decision Rule (at the 1% Level) 2-5
2.2.6 Conclusion and Interpretation of Results 2-5
2.2.7 Input Size Recommendation 2-5
2.2.8 Example 2-5
2.3 Runs Test 2-5
2.3.1 Test Purpose 2-5
2.3.2 Function Call 2-6
2.3.3 Test Statistic and Reference Distribution 2-6
2.3.4 Test Description 2-6
2.3.5 Decision Rule (at the 1% Level) 2-7
2.3.6 Conclusion and Interpretation of Results 2-7
2.3.7 Input Size Recommendation 2-7
2.3.8 Example 2-7
2.4 Test for the Longest Run of Ones in a Block 2-7
2.4.1 Test Purpose 2-7
2.4.2 Function Call 2-8
2.4.3 Test Statistic and Reference Distribution 2-8
2.4.4 Test Description 2-8
2.4.5 Decision Rule (at the 1% Level) 2-9

2.4.6 Conclusion and Interpretation of Results 2-9
2.4.7 Input Size Recommendation 2-9
2.4.8 Example 2-9
2.5 Binary Matrix Rank Test........ 2-10
2.5.1 Test Purpose........ 2-10
2.5.2 Function Call 2-10
2.5.3 Test Statistic and Reference Distribution 2-10
2.5.4 Test Description 2-10
2.5.5 Decision Rule (at the 1% Level)........ 2-11
2.5.6 Conclusion and Interpretation of Results 2-12
2.5.7 Input Size Recommendation 2-12
2.5.8 Example 2-12
2.6 Discrete Fourier Transform (Spectral) Test 2-12
2.6.1 Test Purpose........ 2-12
2.6.2 Function Call 2-12
2.6.3 Test Statistic and Reference Distribution 2-13
2.6.4 Test Description 2-13
2.6.5 Decision Rule (at the 1% Level)........ 2-14
2.6.6 Conclusion and Interpretation of Results 2-14
2.6.7 Input Size Recommendation 2-14
2.6.8 Example 2-14
2.7 Non-overlapping Template Matching Test 2-14
2.7.1 Test Purpose........ 2-14
2.7.2 Function Call 2-14
2.7.3 Test Statistic and Reference Distribution 2-15
2.7.4 Test Description 2-15
2.7.5 Decision Rule (at the 1% Level)........ 2-16
2.7.6 Conclusion and Interpretation of Results 2-16
2.7.7 Input Size Recommendation 2-16
2.7.8 Example 2-16
2.8 Overlapping Template Matching Test 2-17
2.8.1 Test Purpose........ 2-17
2.8.2 Function Call 2-17
2.8.3 Test Statistic and Reference Distribution 2-17
2.8.4 Test Description 2-17
2.8.5 Decision Rule (at the 1% Level)........ 2-19
2.8.6 Conclusion and Interpretation of Results 2-19
2.8.7 Input Size Recommendation 2-19
2.8.8 Example 2-19
2.9 Maurer's "Universal Statistical" Test 2-20
2.9.1 Test Purpose........ 2-20
2.9.2 Function Call 2-20
2.9.3 Test Statistic and Reference Distribution 2-20
2.9.4 Test Description 2-20
2.9.5 Decision Rule (at the 1% Level)........ 2-23
2.9.6 Conclusion and Interpretation of Results 2-23
2.9.7 Input Size Recommendation 2-23
2.9.8 Example 2-23
2.10 Linear Complexity Test 2-24
2.10.1 Test Purpose........ 2-24
2.10.2 Function Call 2-24

