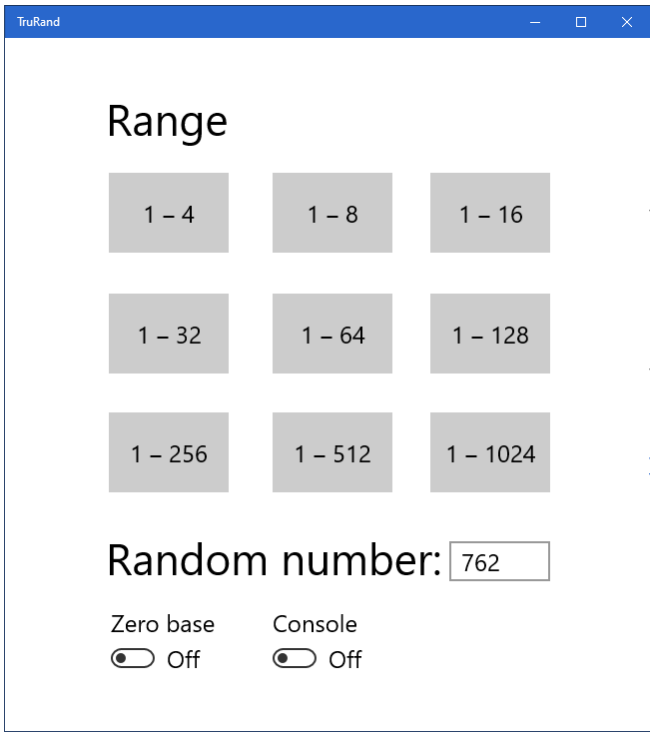
TrueRand User’s Guide

Getting started

The first time TrueRand 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 TrueRand is subsequently launched.



Using TrueRand

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 next 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 the "Zero base" switch on.

Turning the “Console” switch on outputs the generated random numbers to a terminal window. Strings of random numbers can be accumulated there and saved to a file by the following procedure. Select desired text by left-clicking and dragging the mouse pointer, then right-click or press Enter to save the selected text to the clipboard. From there, text can be pasted into an application such as Notepad and saved to disk. All of the text in the terminal window, including text that has scrolled off the top or below the bottom of the window, can be selected by clicking the small icon in the top-left corner of the terminal window, selecting “Edit” and “Select All” from the drop-down menu. The selected text can then be copied to the clipboard by pressing Enter or by right-clicking the mouse. Selected text becomes deselected when it is copied to the clipboard. A Range button should not be clicked while text is selected in the terminal window.

480 lines of text can accumulate in the terminal window buffer, regardless of the size of the window. Text can be scrolled by means of the mouse wheel when the mouse pointer is in the terminal window. When the screen buffer is full, text at the top is lost as more text is added at the bottom. To clear the terminal window of text, turn the “Console” switch off and back on again. The terminal window can be resized by the user, and that size will be saved and restored in the next session. TrueRand is closed by clicking the X in the upper-right corner of the main window, not the terminal window. If the terminal window is closed that way, settings will not be saved. The terminal window can be closed, without closing the program, by means of the “Console” switch.

Large random numbers

An arbitrarily large random number could 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, or the 0–255 range button can be right-clicked to produce two hex digits in the range 00–FF. Subsequent clicking of the right mouse button adds digits, one or two

at a time, to the hexadecimal number in the terminal window, and that number can become arbitrarily large. The resulting large hexadecimal number can be used as an encryption key, or it can be converted to a decimal number by copying it to the clipboard and pasting it into Windows Calculator, where in Programmer mode it can be converted to a decimal number. Make sure “HEX” is selected before pasting, then select “DEC” to convert to decimal.

Normally, the lower bound of a hexadecimal number is 0, and the upper bound is 16^n - 1, where n is the number of hexadecimal digits. For that reason, right-clicking the 1–16 range button or the 1–256 range button turns the “Zero base” switch on. To make the lower bound 1, add 1 to the hexadecimal number, and the upper bound becomes 16^n.

A hidden feature of TrueRand 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 output text box and in the terminal window.

Theory of Operation

Computers normally use a mathematical algorithm to generate numbers that are pseudo-random. TrueRand takes a different 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 TrueRand 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 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. The processing of an interrupt request is asynchronous with the instantaneous count in the TSC, and the time at which a human impulse to click the mouse occurs is unrelated to the timing of events in computer hardware. Hence, a number sampled from the low-order bits of the TSC, in response to a click of the mouse, is random. To draw an analogy, clicking the mouse is like throwing a dart at a wheel divided into 64 segments labeled 0 through 63, spinning at 156,250 rpm.

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 TrueRand, 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 more for a wide range and less 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. The way to preserve randomness 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 an arbitrary range of numbers within a set of random numbers is also random.

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