kiPrng DLL Demo Kenneth Ives kenaso@tx.rr.com

I am open to ways to improve this application, please email me.

Visual Basic 6.0 with Service Pack 6 runtime files required.
To obtain required files (VBRun60sp6.exe):
http://www.microsoft.com/downloads/details.aspx?FamilyId=7B9BA261-7A9C-43E7-9117-F6730
77FFB3C

VBRun60sp6.exe installs Visual Basic 6.0 SP6 run-time files.
http://support.microsoft.com/kb/290887

This software has been tested on Windows XP through Windows 7.
Windows 9x, 2000 and NT4 are no longer supported.

NOTE: This application is slow due to the formatting for display purposes
and file creation, not the generation of the data. The primary
purpose of this application is to introduce you to more secure ways
of creating random values.

==========

All nine algorithms have output within these ranges:

-0.9999999999999 to 0.9999999999999	Double Precision
-2147483648 to 2147483647	Long Integer

My observations have been that any of the below listed random number generators
will pass or fail any particular test when values are generated because there
is no such thing as true randomness without an external reference such as
radioactive decay, noise, etc. However, these random number generators will
pass all or most of the Diehard and ENT tests the majority of the time. TT800
has been tweaked by me to enhance the quality of output values in order to pass
the Diehard test scenarios. See TestResults.zip for results of testing.

See the section "Testing Software Available" below for the various web sites
for the testing software.

****

Comments about testing of random number generators (RNG)
by George Marsaglia
http://stat.fsu.edu/pub/diehard/

"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
.0012 or .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 < .025 or p > .975 means that the RNG has 'failed the test at the .05
level'. Such p's happen among the hundreds that DIEHARD produces, even with
good RNG's. So keep in mind that 'p happens'."

Intel® states in The Intel® Random Number Generator
http://www.utdallas.edu/~xinchou/intel-rng-1.pdf

"Intel has performed testing with Diehard using the output from the hardware
RNG. Appendix C contains sample test results from one of the runs of the
Diehard test suite performed on a 10-Mbyte sample. A full understanding of

the Diehard output requires detailed knowledge of statistics. However, passing the Diehard tests is not very well defined since Dr. Marsaglia does not provide concrete criteria. An individual test can be considered passing if the p-value is between 0.025 and 0.975, forming a 95% confidence interval around the theoretical value specified within the test. However, to evaluate a data sample against the entire test suite requires consideration of all 250 p-values that are generated and the calculation of the probability that the entire suite passes with 95% confidence. This calculation yields a 95% confidence interval of 0.0001 and 0.9999 for the p-value. Therefore, the RNG fails the Diehard tests if there is a p-value greater than or equal to 0.9999 or less than or equal to 0.0001."

Ken's Observation

My observation is when I see any of the following in the Diehard results, I know I have failed that particular series of tests. Especially, if I see asteriks anywhere in the p-value columns.

Failure indicators in the p-value columns:

0.9999	Upper bounds error
1.0000	Upper bounds error
.0000	Lower bounds error
0.0001	Lower bounds error
******	Asteriks = Back to the drawing board

The below statistics are consistant results of the random number generators.

Diehard Testing results:	CryptoAPI	ISAAC	Mother Of All	KISS	MWC
Birthday Spacings	Passed	Passed	Passed	Passed	Passed
Overlapping Permutations	Passed	Passed	Passed	Passed	Passed
Ranks of 31x31 & 32x32 matrices					
Binary rank 1	Passed	Passed	Passed	Passed	Passed
Binary rank 2	Passed	Passed	Passed	Passed	Passed
Ranks of 6x8 matrices	Passed	Passed	Passed	Passed	Passed
Monkey tests on 20-bit words	Passed	Passed	Passed	Passed	Passed
Monkey tests OPSO, OQSO, DNA					
OPSO	Passed	Passed	Passed	Passed	Passed
OQSO	Passed	Passed	Passed	Passed	Passed
DNA	Passed	Passed	Passed	Passed	Passed
Count_The_1's in a stream	Passed	Passed	Passed	Passed	Passed
Count_The_1's specific	Passed	Passed	Passed	Passed	Passed
Parking Lot	Passed	Passed	Passed	Passed	Passed
Minimum distance	Passed	Passed	Passed	Passed	Passed
Random Spheres	Passed	Passed	Passed	Passed	Passed
Squeeze	Passed	Passed	Passed	Passed	Passed
Overlapping Sums	Passed	Passed	Passed	Passed	Passed
Runs	Passed	Passed	Passed	Passed	Passed
Craps	Passed	Passed	Passed	Passed	Passed

