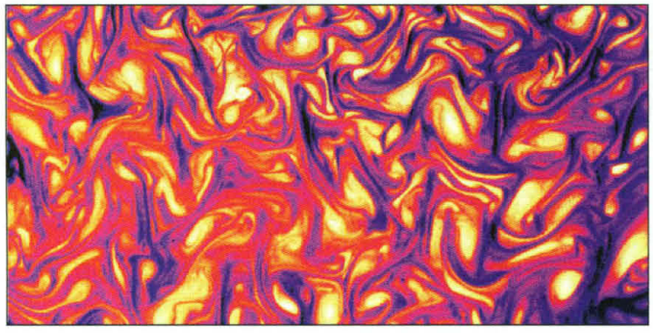
NETWATCH

edited by Jocelyn Kaiser



P. VOROBIEFF AND R. ECKE/LANL

COOL IMAGES

Sudsy Physics

Soapy water swirls at various speeds in this false-color image of turbulence in a soap film—water sandwiched between layers of surfactant molecules. Ordinary though soap films may seem, physicists look to them as a model for two-dimensional turbulent flows in the oceans and on the surfaces of some planets. This image, posted at the American Institute of Physics (AIP) site, is from an experiment in which Peter Vorobieff of Los Alamos National Lab and others used a digital camera to quantify how thickness and velocity are related in flow throughout an entire soap film, not just at certain points, as they report in the 17 August *Physical Review Letters*.

AIP's Physics News Graphics page holds dozens of images and drawings from news features over the past 2 years on everything from purported cosmic snowballs to sonoluminescence. Many are nuts-and-bolts diagrams, but others, like these soapy twists, are quite striking. www.aip.org/physnews/graphics/

HOT PICKS

Cyber lecture hall. Hear live talks this fall by Judah Folkman on angiogenesis, W. French Anderson on gene therapy, and others in a 1997–1998 George Washington University series of audio-streamed biomedical lectures at this site, which includes archives of past talks. 207.78.88.15/

Sport and spots. What ties together baseball and sunspots? No, not a dropped fly ball. They are the subjects of two new online exhibits at the San Francisco Exploratorium. Sunspots features history, images, and interviews with solar physicists, while Science of Baseball will fill you in on the physics of a curve ball, how weather affects a home run, and more. www.exploratorium.edu

NET NEWS

Race to Pick a Better U.S. Cipher

Last month, 15 teams of cryptographers began a unique and unprecedented contest: Their proposed codes are vying to become the U.S. government's new standard for encoding sensitive data. Like the current Data Encryption Standard (DES), the winner of the competition—run by the National Institute of Standards and Technology (NIST)—will likely become the de facto standard for all sorts of commercial applications as well, from automatic teller machines to video phones.

The need to replace DES became more apparent in July, when a group of cryptologists cracked a DES-encoded message in just 3 days. Their computer, called "Deep Crack," picked the DES lock by brute force, trying combinations until it found one that worked. Each "combination" is a random string, or key, of 56 bits. Though the feat made headlines, it was scarcely news to cryptologists, who have argued for years that 56-bit keys are too short. In fact, the secret message decoded by Deep Crack read: "It's time for those 128-, 192-, and 256-bit keys."

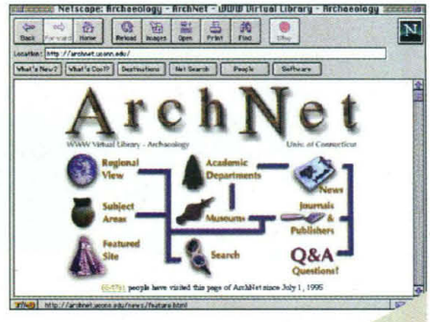
NIST asked for proposals to create a new Advanced Encryption Standard last year and announced the 15 candidates from around the world last month. The entrants include IBM, which developed DES in 1977, and RSA Labs, which sponsored the decryption contest in July. Each group has made its algorithm available on the Web so that other cryptanalysts can look for weaknesses (www.nist.gov/aes). (Indeed, at least one has already been cracked.) NIST will also judge the schemes on speed and adaptability to different platforms. Though the field will be narrowed to five candidates in 1999, just how NIST will determine a winner is still uncertain. "The world has never picked an encryption standard from a multiplicity of choices," says Bruce Schneier, president of Counterpane Systems, one of the entrants. "We're learning as we go."

SITE VISIT

Digging Into Archaeology Online

Archaeologists spend enough time in the field sifting through dirt and junk to find a few artifacts. So, when it comes to the Web, they welcome help in combing through the detritus. One of the best repositories of archaeological information is ArchNet, a Web directory of everything from virtual tours of digs to software for classifying projectile points.

Nicely designed with a home page in seven languages, the University of Connecticut–hosted ArchNet sorts hundreds of Web sites by subject and geographic region. A brief sampling: Radiocarbon dating labs, a course in Australian archaeology, a list of references on antiquities theft, a space radar image of China's silk road, and even a site at Texas A&M University that posts the latest news stories on anthropology. ArchNet also points to museums, journals and news groups, and more archeo Web directories, including one for Europe. Some sections, like reviews of notable sites, haven't been updated for a while, but ArchNet's Jonathan Lizee explains that the reason is a deluge of e-mails suggesting around 25 new sites a day. He and colleague Tom Plunkett now plan to make the site an automated database, although they'll still check for quality: "We do want to represent the best face of archaeology," Lizee says. "That's been our goal all along."



archnet.uconn.edu

SCIENCE ONLINE

Lunar Prospector is in the midst of a 1-year voyage to map our moon. This week's *Science* features seven Reports on the latest scientific results from the mission, which has found signs of water ice and an iron core, among other details. The Prospector Reports are available to all interested readers—including those without online subscriptions—at www.sciencemag.org

Send Internet news and great Web site suggestions to netwatch@aaas.org