Digital Security Signed, Sealed, Delivered

The handwritten signature at the end of a letter or contract stands as a simple and reasonably reliable means of authenticating the document. But when a document exists only in electronic form, anyone can affix an identifying string of electronic characters, or alter the text itself, without leaving a trace of forgery.

Over the last decade or so, computer scientists and cryptographers have developed a variety of ingenious schemes, known as digital signatures, to guarantee that an electronic document is genuine. Now the National Institute of Standards and Technology (NIST) in Gaithersburg, Md., has issued a proposal for a digital signature standard, which allows recipients of electronically transmitted information to verify the sender's identity and the data's integrity. The announcement appears in the Aug. 30 FEDERAL REGISTER.

"The fact that the government has finally come forth with a proposed standard is very important," says Stephen T. Walker, president of Trusted Information Systems, Inc., in Glenwood, Md. "It's too bad that it's taken so long. There's a whole lot of areas where digital signatures are crucial."

The proposed standard specifies a particular mathematical procedure for creating and verifying a digital signature. Although it would apply only to unclassified information in federal government computer systems, it would likely have a considerable influence on other computer users as well. Many companies, for example, have been reluctant to select a particular digital signature scheme for their electronic transmissions without some assurance that the chosen method will be widely used and that it harbors no weaknesses that could be exploited by an unscrupulous party bent on fraud.

"The existence of a standard should make vendors more willing to offer [a digital signature scheme] and people more willing to use it," says Joan Feigenbaum of AT&T Bell Laboratories in Murray Hill, N.J.

But controversy surrounds NIST's choice of an unfamiliar mathematical algorithm as the federal standard for generating and verifying a digital signature. "If no one challenges what they've done, we'll be stuck with a weakened standard," says Jim Bidzos, president of RSA Data Security, Inc., in Redwood City, Calif., which produces equipment and software based on a rival, proprietary digital signature and encryption method known as RSA.

The proposed NIST algorithm, like most digital signature methods, relies on a concept known as public-key cryptography. Such schemes use two mathematically related "keys" – one for encrypting a message as a scrambled string of bits, and a complementary key for unscrambling the encoded message.

Because one key can't easily be derived from the other, a user can keep one key secret, using it to create a digital signature, and make public the other key so that anyone can verify – but not forge – that signature. The same procedure can be applied to a sample of bits from the text itself, which acts as a kind of fingerprint to allow detection of surreptitious alterations in an electronically transmitted or stored document.

The RSA method is the most widely used and best-known method for producing such keys for both encrypting messages and creating digital signatures. Its security depends on the computational difficulty of factoring a large number to find the two prime numbers that were multiplied together to generate the original number. In contrast, the proposed NIST method relies for its security on the difficulty of computing what are called discrete logarithms.

At a congressional hearing in June, NIST Deputy Director Raymond G. Kammer described the criteria used to select the proposed standard. "Our efforts in this area have been slow, difficult and complex," he testified. "We evaluated a number of alternative digital signature techniques and considered a variety of factors in this review." Those factors included the degree of security provided, the ease of implementation in both hardware and software, the ease of export from the United States, the applicability of patents, and the level of efficiency for generating and verifying signatures.

Guided by these criteria and assisted by representatives from the National Security Agency, NIST officials rejected the RSA method, which is protected by a number of patents in the United States, and developed an alternative approach that, according to government lawyers, isn't covered by existing patents. The future of the proposed standard now depends on how well it survives a concerted mathematical attack regarding its security, and on the resolution of any conflicting patent claims that may arise.

"Should there be some kind of weakness, [NIST] is putting its method into the public record in order to enable people to try to uncover that weakness," says computer scientist Michael O. Rabin of Harvard University. "If the system passes the mathematical test, then it would certainly be a possible way of doing digital signatures." – *I. Peterson*

Milking engineered 'pharm animals'

In the first steps toward populating a biotechnological barnyard, research teams in the United States and Scotland report that genetically engineered goats and sheep can secrete medically useful quantities of drugs in their milk. And according to scientists in the Netherlands, cows may become the next four-legged drug factories down on the pharm.

