Radiation Randomness: The Entropy of Thin Air

Marcuse, Dominic

This project tested the entropy and randomness of several sets of data from different sources to determine the best way to generate random numbers. Random numbers are used in applications where randomness is important, such as cryptography. Random numbers can be generated in many ways - although in most cases, pseudorandom number generators (PRNGs - also known as "fake" random number generators) are used because there are few sources of true randomness, and they tend to be much slower than pseudo-random number generators. Radioactive decay is truly random - there is no way to predict or replicate a radioactive event before or after it has occurred. Because of this, I believe that a random number generator that uses radioactive decay to generate numbers will generate more entroptic numbers than other random number generators. For this project a random number generator that uses a Geiger counter as input was used to generate data and compare the entropy of its output with other, pre-existing generators. After running the tests, we can see that the hypothesis was correct. The RNG from Java (a programming language) scored the lowest of the three generators - because it was not a "true" random number generator. The Geiger counter generator was in the middle because it used radioactive decay, and the random.org RNG (which uses atmospheric noise) scored the highest of the three generators.

Awards Won: