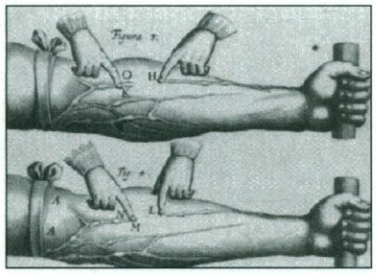
NETWATCH
edited by ERIK STOKSTAD

COOL IMAGES

Old Medicine



Ever since William Harvey demonstrated in 1628 how blood circulates in the body, his landmark treatise *De Motu Cordis* has been a model of observation and experimentation. You can download some of Harvey's famous illustrations, such as this engraving, and many other icons of medical history by visiting Images From the History of Medicine.* A project of the U.S. National Library of Medicine, the Web site contains nearly 60,000 prints and photographs—ranging from medieval astrology to Victorian slums. Although most images predate the 20th century, you can also find photos of World War I hospitals and international posters in the fight against AIDS. "People who like to teach with slides have a wonderful resource here," says Elizabeth Fee, chief of the History of Medicine Division. High resolution reproductions can also be ordered.

* wwwihm.nlm.nih.gov

HOT PICKS

It's a breeze. From dew points to Doppler radar, the Weather World 2010 Project explains the basics behind everyday weather and presents case studies of devastating events such as Hurricane Andrew. ww2010.atmos.uiuc.edu/(Gh)/guides/mtr/home.rxml

A small world. In addition to keeping tabs on the United States, the Census Bureau Web site hosts a demographic database of 189 other countries. Get the latest stats on global population growth, including a special report on the impact of the HIV pandemic, at www.census.gov/ipc/www/wp98.html

Transgenic grapevine. Biotech buy outs and mergers, layoffs and splits, hot technologies, lawsuits, the risks of transgenic foods ... get the latest gossip on the industry or add your own two cents in comfortable anonymity at the Biotech Rumor Mill. www2.biofind.com/rumor

NET NEWS

Hunting for Passwords

The boss is lunching at Burger King, and he's left his office open and his computer running. Can you find the secret digital key on his computer that authorizes electronic fund transfers and move $1000 surreptitiously from the company's bank account into your own? According to two computer scientists, if the key is stored on a typical 2-gigabyte hard drive, it's possible to find it before the boss finishes his cheeseburger.

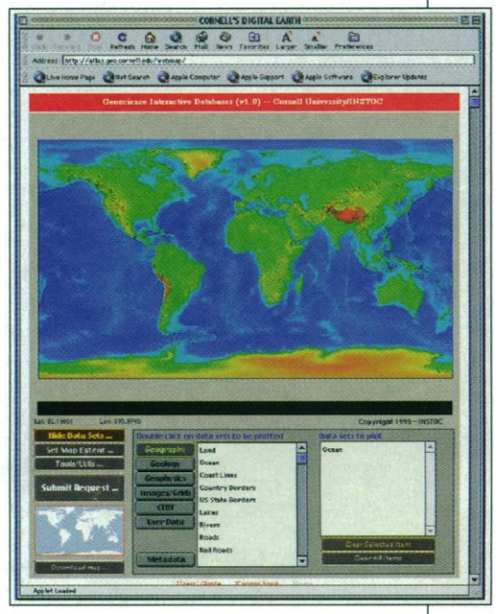
Software makers often hide the secret keys needed to run encryption programs inside the reams of code that make up the program, assuming this will provide sufficient protection against unwanted detection. "You could call that the needle-in-the-haystack approach," says Nicko van Someren of nCipher Corp. in Cambridge, United Kingdom. "We've just invented the metal detector for finding the needle."

Designed by van Someren and Adi Shamir of the Weizmann Institute of Science in Rehovot, Israel, the detector is simply a program that looks for unusually random bits of code. The data in a typical computer program may look like gibberish, but it's highly patterned. By contrast, a typical encryption or decryption key is usually made of random data, with no pattern at all. At the Financial Cryptography '99 conference in Anguilla last February, van Someren announced that he'd used this strategy to find the key required to add a plug-in to a commercial encryption program. The key is publicly available in the United States, but the company that makes the program was not allowed to provide it to nCipher because of U.S. export restrictions. "The developer had assumed we'd never be able to find it," van Someren says.

The problem of hiding keys "can become a serious issue," especially in the coming era of e-commerce, says Yakov Yacobi, the head of the cryptography group at Microsoft Research. The long-term solution, he believes, is to store keys on hardware, such as smart cards, that can be detached from the computer. When smart cards become available—probably in a year or so—he predicts that they will be an essential ingredient in the security of e-commerce.

SITE VISIT

Digital Earth



Forget about rifling through musty library drawers to find a geologic map—a new Web site* makes plotting your own detailed maps almost effortless. The Geoscience Information System Interactive Map Server, created by the Institute for the Study of the Continents at Cornell University, allows anyone to tailor and download maps with everything from earthquakes to active volcanoes.

To make a map, you choose an area with the cursor or punch in longitude and latitude, then select from menus to add features such as rivers, roads, and cities. It's also fairly easy to create a profile of regional topography or cross sections of Earth's crust in some areas. You can learn about the rocks underfoot anywhere in the United States (down to 1:2,500,000 scale—"good for statewide views," says Dogan Seber, a geology research associate who manages the site), Africa, and the Middle East, but the database's geological records are spotty for other regions. You can also upload your own data.

The site's own maps are interactive: Click on a volcano, for example, and you'll learn when it last erupted. Appendices describe the source and quality of all the available data.

* atlas.geo.cornell.edu

Science ONLINE

Most scientists loathe the idea of marketing. But get involved with a start-up company, and you'd better know how to make a pitch. Check out the latest "Learnin's From My MBA" column on *Science*'s Next Wave. www.nextwave.org

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