Mersenne Twister family (Monte Carlo) generators will pass all Diehard and ENT randomness tests even if cryptographic quality has not been selected. This is due to my personal tweakings within the code. Well documented.

	MT19937	MT11231A	MT11231B	TT800
Birthday Spacings	Passed	Passed	Passed	Passed
Overlapping Permutations	Passed	Passed	Passed	Passed
Ranks of 31x31 & 32x32 matrices				
Binary rank 1	Passed	Passed	Passed	Passed
Binary rank 2	Passed	Passed	Passed	Passed
Ranks of 6x8 matrices	Passed	Passed	Passed	Passed
Monkey tests on 20-bit words	Passed	Passed	Passed	Passed
Monkey tests OPSO, OQSO, DNA				
OPSO	Passed	Passed	Passed	Passed
OQSO	Passed	Passed	Passed	Passed
DNA	Passed	Passed	Passed	Passed
Count_The_1's in a stream	Passed	Passed	Passed	Passed
Count_The_1's specific	Passed	Passed	Passed	Passed
Parking Lot	Passed	Passed	Passed	Passed
Minimum distance	Passed	Passed	Passed	Passed
Random Spheres	Passed	Passed	Passed	Passed
Squeeze	Passed	Passed	Passed	Passed
Overlapping Sums	Passed	Passed	Passed	Passed
Runs	Passed	Passed	Passed	Passed
Craps	Passed	Passed	Passed	Passed

****
Testing software available
****

The easiest way to create a test file is to check the Diehard checkbox
on the main screen of the demo program. This option will create an
11mb (approx) binary file with an extension of ".BIN". Use this binary
file as the input for your tests with Diehard, ENT, or NIST.

Diehard software
http://stat.fsu.edu/pub/diehard/

Ent Software
http://www.fourmilab.ch/random/
download file Random.zip

NIST (National Institute of Standards and Technology) testing software
http://csrc.nist.gov/groups/ST/toolkit/rng/index.html

1. Download source code
   http://csrc.nist.gov/groups/ST/toolkit/rng/documents/sts-2.1.zip
        or
   http://csrc.nist.gov/groups/ST/toolkit/rng/documents/sts-2.1.1.zip

2. Compile software using Cygwin. If anyone gets this to compile for
   Windows, please email me. I would like to get the binaries so I can
   start testing with the newer version of the NIST software. Thank you.
   http://sourceware.org/cygwin/

3. If you are not a C programmer then download an older version with
   the binaries at:
   http://www.cs.sunysb.edu/~algorith/implement/rng/distrib/sts-1.6.zip

4. Warning! The NIST testing suite is very thorough but time consuming.
   The process may take a few hours to longer than a day to complete.
   The reports are very detailed.

April 27, 2010: NIST Special Publication 800-22rev1a (dated April 2010),
A Statistical Test Suite for the Validation of Random Number Generators
and Pseudo Random Number Generators for Cryptographic Applications, that
describes the test suite.
http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf

Read PDF file Prng_Testing.pdf distributed with this application
concerning the parameters for NIST testing.

****

If you want to use the Visual Basic random number generator, then
here are some references.

References:

Randomize Statement Doesn't Re-initialize Rnd Function
http://support.microsoft.com/default.aspx?scid=kb;en-us;120587

"To re-initialize the random-number generator, use the Rnd
function with a value of -1 and then use the Randomize
and then use the Randomize statement with the value you want
to for the Rnd function."