All three groups, who describe their work in the September BIO/TECHNOLOGY, say the new findings illustrate the potential of harnessing transgenic livestock to produce drugs more rapidly, more cheaply and in greater quantities than the standard "bioreactor" approach, in which vats of gene-altered bacteria or culture dishes of animal cells churn out genetically engineered drugs.

"Commercialization of this technology will permit further development of complicated proteins that are currently difficult and expensive to produce with bacteria or mammalian cells," says Henri A. Termeer, chairman of Genzyme Corp. in Cambridge, Mass.

"Our success with transgenic goats demonstrates the feasibility of producing commercially viable pharmaceuticals from livestock," adds Karl M. Ebert of Tufts University School of Veterinary Medicine in North Grafton, Mass., who coordinated the goat experiments in collaboration with Genzyme.

Genzyme

The milk of this transgenic nanny contains the clot-dissolving drug TPA.

The Tufts-Genzyme study yielded two goats – one male, one female – carrying human genes for an enzyme called tissue plasminogen activator (TPA). Many countries, including the United States, have approved TPA for dissolving blood clots in cases of myocardial infarction, the primary cause of heart attacks.

Ebert and his collaborators produced the transgenic goats by surgically remov-

ing fertilized eggs from normal female goats and injecting the eggs with hybrid genes, which consisted of human TPA genes embedded in genes from goat mammary glands. They surgically implanted more than 200 such eggs into 36 "foster mothers" to yield 29 offspring, only two of which actually carried the hybrid gene. When the female transgenic goat matured and bore her own offspring, she produced a daily supply of 3 to 4 liters of milk containing an average TPA concentration of 3 micrograms per milliliter. One of her five kids inherited the hybrid gene.

Analysts have predicted that milk from transgenic animals must contain more than 1 microgram of drug per milliliter in order for the procedure to prove cost effective as a means of manufacturing pharmaceuticals. The Tufts and Genzyme researchers say they have since refined their gene-splicing technique, producing a female goat that churns out 3 *milli*grams of TPA per milliliter — 10 times the concentration secreted by the first female. A small herd of such goats could match the daily output of a 1,000-liter bioreactor, they estimate.

Researchers in Edinburgh, Scotland, report even greater production efficiency with transgenic sheep. Alan Colman of Pharmaceutical Proteins Ltd. and his colleagues engineered four ewes to carry the human gene for the enzyme alpha-1 antitrypsin. Currently extracted from human blood serum, alpha-1 antitrypsin is used to treat people who risk life-threatening emphysema because of an inherited deficiency of the enzyme. One of the transgenic ewes secreted 35 grams of the drug per liter of milk — nearly 18 times the concentration found in human serum and more than one-fifth the yearly dose required to treat one patient. The other three ewes produced several grams of the drug.

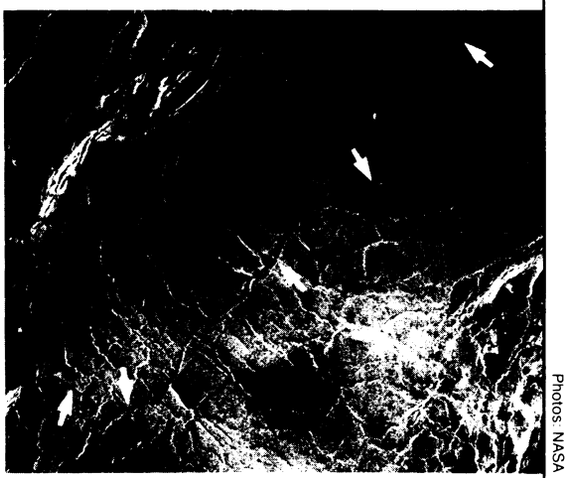
But the Holy Grail of "molecular pharmers" is the production of a drug-lactating dairy cow. Cows can produce thousands of liters of milk per year — far more than goats or sheep. But the expense of performing multiple surgeries on large animals to retrieve the eggs and implant the embryos has stymied efforts at bovine bioengineering. Now, Dutch researchers say they have devised a way to circumvent the surgeries.

