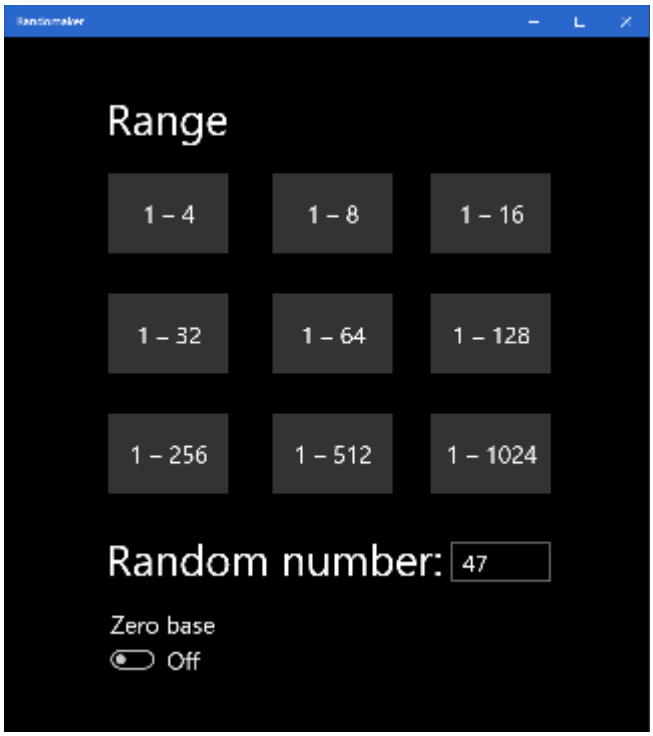
TruRand User’s Guide

Installation

The first time TruRand is run, its window appears in the default size determined by Windows. Dragging the right and bottom borders, the user can resize the window to a practical size, excluding the explanatory text on the right side, as in the screen shot below. Windows will retain that size when TruRand is subsequently launched.



Theory of Operation

Computers normally use a mathematical algorithm to generate numbers that are pseudo-random. Instead, TruRand takes a novel approach, generating numbers that are truly random. A pseudo-random number algorithm is deterministic, approximating a random sequence of numbers, which repeats for a given seed value. The method TruRand uses is not a mathematical

simulation, does not use a seed value, and generates sequences that do not repeat. It does that by utilizing asynchronous aspects of computer hardware and the asynchronous nature of the human-to-computer interface.

Modern CPUs in personal computers and business servers have a TSC (Time Stamp Counter), a 64-bit register that is incremented at a constant rate, usually 10 megahertz. The rate at which the TSC is incremented does not vary, while the rate of the CPU clock, running many times faster than the TSC, does vary in response to computational demand and thermal regulation. When human input occurs in the form of a mouse click, a hardware interrupt request is sent to the CPU, which responds to the interrupt at the end of execution of the current instruction. That and previous instructions typically take one to several CPU clock cycles to execute. Hence, the time at which an interrupt request triggered by a mouse click is processed is random in terms of the instantaneous count in the TSC.

The low-order bits of the TSC function as a counter that cycles rapidly through a chosen range. For example, the 0–63 range utilizes the six least significant bits of the TSC. Incremented at 10 MHz, the count from 0 to 63 repeats 156,250 times per second, and the value of the count within that range is random at the time a mouse click is processed. When the user clicks a Range button in TruRand, the low-order bits of the TSC are sampled and translated to a number derived from the set of bits corresponding to the selected range. The number of bits in the set is greater for a wide range than for a narrow range. The number derived from the set of bits is output to the “Random number” text box. The lower and upper bounds of the range are determined by the minimum and maximum numbers that set of bits can represent. That is why the ranges correspond to powers of 2 in the binary number system.

A number sampled from the TSC at the time of a mouse click could be forced algorithmically to exist within an arbitrary range, but doing so would destroy the random nature of a sequence of numbers. For example, if the range 1–64 were forced to 1–47, numbers from 48 to 64 would have to be mapped to numbers in the range 1–47. However, there are only 16 numbers in the range 48–64, so mapping those numbers to arbitrary numbers in the range 1–47

would cause those numbers to occur more frequently than numbers not mapped to numbers above the range 1–47.

The way to preserve the random nature of a sequence of numbers within an arbitrary range is to disregard numbers outside the desired range and click the button again, until a number in the desired range appears. That works because a range of numbers within a set of random numbers is also random.

Using TruRand

Click a Range button to generate a random number within that range. After a range is selected, additional random numbers can be generated in that range by clicking again or by pressing Enter. To generate a random number in a range not specified on a button, for example 1–46, click on the higher range, in this case 1–64. If the generated number is greater than 46, click again, until a number in the desired range appears. To include 0 in the ranges of random numbers, turn "Zero base" on.

A virtual “coin flip” is obtained by clicking any range button and interpreting an even number as “heads” and an odd number as “tails,” or vice versa. An arbitrarily large random number can be made one digit at a time, from the range 0–9. For those familiar with hexadecimal numbers, the 0–15 range button can be right-clicked to produce a hex digit in the range 0–F. After stringing hex digits together, the resulting hexadecimal number can be converted to a decimal number in the Programmer mode of Windows Calculator. Where the lower bound is 0, the upper bound of a hexadecimal number is 16^n - 1, where n is the number of hexadecimal digits. To make the lower bound 1, add 1 to the hexadecimal number, and the upper bound becomes 16^n.

Another hidden feature of TruRand is the ability to get and display the frequency of the TSC (Time Stamp Counter) of the computer on which it is running. Right-clicking the 1–1024 range button causes the frequency to be displayed in MHz (megahertz) in the “Random number” text box.

Steven A. Brown
Programmer
steven.achilles.brown@gmail.com