none of the samples could leave China until a new contract was signed between the relevant U.S. and Chinese institutions. "He was on the [National Geographic Society] grant," protests Lucas, "and he had told us several times that we could take the samples home. But he said the grant was only a personal agreement between us and him, not a research contract."

At that point, Lucas says he even began to fear for his safety. "We had $10,000 in drilling equipment in a remote area within a closed region of China," he recalls. "We wondered if we might suddenly disappear." After Lucas contacted U.S. embassy officials, Cheng announced the fieldwork was being terminated early. Further talks in Beijing failed to resolve the issue, and on 10 September the team flew home.

Chinese officials and researchers paint a very different picture of the events. "The failure of the field investigation ... was the result of Dr. Lucas's lack of understanding of China's principles and policies governing international cooperation," says CAGS vice president Zhao. Cheng offers a similar description in a report on the incident he wrote for CAGS, which runs Cheng's institute. Explaining why his collaborators were not allowed to take specimens out of China, Cheng wrote: "The two sides must first sign a cooperative research agreement which has been approved by the appropriate Chinese authorities so that a cooperative research program can be established between the two sides. This is the only legal way that the specimens can leave China." Such an agreement, the U.S. scientists learned later, could involve a continuing relationship with Cheng and Li at a cost of up to half a million dollars.

Back in New Mexico, Lucas is still angry about what happened. "I paid to bring Cheng to the United States in 1993," says Lucas, who has made several successful trips to China since 1980. "I have a Chinese graduate student, and I've collaborated with Chinese scientists in the past. This is the first time anything like this had ever happened to me." He pauses, then adds, "I'm done with China. I'm pulling up my stakes. It's too risky."

Indeed, Lucas and his colleagues are so upset that they have proposed to colleagues that the IUGS, the discipline's governing body, withhold its approval for any geological activity in Xinjiang. They also want a moratorium on consideration of the Jimusar site and a half dozen other locations in China that IUGS is reviewing as model sites until the Chinese government can promise that all qualified scientists will be granted free and open access to such areas.

Their concerns have drawn some sympathy from other geologists. "Of course, there have been many positive experiences [by foreign researchers in China], but this is not an isolated case," says Jurgen Remane, a professor of paleontology at the University of Neuchatel, Switzerland, who chairs the International Commission on Stratigraphy, which reviews sites proposed as model locations. "[The Chinese] have tried to extort money from these scientists, and they need to make substantial concessions to put the matter right," he says.

At the same time, Remane believes a moratorium on reviewing candidate sites in China may be going too far. "It would be a pity to have a good site turned down for political reasons," he says, adding his panel should stick to scientific matters. That's also how the Chinese feel. "To withdraw support for the Dalongkou section and to recommend a reconsideration of all other proposed sites in China [would be] a loss to the international geological community," says Zhao. "We welcome cooperation with foreign countries on the basis of equality and mutual benefit and respect."

Several Earth scientists with extensive experience in China say that this incident points to the need for Western scientists to be wary of potential snafus when working in China. Unexpected demands can arise, they say, because of increasing economic pressure on scientific institutions to become self-sufficient, a growth in local political autonomy, and language barriers. "The dollar price of doing business in China has gone up in a hurry," says paleontologist Chris Maples of the Kansas Geological Survey, who has made three trips to China since 1991. Maples also notes that the team was working in a region far from the capital where local authorities, who also belong to a minority ethnic group, are much less likely to accede to orders from Beijing.

Others note that researchers also need to be sensitive to cultural differences. "It's easy for a U.S. scientist to feel he was ripped off when he's not allowed to do what he wanted to do and he doesn't understand the reasons why," says Steve Graham, a Stanford University geologist who has worked for 15 years in the region on joint projects with a variety of Chinese geological agencies. "It's not enough to know the facts. You also need to know the context." Indeed, to Graham, the incident is a reminder that foreign researchers must do their homework before working in China. "It's caveat emptor," he says. "That's something business leaders have known for a long time, and that scientists are just beginning to learn."

