Eyecon Alderney Limited

RNG Certification Report

Report No.: EYE-RNG_20160025
Version: 1.0
Date: 16 May 2016

Enex Pty Ltd (Trading as: Enex TestLab)
ABN 77 096 299 099

Accredited for compliance with ISO/IEC 17025
Accreditation Number 15589

Version Control

Version	Date	Status	Author	Description
0.1	3/05/2016	Draft	Eric Lozano	Initial
1.0	16/05/2016	Final	Kire Terzievski	Reviewed and approved for release

Table of Contents

1. General Information

No.	Description	Details
1.	Test Laboratory and Address:	Enex TestLab Unit 10, 355-365 South Gippsland Highway, Dandenong VIC 3175
2.	Enex TestLab's Project Manager	Kire Terzievski Operations Manager +61 3 8899 6402 kiret@testlab.com.au
3.	Licensee Name and Address:	Eyecon Alderney Limited New Century House 2 Jubilee Terrace, South Esplanade St Peter Port, Guernsey, GY1 1AH
4.	Eyecon Alderney Limited's Contact	Liam Wickham Tel: +44 (0) 1481 714 777 Mob: +44 7781 162 098
5.	Project Name:	RNG
6.	Evaluation Type:	RNG
7.	Evaluation Period:	14/04/2016 to 3/05/2016
8.	Enex Report Reference:	EYE-RNG_20160025
9.	Previous Report Reference:	NA
10.	Certificate Reference:	RNG-ENEX-20160506
11.	Jurisdiction:	UK, Alderney
12.	Regulator:	UKGC, AGCC
13.	Applicable Standards:	AGCC - Technical Standards and Guidelines for Internal Control Systems and Internet Gambling Systems, Version 4.1. UKGC - Remote gambling and software technical standards, first published August 2009, updated July 2015.

2. Evaluation Summary

2.1 *Submission*

Enex TestLab ("Enex") was engaged by Eyecon Alderney Limited to perform an evaluation of the *Random Number Generator (RNG)* for use within the jurisdiction of UK as regulated by UKGC. RNG Version 1.0.1 was tested with the aim of verifying compliance with the following sets of standards:

- AGCC's *Technical Standards and Guidelines for Internal Control Systems and Internet Gambling Systems, Version 4.1.*
- UKGC's *Remote gambling and software technical standards, first published August 2009, updated July 2015.*
- UKGC' *Testing strategy for compliance with remote gambling and software technical standards, first published June 2014, updated July 2015.*

2.2 *Objective*

The evaluation main objectives were to measure the statistical properties the RNG's to assess whether it is suitable for its intended use and identify any potential contraventions to regulations *(refer to section 6 for full details of the evaluation findings)*.

Throughout the test, the following RNG properties were verified:

- Choice of algorithm
- Integrity and Fairness
- Period
- Range
- Seeding / Re-seeding
- Background Cycling
- Scaling and Mapping
- Mechanism to detect and handle RNG failures

2.3 *Testing Criteria*

Alderney

Testing was completed against relevant provisions of section *4.3 Random Number Generator (RNG) Requirements* of the AGCC's standards.

UK

The evaluation was completed against Level 1 testing criteria as indicated in UKGC's *Testing strategy for compliance with remote gambling and software technical standards,* and incorporated a theoretical assessment and the execution statistical test suits namely DIEHARD tests and Final Outcome Distributions tests *(refer to section 5 for a full description of the testing methodology)*.

2.4 *Evaluation Conclusion and Certificate Statement*

Subject to the limitations discussed in section *3 – Disclaimer and Comments*, Enex TestLab certifies that the RNG complies with all applicable sections of the set of standards listed above.

Accordingly, Enex TestLab recommends the approval of the RNG, as identified in section ***4*** *– Software Identification,* for operation in UK, as regulated by the UKGC.

Mr. Kire Terzievski
Operational Manager

3. Disclaimer and Comments

The RNG may only be used on gaming products that call the RNG with numbers within the ranges as specified in this report.

There is a call for method setseed (`SHA1PRNGAdapter final String seed`) in the SHA1PRNG Adapter class. This call must never be called in live games. This call may only be used for predetermined outcomes for the testing purpose only.

When using the SHA1PRNG, Eyecon should consider modifying the RNG to always call `java.security.SecureRandom.nextBytes(byte[])` immediately after creating a new instance of the PRNG. This will force the PRNG to seed itself securely.

There are unavoidable limitations inherent to performing evaluations within a laboratory environment. It is not possible to verify the effects of all potential configurations and environments that may occur during field operations in actual gaming venues or equipment.

4. RNG Identification and Hardware Configuration

4.1 *RNG*

The Random Number Generator and associated classes can be identified as follows:

Description	Details
RNG Type	Software
RNG Algorithm	RNG algorithm is based on SecureRandom class of Java *(refer to section 6.1 for full details)*.
Group	com.eyecon.common
Artefact	eyecon-rng
Version	1.0.1
SHA-1	d2bfe8ef8fb4f0c33d2988f9a2a030fd66a295f9
MD5	35404c0d27ae6299128144007e930520

4.2 *Hardware*

Data sets used for the evaluation of the RNG were generated using the following system configuration.

