



**Certification Report: ITL1902318-1**

## **Habanero Systems Limited**

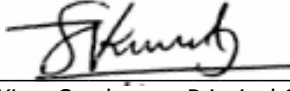
# **Random Number Generator Certification Report Malta Gaming Authority**

**18 September 2019**

**This is an amended report issued on 29 October 2019 to replace report ITL1902318.  
Details of changes are listed in Appendix B.**

## Certification Report: ITL1902318-1

### 1 Test Laboratory details

N°	Description	Details
1.	Contact Details of Test Laboratory	iTech Labs Suite 24, 40 Montclair Ave, Glen Waverley, VIC 3150, Australia URL: <a href="http://www.itechlabs.com">www.itechlabs.com</a> E-mail: <a href="mailto:info@itechlabs.com">info@itechlabs.com</a>
2.	Physical location of where testing was performed	iTech Labs, Suite 24, 40 Montclair Ave, Glen Waverley, VIC 3150, Australia
3.	Date Commenced	25 July 2019
4.	Date Completed	18 September 2019
5.	Scope of Work	Certification of the new software RNG for the software provider, Habanero Systems Limited
6.	Result	Passed all tests, subject to Section 5 Final declaration and conformity, Item 1 Conditions.
7.	Other	None
8.	Test Supervisor Signature:	 Kiren Sreekumar, Principal Consultant, iTech Labs

### 2 Executive summary

#### 2.1 General Information

N°	Description	Details
1.	Identification	Habanero Systems Limited RNG
2.	Type of system:	Online Casino
3.	Games using this RNG:	Non-card games: American Roulette European Roulette Keno Dice Slots  Card games: eight decks without joker six decks without joker five decks without joker single deck without joker single deck with joker
4.	Jurisdiction	Malta
5.	Guidelines used for testing	Malta Remote Gaming Regulations 2004 S.L.438.04.
6.	Software provider	Name: Habanero Systems Limited Address: Company Number C 89602, Level 5 Quantum House, 75 Abate Rigord Street, Ta'Xbiex XBX 1120, Malta URL: <a href="http://www.habanerosystems.com">www.habanerosystems.com</a> Contact: Chris Visser Email: <a href="mailto:chris@habanerosystems.com">chris@habanerosystems.com</a>
7.	Operator details	Not Applicable



# Certification Report: ITL1902318-1

## 2.2 Description of RNG

### 2.2.1 Software Details

N°	Description	Details
1.	RNG type	Pseudo Random Number Generator (PRNG)
2.	Implementation language	C#
3.	RNG version number	5.1.4478.308
4.	RNG build number	5.1.4478.308
5.	Superseded RNG	The RNG has not been previously certified.
6.	RNG algorithm	ISAAC
7.	Period of algorithm	There are no cycles in ISAAC shorter than 2 <sup>40</sup> values and the expected cycle length is 2 <sup>8295</sup> values.
8.	Dimension of numbers from algorithm	32-bit integer with the interval 0 to (2 <sup>32</sup> -1).
9.	Seeding	Seeding is done using a combination of the following: The current process ID, the current thread ID, the tick count since boot time, the current time, various high-precision performance counters, hash of the user's environment block and high-precision internal CPU counters
10.	Reseeding	Reseeding is done: 1) when any RNG monitoring test fails 2) after 1,000,000 RNG calls and 4 hours have elapsed since last seeding (both have to be satisfied)
11.	Library name and version	Not Applicable
12.	Operating system	Windows
13.	Environmental particulars	Platform supplier hosting the RNG: Not Applicable Platform version hosting the RNG: Not Applicable
14.	Files and SHA-1 hashes	Refer to Section 2.3 Critical Components of RNG; Table 1 and Table 2 below for the list hashes of source code files and binaries (if applicable) of the RNG.

### 2.2.2 Hardware Details

Not Applicable, software RNG.