–Jeffrey Mervis

CRYPTOGRAPHY

New Attacks Breach Computer Codes

"It's the Titanic Effect," says Richard Lipton, a computer scientist at Princeton University. Lately, the seas have been full of icebergs for the computer security systems that lock up messages in supposedly unreadable code. And like the "unsinkable" Titanic, the systems have taken on a lot of water. In the past year, a security consultant found a sneaky way to read "secure" public-key messages, and Lipton and a team of scientists from Bellcore showed how to unravel entire public-key encryption systems. Now, Adi Shamir, an eminent cryptographer at the Weizmann Institute in Israel, has cracked tough secret-key systems, including the Data Encryption Standard (DES) widely used in credit card verification and automated teller machines.

"It's a new paradigm. There's going to be more of this in the future."
–Richard Lipton

Underlying the spate of attacks is a new strategy for cracking security codes. Instead of dwelling in the abstract realm of pure mathematics, cryptanalysts have begun to crack codes based on observing how imperfect computers implement the systems in the real world. "It's a new paradigm," says Lipton. "There's going to be more of this in the future." Even though many of the attacks aren't practical for the average hacker, "it's a matter of recognizing vulnerability," says Richard DeMillo, a member of the Bellcore group.

It all started last December when Paul Kocher, a computer-security consultant based in California, opened a breach in public-key cryptography, a scheme in which one party (conventionally called Bob) can send a secure message to a target (Alice), even if Bob and Alice have never met to exchange a key. This method relies upon mathematical functions that are easy to do but very hard to undo: multiplying two numbers versus factoring the product, for example. The function acts like a mailbox; you can put a message in, but you can't take it out. The public key is like the address on the mailbox; by publishing it, a business can enable clients it has never contacted before to send it secure information. The business retains a second, private key, which opens the mailbox.

Instead of trying to steal that second key

by unraveling the hard-to-undo functions, Kocher made an end run around the mathematics. By timing how long it takes for a computer to decipher something, Kocher was able to figure out what the message was. In effect, rather than trying to crack the combination lock on the mailbox, Kocher watched the user open the box and figured out the combination by seeing how long it takes to spin the dials.

Kocher's attack, which could be staged over the World Wide Web, is easy to block by a technique called blinding, which mathematically masks the time it takes to perform the decryption. But it demonstrated the power of a strategy that Bruce Schneier, author of *Applied Cryptography*, refers to as a systemic attack: "You look at the device as an organism. You ask, how does it breathe? You listen to its timing, to its radiation, to its power supply," says Schneier. "More intense is poking it, whacking it, hitting it to see how it fails. You can learn a lot about a machine by how it fails," he adds.

The Bellcore scientists took the strategy a step farther by doing just that. In August, Lipton realized that if he could make a computer or encoding chip err in its calculations while encrypting a message, he could make it leak information about the message being encrypted. One way to do this would be to irradiate it, which might flip a bit in its memory. By comparing a number of error-ridden encryptions with a single flawless one, Lipton and his colleagues found that they can crack virtually all public-key systems.

"Every one we could think of, we can break," says Lipton. Even RSA, an extremely popular public-key scheme, fell prey to the attack. It also worked on the codes that protect smartcards—the computer-chip–encrusted credit cards that can carry information like medical records or bank account balances. Though the requirement for a sample of error-ridden encryptions limits the scheme's practicality, a determined hacker could use it—if the stakes were high enough.

The most recent blow came on 18 October, when Shamir (the "S" in RSA) and Eli Biham, a computer scientist also at Weizmann, revealed in an Internet message that they had extended Bellcore's attack. Shamir wrote that his approach can crack "almost any secret-key cryptosystem proposed so far in the open literature," including the DES.