	Description
Operating System	GNU/Linux - CentOS Linux release 7.1.1503 (Core)
Service Pack	3.10.0-229.14.1.el7.x86_64 #1 SMP Tue Sep 15 15:05:51 UTC 2015
Processor Type	x86_64
Processor Speed	Intel(R) Xeon(R) CPU E5-2660 v3 @ 2.60GHz
RAM Type	DDR3
RAM Size	8188 MB
Java Version	java version "1.8.0_92" Java(TM) SE Runtime Environment (build 1.8.0_92-b14) Java HotSpot (TM) 64-Bit Server VM (build 25.92-b14, mixed mode)

5. Testing Methodology

The evaluation comprised a combination of testing techniques and reviews that are standard for this type of evaluation. Testing occurs in stages as specified below:

- Stage 1 - Theoretical Analysis
- Stage 2 - DIEHARD Tests
- Stage 3 - Final Outcome Distribution Tests

The first stage involves a general analysis of the RNG implementation. The second and third stages involve well known statistical tests that measure the RNG randomness and un-predictability. The tests take many sequences of random numbers from a given generator and subject them to a battery of statistical tests. As the sequences pass more of the tests, the confidence in the randomness of the numbers increases and so does the confidence in the generator.

More details about each stage are provided below.

5.1 *Theoretical Analysis*

A theoretical assessment of the Random Number Generator's properties, which included but not limited to the following:

- Identification of RNG algorithm and potential known weaknesses
- Verification of the unpredictability and non-repeatability characteristics of the implementation
- Verification of seeding, reseeding and background cycling

5.2 *DIEHARD Tests*

The diehard tests are battery of statistical tests for measuring the quality of a random number generator. The tests are industry standard and are performed on the raw RNG outcomes (i.e., before scaling and mapping).

Diehard includes the following tests:

1. Birthday Spacings
2. Overlapping permutations
3. Ranks of matrices
4. Bitstream
5. OPSP
6. OQSO
7. DNA
8. Count the 1s
9. Parking lot
10. Minimum distance
11. 3D Spheres
12. The squeeze
13. Overlapping sums
14. Runs
15. Craps

Refer to Appendix B- DIEHARD Test Definitions for more information about what each test entails.
https://en.wikipedia.org/wiki/Diehard_tests

5.2.1 DIEHARD Test Results Interpretation

All the above statistical tests produce P-Values and KS-Values. P-Value is a parameter that must be within the pass range between zero and one, which is an indication that the test data contains truly independent random bits. The KS-Value allows for a more accurate judgment of the test results.

The results are provided in the format (a/b/c), where:

- "a" represents values that always occur for the particular test
- "b" values that are required to pass the test
- "c" are the actual values obtained from testing

5.3 Final Outcome Distribution Tests

The Final Outcome Distribution Tests are battery of statistical tests that measures the RNG randomness after scaling and mapping have occurred.

Final Outcome Distribution tests are recognised gaming industry standard tests and comprises the following elements:

1. Equi-Distribution Test
2. Serial Test
3. Coupon Collector's Test

5.3.1 Equi-Distribution Test

The Equi-Distribution Test is a common statistical test, also known as the Frequency Test. Enex Testlab applies the Equi-Distribution Test to integer-valued number sequences within a sample size to help determine the level of randomness. Consider the following sequence: $X_n = X_0, X_1, X_2, X_3$, etc., $(0 <= X_n <= y)$. y = highest possible value of application's scaled and mapped outcomes. r = the number of times that X_m (any single value within X_n) appears within the entire sample size. Apply the chi-squared test using d = degrees of freedom + 1 and probability $p_s = 1/d$ for each value of X_m.

The focus of this test is the proportion of zeroes and ones for the entire sequence. The purpose of this test is to determine whether that number of ones and zeros in a sequence are approximately the same as would be expected for a truly random sequence. The test assesses the closeness of the fraction of ones to ½, that is, the number of ones and zeroes in a sequence should be about the same.

5.3.2 Serial Test

The serial Test is a common statistical test. This test will test pairs of successive outcomes within a sample size. It will determine whether all possible pairs occur with a uniform distribution (i.e.: does each possible pair occur an acceptable number of times throughout the sample size). To perform the serial test, count the number of times that the pair $(X_{2m}, X_{2m+1}) = (q, r)$, for $0 < m < f$ (where f = degrees of freedom / 2 (rounded up)). These counts are to be made for each pair of integers (q, r), for $0 < q < d$ (where d = degrees of freedom + 1). Apply the chi-squared test to d^2 pairs with a probability of $1 / d^2$ for each pair.

The focus of this test is the frequency of each and every overlapping m-bit pattern across the entire sequence. The purpose of this test is to determine whether the number of occurrences of the 2m m-bit overlapping patterns is approximately the same as would be expected for a random sequence. The pattern can overlap.

