CALIFORNIA STATE SCIENCE FAIR
2009 PROJECT SUMMARY

Name(s)

Dylan Freedman

Project Number

S1605

Project Title

Efficient True Random Number Generation

Abstract

Objectives/Goals

Through this project, I investigated algorithms that efficiently generated true high quality random numbers from a source of entropy. My objective was to create a random number generator that would produce high quality, cryptographically secure random numbers in large quantities.

Methods/Materials

First, I created a basic framework to implement methods in Java. I used a public online webcam focused on Times Square, New York as a source of entropy and wrote a simple class to process these pixel values. Then, I created five control methods based on preexisting algorithms or data sources. I constructed twelve of my own methods, six of which applied pseudorandom algorithms to my true source of entropy. For each of my methods, I computed the average processing time taken in bits per millisecond and the average data produced in bits per image. The quality of the random numbers outputted was evaluated with the NIST Statistical Test Suite. All of these quantities were measured with the same sample sizes.

Results

The final method I created was by far the most efficient. It strategically applied true random numbers to reseed the famous Mersenne Twister algorithm. To further obfuscate the data, it used an xor operation on the results of one iteration and the seeding values of the previous iteration. This method quickly and efficiently produced a high quantity of high quality, cryptographically secure, true random numbers.

Conclusions/Discussion

Most of the methods I created had various failures and shortcomings; however, all my methods were insightful and led to many small observations about the properties of various statistical tests for randomness. My final method fulfilled all of my project's objectives. Compared to the random number generating algorithms I have researched, this method appears to be the most effective in quantity, quality, and cryptographic security of random numbers produced.

Summary Statement

My project establishes a method that overcomes the difficulty of efficiently generating high quantities of true random numbers.

Help Received

Parents helped proofread report; Upon completion of project, received professional review from a computer scientist, a mathematics professor, and a social scientist