



Skill On Net

RNG evaluation report

07 April 2006

iTech Labs Australia ACN 108 249 761

Suite 24, 40 Montclair Ave, Glen Waverley, VIC 3150, Australia. Tel. +61 3 9561 9955 Fax: +61 3 9545 1596
www.itechlabs.com.au e-mail: info@itechlabs.com.au



1. Operator

Skill on Net	URL: www.BGroom.com
Attention: Andria	e-mail: admin@skillonnet.com

2. Tester

iTech Labs Australia	URL: http://www.itechlabs.com.au
Suite 24, 40 Montclair Ave Glen Waverley VIC 3150, Australia	e-mail: info@itechlabs.com.au

3. Item tested

Random Number Generator (RNG) and scaling algorithm for Backgammon games	
Date Requested:	28 February, 2006
Date Completed:	06 March, 2006

4. Technical Requirements

iTech Labs standards http://www.itechlabs.com.au/gaming/iTech_Labs_IGS_Standards.pdf (includes Marsaglia's 'Diehard' tests, Chi-squared tests and code review).
--

5. Previous history of the system/module under test

No previous history of independent testing available.

6. Evaluation details

<p>Request for evaluation</p> <p>Skill On Net has requested iTech Labs perform the following:</p> <ol style="list-style-type: none">1. Test and certify their RNG.2. Make recommendations (if required) to improve randomness of their RNG. <p>Evaluation performed</p> <p>iTech Labs have conducted evaluation of the Skill On Net RNG as below:</p> <ol style="list-style-type: none">1. Source code was examined for the following:<ol style="list-style-type: none">i) Identification of RNG algorithm;ii) Security of internal state, seeding and re-seeding, thread safety, background cycling;iii) Scaling to dice;2. Marsaglia's "Diehard" test was applied to raw RNG numbers.3. Chi-squared tests were applied to single die and pair of dice. These tests were conducted on three sets of 2 million die numbers each.



7. Evaluation results

1. Source code examination.
 - i) RNG uses Mersenne Twister algorithm. This RNG algorithm is well-known.
 - ii) Security of internal state and seeding are satisfactory.
 - iii) The scaling of RNG to produce dice numbers is statistically acceptable.
2. The numbers generated by the RNG have passed Marsaglia's "diehard" suite of tests for statistical randomness.
3. Chi-squared tests applied to three sets of 2 million die numbers have indicated statistical randomness.

8. Observations

1. Seeding
Seeding is done with low 32 bits of milliseconds elapsed since Jan 1, 1970.
iTech Labs recommends the use of an entropy source to seed the RNG - a previous RNG value, or some less externally predictable value (e.g. thread timing) in addition to the elapsed time.
2. Background cycling
Cycling the RNG (i.e. using some values in addition to those used by the games) ensures that the sequence of numbers delivered to games is not predictable, even if the last RNG value and the algorithm were known. This provides a very high level of surety that the next number cannot be predicted (note that using a single instance of the RNG shared by all games on the site has the same effect i.e. the next RNG number could go to any one of the many clients requesting an RNG number).
iTech Labs recommends that the RNG be cycled by a separate process several times per second.

9. Recommendation

Date of Request: 28 February 2006

Date of Recommendation: 07 April, 2006

System/Module: Skill On Net RNG

Total number of pages: 5

Operator: Bright Oasis

Software provider: Skill On Net

Recommendation for Certification:

iTech Labs certifies that Skill On Net RNG provides suitable random numbers for use with dice based games.

Audit method:

iTech Labs holds a copy of certified Skill On Net RNG source code. At any future time the source code used by Skill On Net can be compared to the reference source code held by iTech Labs.

10. Conditions of the Recommendation

1. The source code provided to iTech Labs (as per Appendix-A) must be used for compilation of the RNG module.
2. Any change to the RNG source code must be verified by iTech Labs.



11. Conclusion

While it is not possible to test all possible scenarios in a laboratory environment, iTech Labs has conducted a level of testing appropriate for a submission of this type.

Accordingly, subject to the above comment, iTech Labs certifies that the item under test complies with industry standard requirements, unless otherwise stated.

A handwritten signature in black ink, reading 'G. F. Nicoll'.

Geoff Nicoll
Principal Consultant

iTech Labs Australia

Date: 07 April, 2006



Appendix-A

Md5sum of RNG source files

1d9ee248997ce613fce568c56b688f9d	*Dice.java
af3292cfa8c43412a7405f46239d558f	*MersenneTwisterFast.java
f709859c0bc212b3362993820728fe69	*RandomNumberGenerator.java

Md5 program

c3fd10de60a769c2f43be3d2e49332db	*md5summer.exe
----------------------------------	----------------

Notes

SKN_RNG_Certification07Apr06.zip file contains the following:

Dice.java	(source file)
MersenneTwisterFast.java	(source file)
RandomNumberGenerator.java	(source file)
md5summer.exe	(program used to generate md5 sum of the source files)
SKN_RNG_SourceCode_md5sum.md5	(md5 sum of the above 4 files)
iTech Labs certification logo.gif	(certification logo)