5.3.3 Coupon Collector Test

The Coupon Collector's Test is a common statistical test. Generate random integers in [0, d-1]. Tally up sequential outcomes within the sequence until at least one instance of each of the d integers is found, and note the length of the segment over which this complete set was found. For example, if d = 3 and the sequence is: 1101221022120202001212200102011 21…, then the length of the segments over which we found a complete set was 5,3,5,6,5,4, and 5.

11012, 210, 22120, 202001, 21220, 0102, 01121, …
5 3 5 6 5 4 5

Continue from the next position in the sequence until n complete sets (in the above example n = 7). The distribution of lengths of segments is compared to the expected distribution.

The coupon collectors test examines the random number generator output for covers; i.e., sub-sequences which contain at least one of each category of values and which do not contain covers as proper sub-sequences themselves.

6. Evaluation Findings

6.1 *General RNG Analysis*

6.1.1 Algorithm

RNG algorithm is based on SecureRandom class of Java.

This class provides a cryptographically strong random number generator (RNG).

A cryptographically strong random number minimally complies with the statistical random number generator tests specified in *FIPS 140-2, Security Requirements for Cryptographic Modules,* section 4.9.1. Additionally, SecureRandom must produce non-deterministic output. Considering that seed material passed to a SecureRandom object are provided by hardware entropy resources, therefore all SecureRandom output sequences are cryptographically strong, as described in *RFC 1750: Randomness. Recommendations for Security.*

A caller obtains a SecureRandom instance via the argument constructor of the following `getInstance` methods:

```
random = SecureRandom.getInstance("SHA1PRNG", "SUN");
```

After this call the system will determine if there is an implementation of the algorithm in the package requested, and throw an exception if there is not.

The SecureRandom implementation attempts to completely randomize the internal state of the generator itself, since there is no call to the setseed.

6.1.2 Period

The period of SHA1PRNG is $2^{159.}$

Furthermore, reseeding of RNG is performed by hardware. Using this re-seeding method means the RNG period will never repeat itself (i.e. making the period undefined). Having an infinite period causes the RNG to act like hardware RNG.

6.1.3 Range

The method called to enforce the RNG to be seeded using system entropy has the range of 32 bits (4,294,967,296). This has been done by calling **`the method long`** `next()` in SHA1PRNGAdapter class.

The method called for final outcome can provide a number between zero and 2,147,483,647 (inclusive, 0 and 2,147,483,647).

6.1.4 Seeding / Re-seeding

The seeding of RNG is called by "`rng.next();`" in `MonitoredSHA1PRNGAdapter` class which calls overwritten method of `next()` in `MonitoredRNG` class.

The following are summary of steps:

1) `random = SecureRandom.getInstance("SHA1PRNG", "SUN");`

2) `rng = new MonitoredRNG(new SHA1PRNGAdapter());`

3) `MonitoredRNG(final RNG rng)`

4) `final MonitoredSHA1PRNGAdapter rng = new MonitoredSHA1PRNGAdapter);`

Note: Trace view has been used for the verification of seeding on this step.

6.1.5 Background Cycling

Re-seeding of RNG is performed by hardware. Unlike the traditional method of re-seeding where the last output is used as the input to then next RNG value, re-seeding through hardware makes next RNG value impossible to predict as the input (i.e. re-seeding number) is whatever number generated by the hardware resources at the time of the request.

Enex TestLab found that no official background cycling mechanism has been implemented. However, due to the re-seeding method implemented, implementation of background cycling is not needed.

6.2 DIEHARD Tests

The DIEHARD test results are summarised in the following tables.

Note: Each sample file used in the DIEHARD tests comprises 3,000,000 lines and each line consists of a 32-bit number.

6.2.1 First Sample

Test Number	Test Name	P Values	KS Values	Test Results	Sample Size Test Result
1	Birthday Spacings	(9 / 6 /8)	(1 / 1 /1)	Pass	Pass
2	Overlapping 5-Permutations	(2 / 1 /2)	N/A	Pass	
3a	Binary Rank 31x31 Matrices	(1 / 1 /1)	N/A	Pass	
3b	Binary Rank 32x32 Matrices	(1 / 1 /1)	N/A	Pass	
3c	Binary Rank 6x8 Matrices	(25 / 20 /25)	(1 / 1 /1)	Pass	
4	Bitstream	(20 / 15 /19)	N/A	Pass	
5	OPSO	(23 / 17 /23)	N/A	Pass	
6	OQSO	(28 / 23 /27)	N/A	Pass	
7	DNA	(31 / 27 /30)	N/A	Pass	
8a	Count 1's (Stream of Bytes)	(2 / 1 / 2)	N/A	Pass	
8b	Count 1's (Specific Byte)	(25 / 20 /23)	N/A	Pass	
9	Parking Lot	(10 / 7 /9)	(1 / 1 /1)	Pass	
10	Minimum Distance	(20 / 15 /20)	(1 / 1 /1)	Pass	
11	3D Spheres	(20 / 15 /17)	(1 / 1 /1)	Pass	
12	Squeeze	(1 / 1 /1)	N/A	Pass	
13	Overlapping Sums	(10 / 7 /7)	(1 / 1 /1)	Pass	
14	Runs	(40 / 30 /38)	(1 / 1 /1)	Pass	
15	Craps	(1 / 1 / 1)	N/A	Pass	