## 2.3 Critical Components of RNG

**Table 1: SHA-1 Signature of RNG source files**

File Name	Size (bytes)	SHA-1
CryptoRNG.cs	5,095	AF1786C6D5FC51B42D143356F40A02F18581D99D
ISAAC.cs	7,089	74D118F22FE88A064B077F201D1E9F3D8EA1294D
PRNG.cs	9,796	74B2729938EC42A4AD83ED9E8A37FFE8EFE710C5
RNGHelper.cs	13,336	FF4816BF1D36829E4CEA546DA4C0308352C578BA

**Table 2: SHA-1 Signature of executables**

File Name	Size (bytes)	SHA-1
Habanero.RNG.dll	26112	eead3c403b3721bb62da82546e60c5fb52174559

## 2.4 Scope of Testing

N°	Description	Details
1.	Vendor supplied output testing	Not Applicable
2.	Test Laboratory generated output from vendor supplied source	Source files were compiled by iTech Labs. Refer to Section 2.3 Critical Components of RNG.

## Certification Report: ITL1902318-1

N°	Description	Details
3.	Source code review	The source code review verified that the implementation of the RNG is in accordance with the technical requirements. This includes, but is not limited to: <ol style="list-style-type: none"> <li>Identification of algorithm;</li> <li>Security of internal state, seeding and re-seeding, thread safety;</li> <li>Scaling for non-card games;</li> <li>Shuffling for card games.</li> </ol>
4.	Statistical tests	The statistical tests undertaken by iTech Labs are: <ol style="list-style-type: none"> <li>Diehard tests</li> <li>Chi-square tests</li> </ol>
5.	Theoretical basis of algorithm and supporting crypto-analysis evidence	Literature is readily available, describing the theoretical basis of the algorithm (refer to Section 2.2) <ol style="list-style-type: none"> <li>Wikipedia: <a href="https://en.wikipedia.org/wiki/ISAAC_(cipher)">https://en.wikipedia.org/wiki/ISAAC_(cipher)</a></li> </ol>

### 2.5 Limitation of use of RNG

N°	Description	Details
1.	Acceptable degrees of freedom (DOF) permitted	Acceptable DOF's are listed in Section 3.1 Item 5 (below).
2.	Dependency on operating system functionality	None
3.	Library-based implementation	None
4.	Other	None

## 3 Detailed test results

### 3.1 Tests methodology

The testing methodologies listed below were used to ensure the RNG complies with the relevant jurisdictional technical requirements and the scope of work.

N°	Test Performed	Test Methodology	Result
1.	Review of RNG documentation	Review of RNG documentation was conducted to understand the implementation of RNG in the gaming system.	Comply
2.	Research conducted about RNG algorithm/ hardware	Research conducted about RNG algorithm to ensure there is no publicly known weakness or vulnerabilities associated the RNG under evaluation.	Comply
3.	Review of source code	Review of source code was conducted to verify that the implementation of the RNG is in accordance with the technical requirements.	Comply
4.	Statistical testing of raw output of RNG.	Marsaglia's diehard tests were applied to 80 million bits of raw 32 bit random numbers generated by the algorithm. The following diehard tests were conducted on 2 sets of 80 million bits; <ol style="list-style-type: none"> <li>BIRTHDAY SPACINGS</li> <li>OVERLAPPING 5-PERMUTATIONS</li> <li>BINARY RANK TEST for 31x31 matrices</li> <li>BINARY RANK TEST for 32x32 matrices</li> <li>BINARY RANK TEST for 6x8 matrices</li> <li>BITSTREAM TESTS ON 20-BIT Words</li> <li>BITSTREAM TESTS OPSO, OQSO, DNA</li> <li>COUNT-THE-1's IN A STREAM OF BYTES</li> <li>COUNT-THE-1's IN SPECIFIC BYTES</li> <li>PARKING LOT TEST</li> <li>MINIMUM DISTANCE TEST</li> <li>THE 3DSPHERES TEST</li> <li>THE SQUEEZE test</li> <li>OVERLAPPING SUMS TEST</li> <li>RUNS TEST</li> </ol>	Comply Refer Section 4.1 for results.