Mark Hutchinson article about the Microsoft Visual BASIC random
number generator
http://www.15seconds.com/issue/051110.htm

VBA's Pseudo Random Number Generator
http://www.noesis.net.au/prng.php

INFO: How Visual Basic Generates Pseudo-Random Numbers for the
RND Function
http://support.microsoft.com/kb/231847/en-us

RND and RANDOMIZE Alternatives for Generating Random Numbers
http://support.microsoft.com/kb/28150/EN-US/

****
Other sites to visit (This should get you started)
****
Ciphers By Ritter
http://www.ciphersbyritter.com/

Counterpane Internet Security
http://www.counterpane.com/labs.html

Cryptographic Randomness
http://world.std.com/~cme/html/randomness.html

ISAAC: a fast cryptographic random number generator
http://burtleburtle.net/bob/rand/isaacafa.html

Mersenne Twister Home Page
http://www.math.keio.ac.jp/~matumoto/emt.html

Random Number Generators
http://www.npac.syr.edu/projects/random/

National Institute of Standards and Technology (NIST)
documentation and software:
http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html

The Scalable Parallel Random Number Generators Library (SPRNG)
http://sprng.cs.fsu.edu/

****

==========
License

Kenneth Ives
kenaso@tx.rr.com

==========

Preamble

This License governs Your use of the Work. This License is intended to allow developers to use the Source Code and Executable Files provided as part of the Work in any application in any form.

The main points subject to the terms of the License are:

- Source Code and Executable Files can be used in commercial applications;
- Source Code and Executable Files can be redistributed; and
- Source Code can be modified to create derivative works.

No claim of suitability, guarantee, or any warranty whatsoever is provided. The software is provided "as-is".

This License is entered between You, the individual or other entity reading or otherwise making use of the Work licensed pursuant to this License and the individual or other entity which offers the Work under the terms of this License ("Author").

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CODE PROJECT OPEN LICENSE ("LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HEREIN, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. THE AUTHOR GRANTS YOU THE RIGHTS CONTAINED HEREIN IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO ACCEPT AND BE BOUND BY THE TERMS OF THIS LICENSE, YOU CANNOT MAKE ANY USE OF THE WORK.

Definitions.

"Articles" means, collectively, all articles written by Author which describes how the Source Code and Executable Files for the Work may be used by a user.

"Author" means the individual or entity that offers the Work under the terms of this License.

"Derivative Work" means a work based upon the Work or upon the Work and other pre-existing works.

"Executable Files" refer to the executables, binary files, configuration and any required data files included in the Work.

"Publisher" means the provider of the website, magazine, CD-ROM, DVD or other medium from or by which the Work is obtained by You.

"Source Code" refers to the collection of source code and configuration files used to create the Executable Files.

"Standard Version" refers to such a Work if it has not been modified, or has been modified in accordance with the consent of the Author, such consent being in the full discretion of the Author.

"Work" refers to the collection of files distributed by the Publisher, including the Source Code, Executable Files, binaries, data files, documentation, whitepapers and the Articles.

"You" is you, an individual or entity wishing to use the Work and exercise your rights under this License.

Fair Use/Fair Use Rights. Nothing in this License is intended to reduce, limit, or restrict any rights arising from fair use, fair dealing, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

License Grant. Subject to the terms and conditions of this License, the Author hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

You may use the standard version of the Source Code or Executable Files in Your own applications.

You may apply bug fixes, portability fixes and other modifications obtained from the Public Domain or from the Author. A Work modified in such a way shall still be considered the standard version and will be subject to this License.

You may otherwise modify Your copy of this Work (excluding the Articles) in any way to create a Derivative Work, provided that You insert a prominent notice in each changed file stating how, when and where You changed that file.

You may distribute the standard version of the Executable Files and Source Code or Derivative Work in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution.