6.2.2 Second Sample File

Test Number	Test Name	P Values	KS Values	Test Results	Sample Size Test Result
1	Birthday Spacings	(9 / 6 /9)	(1 / 1 /1)	Pass	Pass
2	Overlapping 5-Permutations	(2 / 1 /2)	N/A	Pass	
3a	Binary Rank 31x31 Matrices	(1 / 1 /1)	N/A	Pass	
3b	Binary Rank 32x32 Matrices	(1 / 1 /1)	N/A	Pass	
3c	Binary Rank 6x8 Matrices	(25 / 20 /25)	(1 / 1 /1)	Pass	
4	Bitstream	(20 / 15 /20)	N/A	Pass	
5	OPSO	(23 / 17 /23)	N/A	Pass	
6	OQSO	(28 / 23 /26)	N/A	Pass	
7	DNA	(31 / 27 /31)	N/A	Pass	
8a	Count 1's (Stream of Bytes)	(2 / 1 / 2)	N/A	Pass	
8b	Count 1's (Specific Byte)	(25 / 20 /24)	N/A	Pass	

9	Parking Lot	(10 / 7 /9)	(1 / 1 /1)	Pass	
10	Minimum Distance	(20 / 15 /20)	(1 / 1 /1)	Pass	
11	3D Spheres	(20 / 15 /20)	(1 / 1 /1)	Pass	
12	Squeeze	(1 / 1 /1)	N/A	Pass	
13	Overlapping Sums	(10 / 7 /8)	(1 / 1 /0)	Fail	
14	Runs	(40 / 30 /37)	(1 / 1 /1)	Pass	
15	Craps	(1 / 1 / 1)	N/A	Pass	

6.2.3 Third Sample File

Test Number	Test Name	P Values	KS Values	Test Results	Sample Size Test Result
1	Birthday Spacings	(9 / 6 /8)	(1 / 1 /1)	Pass	**Pass**
2	Overlapping 5-Permutations	(2 / 1 /2)	N/A	Pass	
3a	Binary Rank 31x31 Matrices	(1 / 1 /1)	N/A	Pass	
3b	Binary Rank 32x32 Matrices	(1 / 1 /1)	N/A	Pass	
3c	Binary Rank 6x8 Matrices	(25 / 20 /23)	(1 / 1 /1)	Pass	
4	Bitstream	(20 / 15 /20)	N/A	Pass	
5	OPSO	(23 / 17 /21)	N/A	Pass	
6	OQSO	(28 / 23 /27)	N/A	Pass	
7	DNA	(31 / 27 /30)	N/A	Pass	
8a	Count 1's (Stream of Bytes)	(2 / 1 / 2)	N/A	Pass	
8b	Count 1's (Specific Byte)	(25 / 20 /23)	N/A	Pass	
9	Parking Lot	(10 / 7 /10)	(1 / 1 /1)	Pass	
10	Minimum Distance	(20 / 15 /18)	(1 / 1 /1)	Pass	
11	3D Spheres	(20 / 15 /18)	(1 / 1 /1)	Pass	
12	Squeeze	(1 / 1 /1)	N/A	Pass	
13	Overlapping Sums	(10 / 7 /9)	(1 / 1 /0)	Fail	
14	Runs	(40 / 30 /37)	(1 / 1 /1)	Pass	
15	Craps	(1 / 1 / 1)	N/A	Pass	

6.3 *Final Outcome Distribution Tests*

The Final Distribution Tests take scaled / mapped sequences of random numbers and subjects them to a battery of statistical tests. As the sequences pass more of the tests, the confidence in the randomness of the numbers increases and so does the confidence in the generator. However, because it is expected that some sequences to appear non-random, some of the sequences are expected to fail at least some of the tests.

Final Outcome Distributions were run five times for each *Degree of Freedom (DoF)* for the sample sizes as indicated on the table.

The following table presents the overall results achieved for each sample size set.

For each sample size five set of data files were produced. The statistical test results of these five set of data determines “Fail” or “Pass” for that specific sample size. Two or more fails are considered as an overall FAIL, otherwise the test result produces an overall PASS.

