



RNG EVALUATION REPORT

January 04, 2008

Kevin Fraser
The Flash Poker Network
United Kingdom
e-mail: (kevin@pitbullpoker.com)

Re - Recommendation for Random Number Generator (RNG) using SHA-1 algorithm

1. Request for evaluation

Pitbull Poker has requested iTech Labs perform the following:

1. Test and certify RNG using SHA-1 algorithm for card games.
2. Make recommendations (if required) to improve the RNG implementation.

2. Evaluation performed

iTech Labs has conducted evaluation of the RNG implementation for card games as below:

1. Source code was examined for the following:
 - i) Identification of RNG algorithm;
 - ii) Security of internal state, seeding and re-seeding, thread safety;
 - iii) Scaling to 52 cards;
2. Marsaglia's "Diehard" test was applied to raw RNG numbers.
3. Chi-squared tests were applied to shuffled decks. These tests were conducted on 210 sets of shuffled decks, each set ranging from 1,000 to 500,000 decks. The tests were conducted for a total of 5.16 million shuffled decks.

These tests were conducted for compliance to UK Gambling commission (UKGC), Alderney Gambling Control Commission (AGCC) and iTech Labs standards.

3. Evaluation results

1. Source code examination
 - i) RNG uses SHA-1 algorithm. This RNG algorithm is well-known.
 - ii) Security of internal state and initial seeding are satisfactory.
 - iii) The scaling of RNG to produce shuffled decks is statistically acceptable.
2. Chi-squared tests applied to 5.16 million shuffled decks have indicated statistical randomness.

The RNG fully complies with the relevant standards.

4. Observations

None.



5. Recommendation

Date of Request: November 14, 2007

Date of Recommendation: January 04, 2008

System/Module: RNG for card games

Total number of pages: 3

Operator: The Flash Poker Network

Software provider: The Flash Poker Network

iTech Labs certify that the RNG implementation using the source files specified in Appendix-A fully complies with UKGC, AGCC and iTech Labs standards.

Audit method:

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

6. 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 files listed in Appendix-A must be verified by iTech Labs.

7. 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 the relevant requirements, unless otherwise stated.

A handwritten signature in black ink, appearing to read "G. Y. Nicoll".

Geoff Nicoll
Principal Consultant

iTech Labs Australia

Date: January 04, 2008



Appendix-A

Md5sum* of RNG source files

File Name	Date last modified	Size	Md5sum
Shuffler.java	Dec. 14, 2007, 10:44:08 AM	2,450 bytes	b03a3cea3e52bc2550fe6e23ba1e9a8d

* Md5sum is calculated using the Linux program md5sum