The team, led by Herman de Boer at Gene Pharming Europe B.V. in Leiden, obtained bovine eggs from a slaughterhouse, fertilized them in test tubes and then inserted hybrid genes coding for lactoferrin, an antibacterial protein. Using vaginal injections, they implanted 103 of the resulting embryos in the wombs of normal cows, for a yield of 19 calves. One male and one female calf carried the new gene, although the female had only an inactive fragment. The researchers hope to get better results in a repeat of the experiment. — *C. Ezzell*

Record-breaking revelations from Venus

Two record-breaking discoveries — unveiled in a single day — offer compelling evidence of Venus' geologic activity, both past and present.

On the morning of Aug. 30, researchers announced that radar images of Venus revealed the solar system's longest channel, an ancient trough longer than the Nile River. Hours later, at a hastily called press conference, the same team announced an even more dramatic finding: Other images showed that Venus suffered a massive landslide sometime in the past several months, providing the first confirmation of current geologic activity on a planet other than Earth.



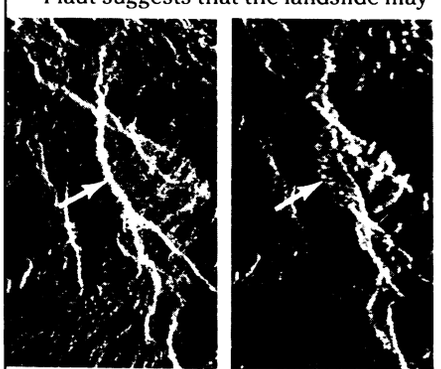
Photos: NASA

Magellan radar image shows a 360-mile-long section of a meandering Venusian channel (arrows), the longest known in the solar system.

Jeffrey Plaut of the Jet Propulsion Laboratory in Pasadena, Calif., says he discovered the landslide while comparing two radar images of Aphrodite Terra, an equatorial plateau. The Magellan spacecraft took one of the images last November and the other in July during its second trip around Venus. Placed side by side under a stereoscope, the images should have merged to form a three-dimensional view of a cliff and steeply sloping valley, with bright areas representing the most jagged regions. But a bright patch at the base of the valley, clearly visible in the July image, did not appear in the earlier picture.

Plaut interprets the patch as a massive heap of rocks, roughly 1 mile wide and 4 miles long, that fell from the cliff at some point during the eight-month interim. A third, more recent Magellan image also shows the feature, he says.

Plaut suggests that the landslide may have been triggered by an underground disturbance, such as a "Venusquake," or by a fracture originating at the planet's surface. It probably released as much energy as a magnitude 5 earthquake, he calculates. Though exciting, the discovery that Venus continues to experience geologic upheavals isn't surprising, he adds, since previous evidence suggests the planet has undergone many volcanic eruptions during the past several million years. Plaut says he expects Magellan to capture other such events as it continues to map Venus.



Left: Aphrodite Terra region as seen by Magellan last November. Arrow points to a fracture. Right: In this image of the same area, taken in July, the fracture has moved to the right and a bright patch (arrow) appears next to it. The patch may depict a large deposit of rocks from a landslide that occurred between mappings.

Magellan's other radar revelation emerged in images taken in August. The unusually long channel, stretching across the plains of Venus for 4,200 miles, begins just above the equatorial highlands in a region west of Atla Regio and follows a smoothly curving, northward course toward a large basin called Atalanta Planitia. Soviet spacecraft spied sections of the trough in 1984, but only with Magellan's higher resolution could researchers gauge its full extent, says project scientist Steve Saunders of the Jet Propulsion Laboratory.

Magellan had previously mapped similar, shorter channels on the Venusian plains. Many of these terminate at lava flows, suggesting they were carved out by molten lava from a volcanic eruption, Saunders says. But it's difficult to understand how a lava flow could have remained fluid long enough to create a channel as extensive as the newly discovered one, he adds.

In a rugged terrain of ridges and impact craters, the remarkably uniform width of this trough — which averages 1.1 miles across — poses another puzzle, says Saunders. He speculates that the region may have been far smoother when the lengthy channel originally formed. — *R. Cowen*