SCIENCE NEWS®
The Weekly Newsmagazine of Science

Science Service Publication
Volume 152, No. 6, August 9, 1997

Thomas Peter Bennett	Publisher
Julie Ann Miller	Editor
Blair Burns Potter	Managing Editor
Dan Skripkar	Production/Design Director
David Lindley	Associate Editor
Janet Raloff	Senior Editor Environment/Policy
Ivars Peterson	Online Editor Mathematics/Physics
Bruce Bower	Behavioral Sciences
Richard Monastersky	Internship Coordinator Earth Science
Kathleen Fackelmann, Nathan Seppa	Biomedicine
Ron Cowen	Astronomy
Christine Mlot	Life Sciences
John Travis	Biology
Corinna Wu	Chemistry/ Materials Science
Evelyn Strauss	Science Writer Intern
Meghan Mitchell	Editorial Assistant
Cait Anthony	Books/Advertising
Donald R. Harless	Business Manager

SCIENCE NEWS (ISSN 0036-8423) is published weekly on Saturday, except the last week in December, for $49.50 for 1 year or $88.00 for 2 years (foreign postage $6.00 additional per year) by Science Service, 1719 N Street, N.W., Washington, D.C. 20036. Preferred Periodicals postage paid at Washington, D.C., and additional mailing office. POSTMASTER: Send address changes to SCIENCE NEWS, P.O. Box 1925, Marion, Ohio 43305. Change of address: Four to six weeks' notice is required — old and new addresses, including zip codes, must be provided.

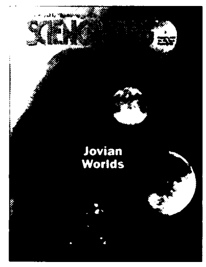
Editorial, Business, and Advertising Offices
1719 N St. N.W., Washington, D.C. 20036
202-785-2255; *scinews@sciserv.org*

Subscription Department
P.O. Box 1925, Marion, Ohio 43305
For new subscriptions and customer service, call 1-800-552-4412.

This Week

Research Notes

Articles



Cover: Four alien worlds—the large moons of Jupiter known as (top to bottom) Io, Europa, Ganymede, and Callisto—are revealing their distinctive personalities. Data recorded by the Galileo spacecraft are providing new evidence that the tug-of-war between these moons and Jupiter has profoundly affected the moons' evolution. This composite image includes a snapshot of Callisto taken by Voyager in 1979 and photos of the other moons from Galileo's current mission. (Image: NASA/JPL)

Departments

SCIENCE NEWS is published by Science Service, a nonprofit corporation founded in 1921. The mission of Science Service is to advance the understanding and appreciation of science through publications and educational programs.

Letters

Anatomically correct cover?

The 3,000-year-old Olmec clay vessel on the cover of the June 14 SCIENCE NEWS may, as you state, "mistakenly depict the heart with two chambers." But I am struck by its anatomically correct depiction of the typical branching off the aorta of a right brachiocephalic trunk, left common carotid artery, and left subclavian artery.

The Olmec may have been better gross anatomists than you suspect.

J. Roger Eagan
Associate Professor of Biology
Adirondack Community College
Queensbury, N.Y.

For a more complete description of the Olmec vessel, see "The Olmec Heart Effigy: Earliest Image of the Human Heart" in the Spring 1997 PERSPECTIVES IN BIOLOGY AND MEDICINE. *The author, Gordon Bendersky of Allegheny University–Hahnemann School of Medicine in Elkins Park, Pa., calls the effigy "the earliest recognizable representation of a [human] heart."* —The Editors

Info secure for trusting parties

In failing to distinguish between two- and three-party cryptographic settings, "Quantum cheating" gives a confusing picture of the implications of the recent discovery that quantum bit commitment is intrinsically insecure (SN: 6/14/97, p. 373).

In the traditional three-party setting—described, for example, in Peterson's lucid article on the quantum cryptographic experiments under Lake Geneva ("Bits of Uncertainty," SN: 2/10/96, p. 90)—the goal is to protect two cooperating users, at opposite ends of the channel, against tampering or eavesdropping by an adversary. In this setting, quantum cryptography is believed to be secure against all attacks allowed by the laws of physics.

In contrast, two-party scenarios aim to enable two mutually distrustful parties to reach a common understanding or decision, despite possible cheating by one party. This is sometimes called post–Cold War cryptography—there is no explicit enemy, but one must cooperate with people one does not entirely trust. Bit commitment, the basic component that Mayers and Lo and Chau have shown to be insecure, is an essential ingredient in all known two-party cryptographic protocols but is not used in the three-party setting.

Thus their discovery, at least in theory, undermines the security of all schemes aiming to facilitate cooperation between two mutually distrustful parties, but it has no known impact on traditional quantum cryptographic schemes aimed at defending against eavesdropping and tampering by a third party.

Charles H. Bennett
IBM Thomas J. Watson Research Center
Yorktown Heights, N.Y.