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector’s Test
25	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	PASS	N/A
	10000	PASS	PASS	PASS
	20000	PASS	PASS	PASS
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
26	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	PASS	N/A
	10000	PASS	PASS	PASS
	20000	PASS	PASS	PASS
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector's Test
27	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	PASS	N/A
	10000	PASS	PASS	PASS
	20000	PASS	PASS	PASS
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
28	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	PASS	N/A
	10000	PASS	PASS	PASS
	20000	PASS	PASS	PASS
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
29	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	PASS	N/A
	10000	PASS	PASS	PASS
	20000	PASS	PASS	PASS
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector's Test
30	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	PASS	N/A
	10000	PASS	PASS	PASS
	20000	PASS	PASS	PASS
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
31	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	PASS	N/A
	20000	PASS	PASS	PASS
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
32	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	PASS	N/A
	20000	PASS	PASS	PASS
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector's Test
33	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	PASS	N/A
	20000	PASS	PASS	PASS
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
34	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	PASS	N/A
	20000	PASS	PASS	PASS
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
35	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	PASS	N/A
	20000	PASS	PASS	PASS
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector's Test
36	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	PASS	N/A
	20000	PASS	PASS	PASS
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
37	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	PASS	N/A
	20000	PASS	PASS	PASS
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	FAIL	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
38	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	PASS	N/A
	20000	PASS	PASS	PASS
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector's Test
39	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	FAIL	N/A	N/A
	10000	PASS	PASS	N/A
	20000	PASS	PASS	PASS
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
40	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	PASS	N/A
	20000	PASS	PASS	PASS
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
41	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	PASS	N/A
	20000	PASS	PASS	PASS
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector's Test
42	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	PASS	N/A
	20000	PASS	PASS	N/A
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
43	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	PASS	N/A
	20000	PASS	PASS	N/A
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
44	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	PASS	N/A
	20000	PASS	PASS	N/A
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector's Test
45	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	PASS	N/A
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
46	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	PASS	N/A
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	FAIL	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
47	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	PASS	N/A
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector's Test
48	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	PASS	N/A
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
49	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	PASS	N/A
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
50	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	PASS	N/A
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector's Test
51	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	PASS	N/A
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
53	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	PASS	N/A
	50000	PASS	PASS	PASS
	100000	PASS	PASS	FAIL
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
55	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	PASS	N/A
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector's Test
55	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	PASS	N/A
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
56	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	PASS	N/A
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
57	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	PASS	N/A
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector's Test
58	200	PASS	N/A	N/A
	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	PASS	N/A
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
59	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	PASS	N/A
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
61	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	PASS	N/A
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector's Test
62	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	PASS	N/A
	50000	PASS	PASS	PASS
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
63	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	N/A	N/A
	50000	PASS	PASS	N/A
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
65	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	N/A	N/A
	50000	PASS	PASS	N/A
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector's Test
66	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	N/A	N/A
	50000	PASS	PASS	N/A
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
67	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	N/A	N/A
	50000	PASS	PASS	N/A
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	FAIL	PASS	PASS
	10000000	PASS	PASS	PASS
68	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	N/A	N/A
	50000	PASS	PASS	N/A
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector's Test
70	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	N/A	N/A
	50000	PASS	PASS	N/A
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
71	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	FAIL	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	N/A	N/A
	50000	PASS	PASS	N/A
	100000	PASS	FAIL	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	FAIL	PASS
72	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	N/A	N/A
	50000	PASS	PASS	N/A
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector's Test
	500	PASS	N/A	N/A

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector's Test
74	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	N/A	N/A
	50000	PASS	PASS	N/A
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
75	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	N/A	N/A
	50000	PASS	PASS	N/A
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
76	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	N/A	N/A
	50000	PASS	PASS	N/A
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector's Test
77	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	N/A	N/A
	50000	PASS	PASS	N/A
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
78	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	N/A	N/A
	50000	PASS	PASS	N/A
	100000	PASS	PASS	PASS
	200000	PASS	PASS	PASS
	500000	PASS	PASS	PASS
	1000000	PASS	PASS	PASS
	2000000	PASS	PASS	PASS
	5000000	PASS	PASS	PASS
	10000000	PASS	PASS	PASS
83	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	N/A	N/A
	50000	PASS	PASS	N/A
	100000	PASS	PASS	N/A
	200000	PASS	PASS	N/A
	500000	PASS	PASS	N/A
	1000000	PASS	PASS	N/A
	2000000	PASS	PASS	N/A
	5000000	PASS	PASS	N/A
	10000000	PASS	PASS	N/A

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector's Test
84	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	N/A	N/A
	50000	PASS	PASS	N/A
	100000	PASS	PASS	N/A
	200000	PASS	PASS	N/A
	500000	PASS	PASS	N/A
	1000000	PASS	PASS	N/A
	2000000	PASS	PASS	N/A
	5000000	PASS	PASS	N/A
	10000000	PASS	PASS	N/A
89	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	N/A	N/A
	50000	PASS	PASS	N/A
	100000	PASS	PASS	N/A
	200000	PASS	PASS	N/A
	500000	PASS	PASS	N/A
	1000000	PASS	PASS	N/A
	2000000	PASS	PASS	N/A
	5000000	PASS	PASS	N/A
	10000000	PASS	PASS	N/A
93	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	N/A	N/A
	50000	PASS	PASS	N/A
	100000	PASS	PASS	N/A
	200000	PASS	PASS	N/A
	500000	PASS	PASS	N/A
	1000000	PASS	PASS	N/A
	2000000	PASS	PASS	N/A
	5000000	PASS	PASS	N/A
	10000000	PASS	PASS	N/A

