Computers

Adopting a digital signature standard

Handwritten signatures on checks, contracts, and other paper forms have long served as a means of affirming that the contents of these documents are authentic. Last month, after nearly 3 years of debate, the National Institute of Standards and Technology in Gaithersburg, Md., announced the approval of the Digital Signature Standard (DSS), which performs a similar function for electronic messages and data (SN: 9/7/91, p.148).

The cryptographic technique underlying the signature standard generates a special number that allows users to verify both the integrity of the electronic information and the identity of the signer. However, though this method can be used to detect tampering and to prevent forgery of signatures, it does not encrypt the file or message itself.

The DSS makes use of a particular variant of a technique known as public-key cryptography. Such schemes require two mathematically related "keys" – one for creating a digital signature as a scrambled string of bits and a complementary key for verifying the encoded signature.

The government insists that its version does not infringe on any of the patents on public-key cryptosystems held by various individuals and companies. It says it will not charge royalties to anyone using the standard. But several inventors have indicated they may sue the government for patent infringement.

Critics have also argued that the government standard is inefficient and may not be trustworthy. A number of computer companies have already adopted an alternative, competing public-key signature scheme for their products.

Prying open the Clipper lock

In the never-ending cat-and-mouse game between those who want to keep secrets and those who want to find them out, the advantage continually shifts from one side to the other.

In a draft paper, computer scientist Matthew Blaze of AT&T Bell Laboratories in Murray Hill, N.J., describes several ways he has discovered for circumventing an important component of the "key-escrow" encryption technology proposed by the federal government as a means of protecting privacy while allowing authorized law enforcement agents to decipher digitally scrambled speech or data (SN: 2/12/94, p.100). Although these loopholes apply only to computer-to-computer communication and don't directly threaten the security of the data encryption system itself, they pinpoint potential weaknesses in certain aspects of the key-escrow plan.

First proposed last year, key-escrow encryption requires the use of a special integrated-circuit chip (sometimes called Clipper) to encrypt digitized speech and data according to a classified mathematical formula. The scheme also provides a special master key, divided into two parts accessible only to authorized officials, to unlock an encrypted message.

To demonstrate one example of a possible flaw, Blaze devised a computer program that makes it practically impossible for the government to unscramble an encrypted data transmission. He does it by taking advantage of the fact that to obtain the right master key to decipher a message, the government has to find out the encryption chip's serial number. This serial number is normally included in a special setup code (called a law enforcement access field, or LEAF) exchanged between two computers at the start of data transfer.

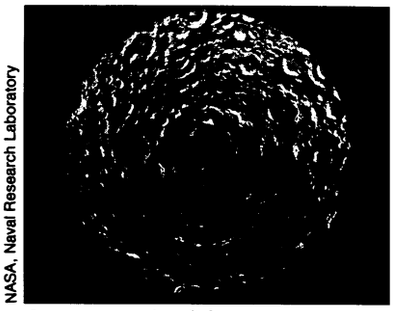
By trying all the mathematical possibilities, Blaze's computer program finds a 16-digit number, called a checksum, used to verify that the LEAF is legitimate. It then substitutes a bogus LEAF, which has the same checksum but includes a fake serial number that can't be used by the government. Officials of the National Security Agency concede the existence of the flaw but say Blaze's strategy takes too long to apply in a realistic situation.

Astronomy

Ron Cowen reports from Baltimore at a meeting of the American Geophysical Union

Ice on Earth's moon?

In its 71 days of orbiting the moon, the Clementine spacecraft took some 1.5 million images in 11 visible and near-infrared colors (SN: 5/21/94, p.326). A mosaic of 1,500 images of the lunar south pole is proving particularly intriguing. The pictures reveal for the first time a 300-kilometer-wide depression, probably an ancient impact basin, near the pole.



NASA, Naval Research Laboratory

Image mosaic of the lunar south pole shows a dark depression at the center.

The heavily shadowed depression may never receive sunlight, says Clementine investigator Eugene M. Shoemaker. If so, the basin may remain at a frigid -230°C and could be an icy storehouse for water delivered to the moon by comets.

"This is the place on the moon where you would go to get ice for your cocktail," jokes Shoemaker, who has retired from the U.S. Geological Survey in Flagstaff, Ariz. In fact, however, any ice deposit would yield a supply of water too dirty for drinking. But its oxygen and hydrogen molecules could provide a valuable resource for refueling spacecraft if a lunar base were established.

Shoemaker adds that a Clementine experiment to analyze the echoes of radio waves beamed by the craft into the south polar area should indicate whether ice exists there.

Ida's moon: Not a chip off the old block

Data are still trickling in from last year's photo shoot of the asteroid 243 Ida. The Galileo spacecraft recorded pictures and spectra of this rocky body when the probe flew within 2,400 kilometers of Ida on Aug. 28, 1993. But because its main antenna is crippled, Galileo had to store the images on its tape recorder and can transmit them only at a painfully slow rate.

Images radioed 3 months ago confirmed that Ida has a tiny moon orbiting it, the first satellite of an asteroid ever observed (SN: 4/2/94, p.214). According to one theory proposed for the origin of the 1.5-km-wide moon, an object that slammed into Ida some time in the past gouged out enough material to form the orbiting body. But new data from the Galileo flyby show that despite similarities in color and brightness, Ida and its moon seem to have different compositions.

Galileo's near-infrared mapping spectrometer hasn't examined the mineral composition of Ida's entire surface, but those regions it has looked at consist mainly of the mineral olivine, with traces of orthopyroxene. In contrast, the moon's surface appears to have roughly equal mixtures of these two minerals and one other, clinopyroxene.

The compositional differences "suggest the moon is not a chip off the asteroid," says Galileo investigator Robert Carlson of NASA's Jet Propulsion Laboratory in Pasadena, Calif. But even if Ida and its moon aren't mother and daughter, they are probably kin. Clark R. Chapman of the Planetary Science Institute in Tucson describes a model in which a violent impact broke a large asteroid into myriad fragments, one of which was Ida. A smaller fragment could have been captured by Ida and become its moon.

To better estimate Ida's size, scientists have now compared a high-resolution image of the asteroid received last fall with recently relayed images. The newly received images show several views of the rotating asteroid during a 3.3-hour interval. (Ida makes one complete revolution in 4.5 hours.) According to this analysis, the asteroid is about 58 km long and 23 km wide.