

v2.0 beta

True Random Number Service

Technical Details

RANDOM.ORG is a true random number service that generates randomness via atmospheric noise. This page explains how the service works.

Step 1: Collecting Raw Entropy

todo: brief overview of the whole process here

todo: a little more detail here, perhaps a figure

The way the generator works is quite simple. A PC running GNU/Linux is equipped with a series of sound cards, each of which is connected to a radio. The radios are tuned into (different) frequencies where nobody is broadcasting, and the atmospheric noise picked up by the receiver is fed into the PC through the sound card. A program samples the noise as an eight-bit mono signal at a frequency of 8 KHz. The upper seven bits of each sample are discarded immediately and the remaining bits are gathered and turned into a stream of bits with a high content of entropy.

Step 2: Initial Processing and Testing

The next step is to perform skew correction on the bit stream, in order to ensure that there is an approximately even distribution of 0s and 1s.

The skew correction algorithm used is based on transition mapping. Bits are read two at a time, and if there is a transition between values (the bits are 01 or 10) one of them - say the first - is passed on as random. If there is no transition (the bits are 00 or 11), the bits are discarded and the next two are read. This simple algorithm was originally due to [John von Neumann](#) and completely eliminates any bias towards 0 or 1 in the data. It is only one of several ways of performing skew correction, though, and has a number of drawbacks. First, it takes an indeterminate number of input bits. Second, it is quite inefficient, resulting in the loss of 75% of the data, even when the bit stream is already unbiased. [RFC1750](#) discusses skew correction in general and lists this method as well as three others. Paul Crowley has written an [article about skew correction for use with Geiger counters](#) and also maintains a page with [implementations](#) of a number of skew correction algorithms.

Finally, after the skew correction has been performed, a series of statistical tests are performed on the numbers, before they are fed to a buffering program that caches the numbers before the final processing stage. The tests are based on the test suite recommended by the US National Institute of Standards and Technology (NIST) in [NIST Special Publication 800-22](#), which deals with evaluation of random number generators. You will find more information about the tests and the current performance of the generator at the [RANDOM.ORG statistics page](#).

Step 3: Final Processing

todo: write this section from scratch