Degrees of Freedom	Sample Size	Equi-Distribution Test	Serial Test	Coupon Collector's Test
95	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	N/A	N/A
	50000	PASS	PASS	N/A
	100000	PASS	PASS	N/A
	200000	PASS	PASS	N/A
	500000	PASS	PASS	N/A
	1000000	PASS	PASS	N/A
	2000000	PASS	PASS	N/A
	5000000	PASS	PASS	N/A
	10000000	PASS	PASS	N/A
125	500	PASS	N/A	N/A
	1000	PASS	N/A	N/A
	2000	PASS	N/A	N/A
	5000	PASS	N/A	N/A
	10000	PASS	N/A	N/A
	20000	PASS	N/A	N/A
	50000	PASS	N/A	N/A
	100000	PASS	PASS	N/A
	200000	PASS	PASS	N/A
	500000	PASS	PASS	N/A
	1000000	PASS	PASS	N/A
	2000000	PASS	PASS	N/A
	5000000	PASS	PASS	N/A
	10000000	PASS	PASS	N/A

7. Appendix A - Definitions

Background Cycling
Background Cycling is the mechanism that constantly generates random numbers in the back ground even if they are not being required by the application. Background cycling improves the un-predictability properties of the RNG.

Final Outcome Distribution Tests
Final Outcome Distribution Tests are an assessment of the distribution of application outcomes after scaling and mapping.

Degrees of Freedom
Always one less than the number of required outcomes (e.g.: with a 31 reel length, the degrees of freedom = 30).

DIEHARD Battery of Tests
The DIEHARD Battery of Tests is an assessment of the level of unpredictability of the application outcomes before scaling and mapping. The DIEHARD Battery of Tests produces P-Values which are used to judge the outcome of the tests.

Mapping
Mapping is the process where the scaled numbers are mapped to a given symbol or value. For example, the number 56 is mapped to the symbol ORANGE in reel 1 in a reel game.

P-Value
A P-Value is a percentage obtained for a particular sample. It is a measure of randomness for a given test element.

Period
Period is how long before the 'random' sequence repeats.

Random Number Generator (RNG)
A Random Number Generator is the algorithm used in generating the numbers mapped to final game outcomes.
Most gambling applications use Pseudo-random algorithms that use mathematical formulae to produce sequences of numbers that appear random.

Range
Range indicates the size of the RNG output and it is dependant of the size of the variable used in its implementation. For example, a 32 bit RNG implementation has a range of **4,294,967,296**, and a 63 bit RNG has a range of 1.8×10^{19}.

Raw Values
RNG unscaled output.

Sample
A sample is a single RNG outcome. For the DIEHARD Battery of Tests, samples must be taken from the raw RNG output. For the Final Outcome Distribution Tests, samples must be taken from the scaled and mapped RNG output.

Scaling

Scaling is required to divide the RAW output into smaller and usable numbers.

Seed
The seed is the RNG value used as the input for the next RNG iteration.

Seeding
Seeding is the method used to seed RNGs in the very first instance.

8. Appendix B - DIEHARD Tests

The following definitions are provided as specified in the DIEHARD office documentation.

Birthday Spacings

Choose m birthdays in a year of n days. List the spacings between the birthdays. If j is the number of values that occur more than once (1) in that list, then j is asymptotically Poisson distributed with mean m^3/(4n). Experience shows n must be quite large, say n>=2^18, for comparing the results to the Poisson distribution with that mean. This test uses n=2^24 and m=2^9, so that the underlying distribution for j is taken to be Poisson with lambda=2^27/(2^26)=2. A sample of 500 j's is taken, and a chi-square goodness of fit test provides a p value. The first test uses bits 1-24 (counting from the left) from integers in the specified file. Then the file is closed and reopened. Next, bits 2-25 are used to provide birthdays, then 3-26 and so on to bits 9-32. Each set of bits provides a p-value, and the nine p-values provide a sample for a KSTEST.

Overlapping 5-Permutations

This test looks at a sequence of one million 32-bit random integers. Each set of five consecutive integers can be in one of 120 states, for the 5! possible orderings of five numbers. Thus the 5th, 6th, 7th, etc... numbers each provide a state. As many thousands of state transitions are observed, cumulative counts are made of the number of occurrences of each state. Then the quadratic form in the weak inverse of the 120x120 covariance matrix yields a test equivalent to the likelihood ratio test that the 120 cell counts came from the specified (asymptotically) normal distribution with the specified 120x120 covariance matrix (with rank 99). This version uses 1,000,000 integers, twice.

Test #3a: Binary Rank 31x31 Matrices

This is the BINARY RANK TEST for 31x31 matrices. The leftmost 31 bits of 31 random integers from the test sequence are used to form a 31x31 binary matrix over the field {0,1}. The rank is determined. That rank can be from 0 to 31, but ranks < 28 are rare, and their counts are pooled with those for rank 28. Ranks are found for 40,000 such random matrices and a chi-square test is performed on counts for ranks 31,30,29 and <=28.

