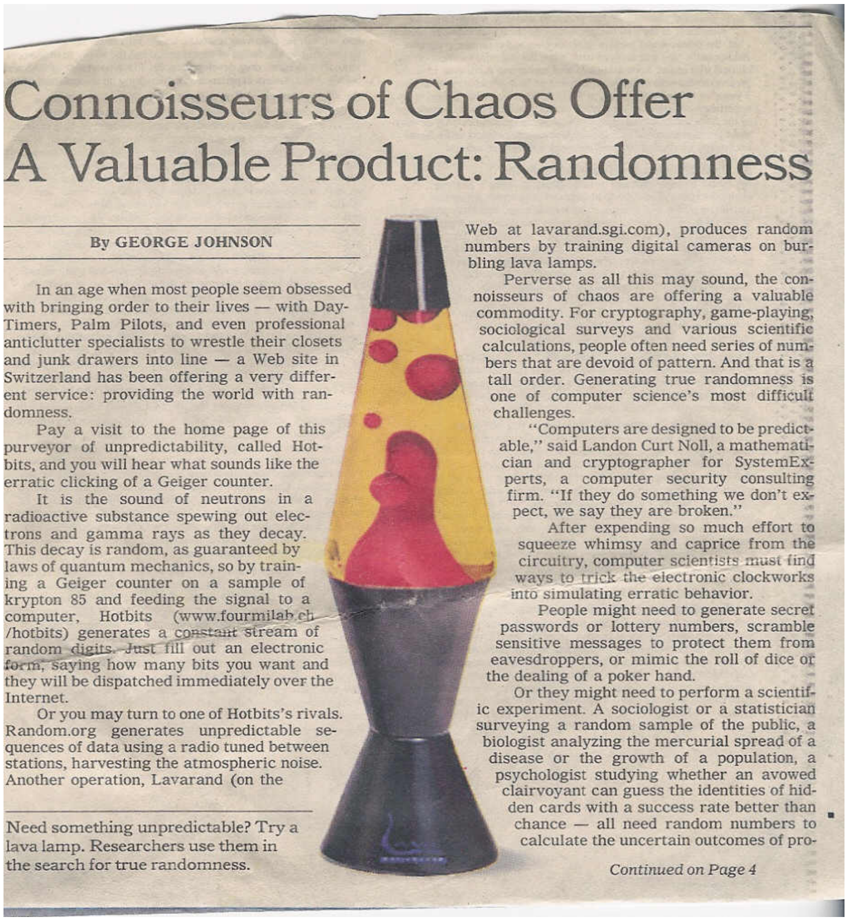

Connoisseurs of Chaos Offer A Valuable Product: Randomness

By GEORGE JOHNSON

In an age when most people seem obsessed with bringing order to their lives — with Day-Timers, Palm Pilots, and even professional anticlutter specialists to wrestle their closets and junk drawers into line — a Web site in Switzerland has been offering a very different service: providing the world with randomness.

Pay a visit to the home page of this purveyor of unpredictability, called Hotbits, and you will hear what sounds like the erratic clicking of a Geiger counter.

It is the sound of neutrons in a radioactive substance spewing out electrons and gamma rays as they decay. This decay is random, as guaranteed by laws of quantum mechanics, so by training a Geiger counter on a sample of krypton 85 and feeding the signal to a computer, Hotbits (www.fourmilab.ch/hotbits) generates a constant stream of random digits. Just fill out an electronic form, saying how many bits you want and they will be dispatched immediately over the Internet.

Or you may turn to one of Hotbits's rivals. Random.org generates unpredictable sequences of data using a radio tuned between stations, harvesting the atmospheric noise. Another operation, Lavarand (on the Web at lavarand.sgi.com), produces random numbers by training digital cameras on burbling lava lamps.

Perverse as all this may sound, the connoisseurs of chaos are offering a valuable commodity. For cryptography, game-playing, sociological surveys and various scientific calculations, people often need series of numbers that are devoid of pattern. And that is a tall order. Generating true randomness is one of computer science's most difficult challenges.

"Computers are designed to be predictable," said Landon Curt Noll, a mathematician and cryptographer for SystemExperts, a computer security consulting firm. "If they do something we don't expect, we say they are broken."

After expending so much effort to squeeze whimsy and caprice from the circuitry, computer scientists must find ways to trick the electronic clockworks into simulating erratic behavior.

People might need to generate secret passwords or lottery numbers, scramble sensitive messages to protect them from eavesdroppers, or mimic the roll of dice or the dealing of a poker hand.

Or they might need to perform a scientific experiment. A sociologist or a statistician surveying a random sample of the public, a biologist analyzing the mercurial spread of a disease or the growth of a population, a psychologist studying whether an avowed clairvoyant can guess the identities of hidden cards with a success rate better than chance — all need random numbers to calculate the uncertain outcomes of pro-

Continued on Page 4

Need something unpredictable? Try a lava lamp. Researchers use them in the search for true randomness.

… Hotbits and Random.org exist mostly as educational diversions. They don't pour out random numbers fast enough for such voracious demands as ultra high-security cryptography. Several years ago, Mr. Noll and some colleagues at the Silicon Graphics Corporation began an effort to make an industrial strength random-number dispenser out of lava lamps (or, as their maker, Haggerty Enterprises, insists they should be called, "Lava Lite" lamps.)

A lava lamp is a chaotic system, meaning that it is ruled by a phenomenon called "sensitive dependence on initial conditions." The slightest variations in the temperature, the distribution of the "lava," and many other variables lead to wildly divergent patterns in the slow, burbling ballet.

Throwing in even more wild cards, Mr. Noll and his cohorts used six lava lamps, each of a different color. The result was called Lavarand. Every second a digital camera snapped an image of the fluctuating scene converting the array of pixels into a string of bits.

This stream of ones and zeroes still contained an undesirable amount of predictability. The lava, after all, had to stay within the confines of the six stationery lamps — it couldn't go jumping from one to another. A red lava lamp couldn't randomly turn yellow or blue.

To weed out the pockets of order, the scientists sent the signal through an automatic number mangler called a hash function — a kind of distiller of randomness. A tiny fluctuation in the algorithm's input — a subtle variation in the brightness or hue of a single pixel — would cause the output to wildly fluctuate. The result was a smaller, messier bit string — call it Essence of Chaos. Finally these digits were used to seed a heavy-duty pseudorandom generator called a **Blum Blum Shub** (after its inventors, the computer scientists **Lenore Blum, Manuel Blum** and **Mike Shub**.)

…

See: **Connoisseurs of Chaos Offer a Valuable Product: Randomness**

The New York Times, July 12, 2001