The Articles discussing the Work published in any form by the author may not be distributed or republished without the Author's consent. The author retains copyright to any such Articles. You may use the Executable Files and Source Code pursuant to this License but you may not repost or republish or otherwise distribute or make available the Articles, without the prior written consent of the Author.

Any subroutines or modules supplied by You and linked into the Source Code or Executable Files this Work shall not be considered part of this Work and will not be subject to the terms of this License.

Patent License. Subject to the terms and conditions of this License, each Author hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, import, and otherwise transfer the Work.

Restrictions. The license granted in Section 3 above is expressly

made subject to and limited by the following restrictions:

You agree not to remove any of the original copyright, patent, trademark, and attribution notices and associated disclaimers that may appear in the Source Code or Executable Files.

You agree not to advertise or in any way imply that this Work is a product of Your own.

The name of the Author may not be used to endorse or promote products derived from the Work without the prior written consent of the Author.

You agree not to sell, lease, or rent any part of the Work.

You may distribute the Executable Files and Source Code only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy of the Executable Files or Source Code You distribute and ensure that anyone receiving such Executable Files and Source Code agrees that the terms of this License apply to such Executable Files and/or Source Code. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute the Executable Files or Source Code with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License.

You agree not to use the Work for illegal, immoral or improper purposes, or on pages containing illegal, immoral or improper material. The Work is subject to applicable export laws. You agree to comply with all such laws and regulations that may apply to the Work after Your receipt of the Work.

Representations, Warranties and Disclaimer. THIS WORK IS PROVIDED "AS IS", "WHERE IS" AND "AS AVAILABLE", WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OR GUARANTEES. YOU, THE USER, ASSUME ALL RISK IN ITS USE, INCLUDING COPYRIGHT INFRINGEMENT, PATENT INFRINGEMENT, SUITABILITY, ETC. AUTHOR EXPRESSLY DISCLAIMS ALL EXPRESS, IMPLIED OR STATUTORY WARRANTIES OR CONDITIONS, INCLUDING WITHOUT LIMITATION, WARRANTIES OR CONDITIONS OF MERCHANTABILITY, MERCHANTABLE QUALITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTY OF TITLE OR NON-INFRINGEMENT, OR THAT THE WORK (OR ANY PORTION THEREOF) IS CORRECT, USEFUL, BUG-FREE OR FREE OF VIRUSES. YOU MUST PASS THIS DISCLAIMER ON WHENEVER YOU DISTRIBUTE THE WORK OR DERIVATIVE WORKS.

Indemnity. You agree to defend, indemnify and hold harmless the Author and the Publisher from and against any claims, suits, losses, damages, liabilities, costs, and expenses (including reasonable legal or attorneys' fees) resulting from or relating to any use of the Work by You.

Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL THE AUTHOR OR THE PUBLISHER BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK OR OTHERWISE, EVEN IF THE AUTHOR OR THE PUBLISHER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Termination.

This License and the rights granted hereunder will terminate automatically upon any breach by You of any term of this License. Individualss or entities who have received Derivative Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 6, 7, 8, 9, 10 and 11 will survive any termination of this License.

If You bring a copyright, trademark, patent or any other infringement claim against any contributor over infringements You claim are made by the Work, your License from such contributor to the Work ends automatically.

Subject to the above terms and conditions, this License is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, the Author reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

Publisher. The parties hereby confirm that the Publisher shall not, under any circumstances, be responsible for and shall not have any liability in respect of the subject matter of this License. The Publisher makes no warranty whatsoever in connection with the Work and shall not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. The Publisher reserves the right to cease making the Work available to You at any time without notice

Miscellaneous.

This License shall be governed by the laws of the location of the head office of the Author or if the Author is an individual, the laws of location of the principal place of residence of the Author.

If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this License, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

This License constitutes the entire agreement between the parties with respect to the Work licensed herein. There are no understandings, agreements or representations with respect to the Work not specified herein. The Author shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Author and You.

Kenneth Ives kenaso@tx.rr.com