## Certification Report: ITL1902318-1

N°	Test Performed	Test Methodology	Result
		xvi. CRAPS TEST	
5.	Statistical testing of scaled / shuffled data	<p>Chi-square tests were conducted for the following:</p> <ul style="list-style-type: none"> <li>• DOF for American Roulette (Range= 38): 37</li> <li>• DOF for European Roulette (Range= 37): 36</li> <li>• DOF for Slots (Reel size =35): 34</li> <li>• DOF for Slots (Reel size =65): 64</li> <li>• DOF for Slots (Reel size =70): 69</li> <li>• DOF for Keno (Range=20 from 80): 1580</li> <li>• DOF for Dice: 5</li> <li>• DOF for eight decks (without joker): <ul style="list-style-type: none"> <li>Card/deal: 416</li> <li>Suit: 1248</li> <li>Rank: 4992</li> <li>Card: 21216</li> </ul> </li> <li>• DOF for six decks (without joker): <ul style="list-style-type: none"> <li>Card/deal: 312</li> <li>Suit: 936</li> <li>Rank: 3744</li> <li>Card: 15912</li> </ul> </li> <li>• DOF for five decks (without joker): <ul style="list-style-type: none"> <li>Card/deal: 260</li> <li>Suit: 780</li> <li>Rank: 3120</li> <li>Card: 13260</li> </ul> </li> <li>• DOF for single deck (without joker): <ul style="list-style-type: none"> <li>Card/deal: 52</li> <li>Suit: 156</li> <li>Rank: 624</li> <li>Card: 2652</li> </ul> </li> <li>• DOF for single deck (with joker): <ul style="list-style-type: none"> <li>Card/deal: 53</li> <li>Suit: 212</li> <li>Rank: 689</li> <li>Card: 2756</li> </ul> </li> </ul>	Comply Refer Section 4.2 for results
6.	Other issues	None	-

### 3.2 Compliance to technical standards

N°	Requirement Description	Results	Comments
<b>3<sup>rd</sup> Schedule Regulation 25</b>			
3.	The gaming machine must satisfy the randomness following Schneier:		
	(a) the data must be randomly generated, passing appropriate statistical tests of randomness;	Comply	
	(b) the data must be unpredictable, i.e. it must be computationally infeasible to predict what the next number will be, given complete knowledge of the algorithm or hardware generating the sequence, and all previously generated numbers;	Comply	
	(c) the series cannot be reliably reproduced, i.e. if the sequence generator is activated again with the same input (as exactly as is reasonably possible) it will produce two completely unrelated random sequences.	Comply	



## Certification Report: ITL1902318-1

### 4 Statistical test results

#### 4.1 Testing results for raw output of RNG

The Diehard tests were performed on two random sequences. The columns 'Result Random sequence-1' and 'Result Random sequence-2' contain the filenames for the detailed results. These files are supplied as attachments with this Certification report.

Confidence Level for the tests is: 95%

**Overall result:** Pass

Result Random sequence-1	Result Random sequence-2	Sample size	Confidence level	Result
Refer to attachment hab1.txt	Refer to attachment hab2.txt	80 million bits	95%	Pass

#### 4.2 Testing results for scaled/ shuffled data

The Chi-square tests were performed with the results listed in Appendix A. The columns 'Result Datafile1' and 'Result Datafile 2' contain the filenames for the detailed results. These files are supplied with this Certification report.

Confidence Level for the tests is:95%

**Overall result:** Pass

### 5 Final declaration and conformity


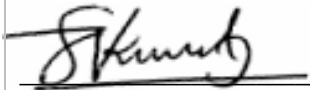
Nº	Description	Details
1.	Conditions/Observations	None
2.	Certification	<p>Certification Date: 18 September 2019  Software Provider: Habanero Systems Limited  Software Provider site URL: <a href="http://www.habanerosystems.com">www.habanerosystems.com</a>  Operator Name: Not Applicable  Operator site URL: Not Applicable</p> <p>This is to certify that iTech Labs has evaluated the Random Number Generator (RNG) by Habanero Systems Limited and found that the RNG complies with the relevant standards and is in conformity to the Malta Remote Gaming Regulations S.L.438.04.</p> <p>It is hereby certified that the Random Number Generator (RNG) as specified in Section 2.3, and used by the games listed in Section 2.1 Item 3, is compliant with the technical requirements set in the Third Schedule of the Malta Remote Gaming Regulations S.L.438.04 and that the Random Number Generator (RNG) was tested as an integral part of the gaming system.</p>

### 6 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 items under test comply with the relevant Technical Standards, unless otherwise stated.