Binary Rank 32x32 Matrices

A random 32 x 32 binary matrix is formed, each row a 32-bit random integer. The rank is determined. That rank can be from 0 to 32, ranks less than 29 are rare, and their counts are pooled with those for rank 29. Ranks are found for 40,000 such random matrices and a chi-square test is performed on counts for ranks 32,31, 30 and <=29.

Binary Rank 6x8 Matrices

From each of six random 32-bit integers from the generator under test, a specified byte is chosen, and the resulting six bytes form a 6x8 binary matrix whose rank is determined. That rank can be from 0 to 6, but ranks 0,1,2,3 are rare; their counts are pooled with those for rank 4. Ranks are found for 100,000 random matrices, and a chi-square test is performed on counts for ranks 6,5 and <=4.

Bitstream

The file under test is viewed as a stream of bits. Call them b1, b2, etc… Consider an alphabet with two "letters" (0 and 1) and think of the stream of bits as a succession of 20-letter "words", overlapping. Thus the first word is b1b2...b20, the second is b2b3...b21, and so on. The bitstream test counts the number of missing 20-letter (20-bit) words in a string of 2^21 overlapping 20-letter words. There are 2^20 possible 20 letter words. For a truly random string of 2^21+19 bits, the number of missing words j should be (very close to) normally distributed with mean 141,909 and sigma 428. Thus (j-141909)/428 should be a standard normal variate (z score) that leads to a uniform (0,1) p value. The test is repeated twenty times.

OPSO

OPSO means Overlapping-Pairs-Sparse-Occupancy. The OPSO test considers 2-letter words from an alphabet of 1024 letters. Each letter is determined by a specified ten bits from a 32-bit integer in the sequence to be tested. OPSO generates 2^21 (overlapping) 2-letter words (from 2^21+1 "keystrokes") and counts the number of missing words – that is 2-letter words which do not appear in the entire sequence. That count should be very close to normally distributed with mean 141,909, sigma 290. Thus (missingwrds-141909)/290 should be a standard normal variable. The OPSO test takes 32 bits at a time from the test file and uses a designated set of ten consecutive bits. It then restarts the file for the next designated 10 bits, and so on.

OQSO

OQSO means Overlapping-Quadruples-Sparse-Occupancy. The OQSO test is similar to the OPSO test, except that it considers 4-letter words from an alphabet of 32 letters, each letter determined by a designated string of 5 consecutive bits from the test file, elements of which are assumed 32-bit random integers. The mean number of missing words in a sequence of 2^21 four-letter words, (2^21+3 "keystrokes"), is again 141909, with sigma = 295. The mean is based on theory; sigma comes from extensive simulation.

DNA

The DNA test considers an alphabet of 4 letters C, G, A and T, determined by two designated bits in the sequence of random integers being tested. It considers 10-letter words, so that as in OPSO and OQSO, there are 2^20 possible words, and the mean number of missing words from a string of 2^21 (over-lapping) 10-letter words (2^21+9 "keystrokes") is 141909. The standard deviation sigma=339 was determined as for OQSO by simulation. (Sigma for OPSO, 290, is the true value (to three places), not determined by simulation.

Count 1's (Stream of Bytes)

Consider the file under test as a stream of bytes (four per 32 bit integer). Each byte can contain from 0 to 8 1's, with probabilities 1, 8, 28, 56, 70, 56, 28, 8, and 1 over 256. Now let the stream of bytes provide a string of overlapping 5-letter words, each "letter" taking values A, B, C, D or E. The letters are determined by the number of 1's in a byte 0, 1 or 2 yield A, 3 yields B, 4 yields C, 5 yields D and 6, 7 or 8 yield E. Thus we have a monkey at a typewriter hitting five keys with various probabilities (37, 56, 70, 56 and 37 over 256). There are 5^5 possible 5-letter words, and from a string of 256,000 (overlapping) 5-letter words, counts are made on the frequencies for each word. The quadratic form in the weak inverse of the covariance matrix of the cell counts provides a chi-square test Q5-Q4, the difference of the naive Pearson sums of (OBS-EXP)^2/EXP on counts for 5-letter and 4-letter cell counts.

Count 1's (Specific Byte)

Consider the file under test as a stream of 32-bit integers. From each integer, a specific byte is chosen; say the left-most bits 1 to 8. Each byte can contain from 0 to 8 1's, with probabilities 1, 8, 28, 56, 70, 56, 28, 8 and 1 over 256. Now let the specified bytes from successive integers provide a string of (overlapping) 5-letter words, each "letter" taking values A, B, C, D or E. The letters are determined by the number of 1's, in that byte 0, 1 or 2 ⌫ A, 3 ⌫ B, 4 ⌫ C, 5 ⌫ D, and 6, 7 or 8 ⌫ E. Thus we have a monkey at a typewriter hitting five keys with various probabilities 37, 56, 70, 56 and 37 over 256. There are 5^5 possible 5-letter words, and from a string of 256,000 (overlapping) 5-letter words, counts are made on the frequencies for each word. The quadratic form in the weak inverse of the covariance matrix of the cell counts provides a chi-square test Q5-Q4, the difference of the naive Pearson sums of (OBS-EXP)^2/EXP on counts for 5-letter and 4-letter cell counts.