Secret-key cryptosystems are more traditional—and hardier—than their public-key cousins. A single key that Bob and Alice have exchanged in advance serves for encoding and decoding messages, and the secrecy of the key—not some undoable mathematical function—is what guarantees the security of the messages. These schemes are particularly useful for exchanging information between "friendly" machines like military radios or bank computers. And because changing a private key is quite a hassle, requiring all friendly machines to be reset, private keys stay unchanged for a long time. Designers of secret-key systems go to great lengths to protect the secret key from hackers.

But Shamir's attack was able to uncover the secret key from a 56-bit DES algorithm with little trouble by irradiating the chip that implements it and then performing "differential fault analysis," a more intricate version of the Bellcore technique. Even when DES was run three times over to encode the messages, Shamir's strategy was still able to ferret out the key.

All this does not mean that cryptography is unsafe. "Personally, I don't have a problem with safety," says DeMillo. Though a skilled burglar can pick almost any lock, it doesn't mean that locks are worthless. In the same way, even vulnerable cryptosystems add a layer of security. But designers of cryptographic systems have lost some of their hubris. "Just as there's no unsinkable ship," muses Lipton, "there's no unbreakable cryptosystem."

–Charles Seife

Charles Seife is a science writer in Scarsdale, New York.

SCIENCE AND RELIGION

The Vatican's Position Evolves

When Pope John Paul issued a statement last week backing the theory of evolution, newspapers in both the United States and Europe reacted with front-page headlines. The pope's pronouncement didn't come as a revelation to Catholic scholars, however. The statement, made at the annual meeting of the Pontifical Academy of Sciences in Rome, says that "new knowledge leads us to recognize in the theory of evolution more than a hypothesis." But the Vatican had already taken a big step in support of Darwin in a 1950 encyclical, *Humani Generis*, which deemed evolution a "serious hypothesis" worthy of more investigation. Says theologian John F. Haught of Georgetown University, "This Pope has in other communications previously expressed his sense of the compatibility of evolution and Catholic theism."

LES MOORE/UNIPHOTO

Papal blessing. Theory of evolution endorsed.

The statement has symbolic significance, however, and Italians made much of it. "Pope says we may descend from monkeys," hooted the conservative newspaper *Il Giornale*, according to a Reuters dispatch. For their part, many Italian scientists welcomed the Pope's move. Astrophysicist Margherita Hack of the Astronomical Observatory of Trieste told *Science*, "It is the first time that the Church formally accepts the evolutionary hypothesis as proven theory." Molecular biologist Giorgio Tecce of Rome University calls it part of "a process of rethinking the relationship between the Church and scientific developments" that has been going on for the past several years. Philosophy professor Giulio Giorello of the University of Milan says, "It will allow Darwinism to be studied, not as a hypothesis, but as a real scientific truth, which will allow discussions on crucial issues such as bioethics."

The Pope's endorsement of evolution probably will not have much impact on the curriculum of Catholic schools, which have long taught that the theory of evolution need not conflict with Church dogma.

The announcement isn't likely to affect the Church's position on sensitive issues such as fetal research or abortion either. The Vatican has made it abundantly clear that however the human body evolved, the human spirit belongs to God, and a person as a spiritual, moral, and legal entity begins at conception. The Pope's recent statement says: "If the human body has its origin in living material which preexists it, the spiritual soul is immediately created by God." This distinction also was spelled out earlier this year by the Italian National Bioethics Committee, which is dominated by Catholics (*Science*, 12 July 1996, p. 177).

Some observers believe the Pope's pronouncement could take a little wind out of the sails of creationists in the United States. But efforts to weaken the teaching of evolution in the schools are unlikely to be blunted, says Molleen Matsumura of the National Center for Science Education in El Cerrito, California. The statement might straighten out some members of the public who assume that because the church opposes abortion it espouses creationism. But, Matsumura predicts, "creationists are not going to be changed by it."

–Constance Holden

With reporting by Susan Biggin in Venice.