ston in violation of the Animal Welfare Act and Good Laboratory Practices regulations. In a settlement with USDA in 1999, the foundation, without admitting guilt, agreed to give up half of its chimps.

As part of that agreement, NIH in May 2000 took custody of 288 of Coulston's animals, many of which had been infected with HIV or hepatitis C. In May 2001, NIH awarded a contract to Charles River Laboratories to care for the animals at a primate facility at Holloman Air Force Base outside Alamogordo, a property Coulston had been managing. A month later, NIH allowed Coulston's Animal Welfare Assurance to lapse. That left Coulston with more than 250 chimpanzees at its main Alamogordo facility but no possibility of government funding and few private customers.

Looking forward. The Coulston Foundation's chimpanzees will be retired from research.

In December, a local bank filed suit to recover $1.2 million in unpaid loans (*Science*, 18 January, p. 421). Facing mounting debts, Coulston began negotiations with CCCC last spring. The center announced its agreement with Coulston last week. For now, the chimpanzees and monkeys will remain at the Alamogordo facility, Noon says. But the Arcus Foundation in Kalamazoo, Michigan, which donated the $3.7 million for the Coulston purchase, has said it will help fund additional construction at CCCC's sanctuary in Florida.

John Strandberg, head of the National Center for Research Resources at NIH, says the animals' retirement should not affect researchers. "There are enough chimpanzees in the program now to meet needs," he says. "I definitely think it's a positive development. These animals needed a long-term-care solution, and the Center for Captive Chimpanzee Care is able to provide that."

Coulston spokesperson Don McKinney says that the Coulston Foundation will continue to exist but that it "will be taking a different research direction, closer to pure science." He declined to elaborate.

–GRETCHEN VOGEL

CREDIT: (TOP) CRYSTAL MILLER/SPIEGEL/AAVS

COMPUTER SECURITY

Crucial Cipher Flawed, Cryptographers Claim

It was supposed to be as secure as a bank vault: a cryptographic algorithm that would make documents unintelligible to prying eyes for the foreseeable future. But two cryptographers say the vault, the Advanced Encryption Standard (AES), has a hole in it. Although some of their colleagues doubt the validity of their analysis, the cryptographic community is on edge, wondering whether the new cipher can withstand a future assault.

"It's nerve-wracking for me that this stuff is going on," says William Burr, the manager of the Security Technology group at the National Institute of Standards and Technology (NIST) in Gaithersburg, Maryland. "It's very worrisome if [the analysis] holds up, but it may not hold up."

Two years ago, NIST selected an algorithm to replace the aging Digital Encryption Standard. DES, the national standard for a quarter-century, was arguably the most widely used encryption algorithm in the world. But when it began to show its age, NIST held a competition to determine the next standard (*Science*, 19 May 2000, p. 1161). Rijndael, an elegant algorithm created by two Belgians, Vincent Rijmen of the Katholieke Universiteit Leuven and Joan Daemen of Proton World International, a company that makes smart cards, won the contest and became the AES (*Science*, 6 October 2000, p. 25).

Now, attacks aimed at the heart of Rijndael and other algorithms point to a possible weakness. Cryptographers Nicolas Courtois, who works for technology corporation SchlumbergerSema in Louveciennes, France, and Josef Pieprzyk of Macquarie University in Sydney, Australia, believe they have undermined the algorithms by rewriting their "S-boxes."

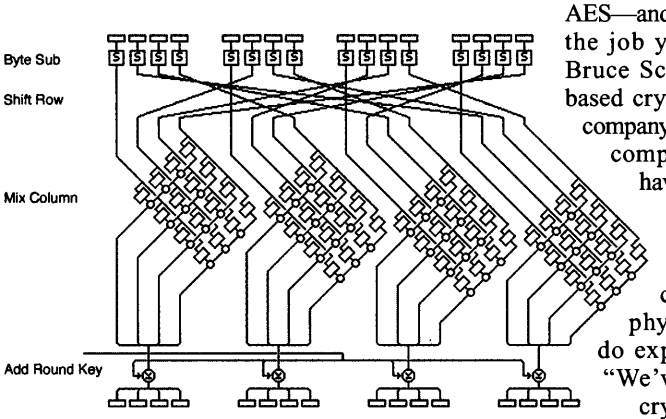
S-boxes are a crucial element in many ciphers. An S-box adds unpredictability to an algorithm. It takes a string of ones and zeros and returns a different set, turning small changes in input into large changes in output—a boost that makes the algorithm much more difficult to crack. Probing for weaknesses, Courtois and Pieprzyk rewrote Rijndael's S-boxes as a system of equations that a cracker must solve to break the cipher. "[Each S-box] can be described by a small system of equations," says Courtois. "Nobody thought it would matter."

But it does matter. Earlier this year, cryptographers Sean Murphy and Matt Robshaw of the Royal Holloway University of London showed that the S-boxes can be reformulated in a way that Courtois and Pieprzyk exploited to make their attack a force to be reckoned with. All told, Courtois and Pieprzyk believe that they have an attack of order 2^{100}: That is, it takes roughly 2^{100} operations to crack the cipher, significantly less than the 2^{128} to 2^{256} operations needed to try every combination.

Even if Courtois and Pieprzyk are correct, AES won't crumble overnight. The fastest computers can mount attacks of perhaps order 2^{70}, Burr says: "With 2^{100}, we might not be able to verify the attack for the next 70 years, maybe more." Still, he says, a theoretically sound attack would be a "very, very disturbing proposition," because attacks get refined over time and computers are speeding up exponentially.

Some analysts think there's nothing to fret about. Don Coppersmith, a cryptographer at IBM in Yorktown, New York, and one of the designers of DES, claims to have found a flaw in the analysis: Courtois and Pieprzyk miscounted the number of equations, he believes. But Courtois says the criticism does not apply to the latest version of the paper, which will be presented in December at the Asiacrypt 2002 conference.

Barring an obvious mathematical error, though, it might take cryptographers years to determine whether the attack is worrisome. The only way to prove that the algorithm works, Courtois says, is to use it to crack AES—and computers aren't up to the job yet. Meanwhile, says Bruce Schneier, a Minnesota-based cryptographer at security company Counterpane Systems, computer-security experts have no way of knowing which attacks pose true threats and which are phantoms. "How could you do particle physics if you couldn't do experiments?" he asks. "We've entered an era of cryptanalysis where you can't verify attacks."



Scrambled. Simplifying the math behind AES might leave the encryption algorithm vulnerable to attack.

–CHARLES SEIFE