Parking Lot

In a square of side 100, randomly "park" a car – a circle of radius 1. Then try to park a 2nd, a 3rd, and so on, each time parking "by ear". That is, if an attempt to park a car causes a crash with one already parked, try again at a new random location. (To avoid path problems, consider parking helicopters rather than cars.) Each attempt leads to a crash or a success, the latter followed by an increment to the list of cars already parked. If we plot n the number of attempts, versus k the number successfully parked, we get a curve that should be similar to those provided by a perfect random number generator. Theory for the behaviour of such a random curve seems beyond reach, and as graphics displays are not available for this battery of tests, a simple characterization of the random experiment is used k, the number of cars successfully parked after n=12,000 attempts. Simulation shows that k should average 3523 with sigma 21.9 and is very close to normally distributed. Thus (k-3523)/21.9 should be a standard normal variable, which, converted to a uniform variable, provides input to a KSTEST based on a sample of 10.

Minimum Distance

(Repeated 100 times) Choose n=8000 random points in a square of side 10,000. Find d, the minimum distance between the (n^2-n)/2 pairs of points. If the points are truly independent uniform, then d^2, the square of the minimum distance should be (very close to) exponentially distributed with mean 0.995. Thus 1-exp(-d^2/0.995) should be uniform on (0,1) and a KSTEST on the resulting 100 values serves as a test of uniformity for random points in the square. Test numbers = 0 mod 5 are printed but the KSTEST is based on the full set of 100 random choices of 8000 points in the 10,000x10,000 square.

3D Spheres

Choose 4,000 random points in a cube of edge 1,000. At each point, centre a sphere large enough to reach the next closest point. Then the volume of the smallest such sphere is (very close to) exponentially distributed with mean 120pi/3. Thus the radius cubed is exponential with mean 30. (The mean is obtained by extensive simulation). The 3D Spheres test generates 4,000 such spheres 20 times. Each min radius cubed leads to a uniform variable by means of 1-exp(-r^3/30.), then a KSTEST is done on the 20 p-values.

Squeeze

Random integers are floated to get uniforms on (0,1). Starting with k=2^31=2147483647, the test finds j, the number of iterations necessary to reduce k to 1, using the reduction k=ceiling(k*U), with U provided by floating integers from the file being tested. Such j's are found 100,000 times, then counts for the number of times j was <= 6, 7, ..., 47, >= 48 are used to provide a chi-square test for cell frequencies.

Overlapping Sums

Integers are floated to get a sequence U(1), U(2), etc... of uniform (0,1) variables. Then overlapping sums, S(1) = U(1) + ... + U(100), S2 = U(2) + ... + U(101), etc... are formed. The S's are virtually normal with a certain covariance matrix. A linear transformation of the S's converts them to a sequence of independent standard normal, which are converted to uniform variables for a KSTEST. The p-values from ten KSTESTs are given still another KSTEST.

Runs

This test counts runs up, and runs down, in a sequence of uniform (0,1) variables, obtained by floating the 32-bit integers in the specified file. This example shows how runs are counted: 0.123, 0.357, 0.789, 0.425, 0.224, 0.416 and 0.95 contains an up-run of length 3, a down-run of length 2 and an up-run of (at least) 2, depending on the next values. The covariance matrices for the runs-up and runs-down are well known, leading to chi-square tests for quadratic forms in the weak inverses of the covariance matrices. Runs are counted for sequences of length 10,000. This is done ten times. Then repeated.

Craps

This test plays 200,000 games of craps, finds the number of wins and the number of throws necessary to end each game. The number of wins should be (very close to) a normal with mean 200000p and variance 200000p (1-p), with p=244/495. Throws necessary to complete the game can vary from 1 to infinity, but counts for all>21 are lumped with 21. A chi-square test is made on the number-of-throws cell counts. Each 32-bit integer from the test file provides the value for the throw of a die, by floating to (0,1), multiplying by 6 and taking 1 plus the integer part of the result.

Note

Most of the tests in DIEHARD return a p-value, which should be uniform on (0, 1) if the input file contains truly independent random bits. Those p-values are obtained by p=F(X), where F is the assumed distribution of the sample random variable X – often normal. But that assumed F is just an asymptotic approximation, for which the fit will be worst in the tails. Thus you should not be surprised with occasional p-values near 0 or 1, such as 0.0012 or 0.9983. When a bit stream really FAILS BIG, you will get p's of 0 or 1 to six or more places. By all means, do not, as a Statistician might, think that a p < 0.025 or p> 0.975 means that the RNG has "failed the test at the 0.05 level". Such p's happen among the hundreds that DIEHARD produces, even with good RNG's. So keep in mind that "p happens".