#### Signatures:

 <b>Geoff Nicoll</b> Principal Consultant <b>iTech Labs</b> 18 September 2019	 <b>Kiren Sreekumar</b> Principal Consultant <b>iTech Labs</b> 18 September 2019
--	--

## Appendix A – Chi Square Testing Result (refer to Section 4.2)

**Table A.1 Non Card Games**

Game Type	Range	DOF	Result Datafile 1 (Refer attachments)	Result Datafile2 (Refer attachments)	Scaled numbers*	C.L.^	Result
American Roulette	38	37	Roulette_38.2019-08-26-15-24-46.slk	Roulette_38.2019-08-26-13-46-43.slk	505000	95%	Pass
European Roulette	37	36	Roulette.2019-08-26-15-24-46.slk	Roulette.2019-08-26-13-46-43.slk	505000	95%	Pass
Slot	70	69	Reel_70.2019-08-26-13-46-43.slk	Reel_70.2019-08-26-11-38-05.slk	505000	95%	Pass
Slot	65	64	Reel_65.2019-09-05-12-25-19.slk	Reel_65.2019-08-26-11-38-05.slk	505000	95%	Pass
Slot	35	34	Reel_35.2019-08-26-15-24-46.slk	Reel_35.2019-08-26-13-46-43.slk	505000	95%	Pass
Keno	20 from 80	1580	Keno.2019-08-26-15-24-46.slk	Keno.2019-08-26-13-46-43.slk	39895000	95%	Pass
Dice	1 to 6	5	Dice_06.2019-09-06-09-25-36.slk	Dice_06.2019-09-06-09-27-44.slk	505000	95%	Pass

**Table A.2 Card Games**

Game Type	DOF	Result Datafile 1 (Refer attachments)	Result Datafile2 (Refer attachments)	Scaled numbers*	C.L.^	Result
Eight decks without joker	Card/deal: 416 Suit: 1248 Rank: 4992 Card: 21216	8Decks_with_0Jokers.2019-08-26-15-24-46.slk	8Decks_with_0Jokers.2019-08-26-13-46-43.slk	628725000	95%	Pass
Six decks without joker	Card/deal: 312 Suit: 936 Rank: 3744 Card: 15912	6Decks_with_0Jokers.2019-08-26-15-24-46.slk	6Decks_with_0Jokers.2019-08-26-13-46-43.slk	628687122	95%	Pass
Five decks without joker	Card/deal: 260 Suit: 780 Rank: 3120 Card: 13260	5Decks_with_0Jokers.2019-10-24-11-41-57.slk	5Decks_with_0Jokers.2019-10-24-12-09-19.slk	628690125	95%	Pass
Single deck without joker	Card/deal: 52 Suit: 156 Rank: 624 Card: 2652	1Decks_with_0Jokers.2019-08-26-15-24-46.slk	1Decks_with_0Jokers.2019-08-26-13-46-43.slk	628719840	95%	Pass

<b>Game Type</b>	<b>DOF</b>	<b>Result Datafile 1</b> (Refer attachments)	<b>Result Datafile2</b> (Refer attachments)	<b>Scaled numbers*</b>	<b>C.L. ^</b>	<b>Result</b>
Single deck with joker	Card/deal: 53 Suit: 212 Rank: 689 Card: 2756	1Deck_with_1Joker.2019-08-26-15-24-46.slk	1Deck_with_1Joker.2019-08-26-13-46-43.slk	78780000	95%	Pass

\* Scaled numbers for each data file; ^ Confidence Level



## Appendix – B

*This report has been amended to address one issue identified in the original report. The issue and the respective amendment are listed below.*

"Five decks without joker" added

"Five decks without joker" was not included in the original certification report (REF: ITL1902318).

It has now been added in this report.

Changes associated with this addition are in the following sections of this report:

2.1.3

3.1.5

Appendix A - Table A.2