2.10.3 Test Statistic and Reference Distribution 2-24
2.10.4 Test Description 2-24
2.10.5 Decision Rule (at the 1% Level) 2-26
2.10.6 Conclusion and Interpretation of Results 2-26
2.10.7 Input Size Recommendation 2-26
2.10.8 Example 2-26
2.11 Serial Test 2-26
2.11.1 Test Purpose 2-26
2.11.2 Function Call 2-26
2.11.3 Test Statistic and Reference Distribution 2-27
2.11.4 Test Description 2-27
2.11.5 Decision Rule (at the 1% Level) 2-28
2.11.6 Conclusion and Interpretation of Results 2-28
2.11.7 Input Size Recommendation 2-28
2.11.8 Example 2-28
2.12 Approximate Entropy Test 2-29
2.12.1 Test Purpose 2-29
2.12.2 Function Call 2-29
2.12.3 Test Statistic and Reference Distribution 2-29
2.12.4 Test Description 2-29
2.12.5 Decision Rule (at the 1% Level) 2-30
2.12.6 Conclusion and Interpretation of Results 2-30
2.12.7 Input Size Recommendation 2-30
2.12.8 Example 2-31
2.13 Cumulative Sums (Cusum) Test 2-31
2.13.1 Test Purpose 2-31
2.13.2 Function Call 2-31
2.13.3 Test Statistic and Reference Distribution 2-31
2.13.4 Test Description 2-31
2.13.5 Decision Rule (at the 1% Level) 2-33
2.13.6 Conclusion and Interpretation of Results 2-33
2.13.7 Input Size Recommendation 2-33
2.13.8 Example 2-33
2.14 Random Excursions Test 2-33
2.14.1 Test Purpose 2-33
2.14.2 Function Call 2-34
2.14.3 Test Statistic and Reference Distribution 2-34
2.14.4 Test Description 2-34
2.14.5 Decision Rule (at the 1% Level) 2-37
2.14.6 Conclusion and Interpretation of Results 2-37
2.14.7 Input Size Recommendation 2-37
2.14.8 Example 2-37
2.15 Random Excursions Variant Test 2-38
2.15.1 Test Purpose 2-38
2.15.2 Function Call 2-38
2.15.3 Test Statistic and Reference Distribution 2-38
2.15.4 Test Description 2-38
2.15.5 Decision Rule (at the 1% Level) 2-39
2.15.6 Conclusion and Interpretation of Results 2-39
2.15.7 Input Size Recommendation 2-40
2.15.8 Example 2-40

3. Technical Description of Tests 3-1

3.1 Frequency (Monobits) Test 3-1
3.2 Frequency Test within a Block 3-1
3.3 Runs Test 3-2
3.4 Test for the Longest Run of Ones in a Block 3-3
3.5 Binary Matrix Rank Test 3-5
3.6 Discrete Fourier Transform (Specral) Test 3-6
3.7 Non-Overlapping Template Matching Test 3-9
3.8 Overlapping Template Matching Test 3-12
3.9 Maurer's "Universal Statistical" Test 3-13
3.10 Linear Complexity Test 3-15
3.11 Serial Test 3-18
3.12 Approximate Entropy Test 3-19
3.13 Cumulative Sums (Cusum) Test 3-21
3.14 Random Excursions Test 3-22
3.15 Random Excursions Variant Test 3-24

4. Testing Strategy and Result Interpretation 4-1

4.1 Strategies for the Statistical Analysis of an RNG 4-1
4.2 The Interpretation of Empirical Results 4-2
4.2.1 Proportion of Sequences Passing a Test 4-2
4.2.2 Uniform Distribution of *P-values* 4-3
4.3 General Recommendations and Guidelines 4-3
4.4 Application of Multiple Tests 4-6

5. User's Guide 5-1

5.1 About the Package 5-1
5.2 System Requirements 5-1
5.3 How to Get Started 5-2
5.4 Data Input and Output of Empirical Results 5-3
5.4.1 Data Input 5-3
5.4.2 Output of Empirical Results 5-3
5.4.3 Test Data Files 5-3
5.5 Program Layout 5-3
5.5.1 General Program 5-3
5.5.2 Global Parameters 5-4
5.5.3 Mathematical Software 5-4
5.6 Running the Test Code 5-5
5.7 Interpretation of Results 5-7

List of Appendices

Appendix A— Source Code A-1

A.1 Hierarchical Directory Structure A-1
A.2 Configuration Information A-3

Appendix B— Empirical Results for Sample Data B-1

Appendix C— Extending the Test Suite C-1

C.1 Incorporating Additional Statistical Tests C-1
C.2 Incorporating Additional PRNGs C-2

Appendix D— Description of Reference Pseudorandom Number Generators................ D-1

D.1 Linear Congruential Generator (LCG) D-1
D.2 Quadratic Congruential Generator I (QCG-I)... D-1
D.3 Quadratic Congruential Generator II (QCG-II)... D-1
D.4 Cubic Congruential Generator II (CCG)... D-2
D.5 Exclusive OR Generator (XORG) D-2
D.6 Modular Exponentiation Generator (MODEXPG) D-2
D.7 Secure Hash Generator (G-SHA1) D-3
D.8 Blum-Blum-Shub (BBSG) D-3
D.9 Micali-Schnorr Generator (MSG) D-4
D.10 Test Results D-5

Appendix E— Numerical Algorithm Issues E-1

Appendix F— Supporting Software F-1

F.1 Rank Computation of Binary Matrices F-1
F.2 Construction of Aperiodic Templates...F-4
F.3 Generation of the Binary Expansion of Irrational Numbers F-7

Appendix G— References... G-1