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."

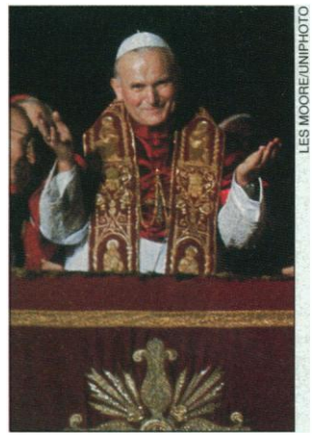
–Charles Seife

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 pre-exists 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.