be repeating itself—as unlikely as that may seem—because, with the expected increased precision measurements to come from the SLC, LEP, and the Tevatron proton-antiproton collider in the next few years, there could be compelling evidence for the low-mass Higgs boson (at least one) even before the Large Hadron Collider begins operation.

Although the comment attributed to Alvaro de Rújula at CERN about possible technical problems with muon collider machines may be true, the Higgs boson is the "crown jewel" in the electroweak theory, and a strong effort to study this particle in detail on a collider seems justified. This aspect of the muon collider is not in competition with the next linear collider (NLC) electron-positron studies around the world.

David B. Cline
Department of Physics and Astronomy, University of California, Los Angeles, CA 90024, USA
dcline@physics.ucla.edu

References

1. See collection of papers in *Nucl. Instrum. Methods* **A350** (1994), pp. 24–56; D. B. Cline, Ed., *Am. Inst. Phys. Conf. Proc.* **352** (1996); *Nucl. Phys. B (PS)* **51A** (1996).

Cracking the Codes

While a crystal ball may seem like an outmoded form of technology these days, it was more accurate than *Science* gives it credit for in foretelling major breaches in computer security for 1997 (Scorecard '96, 19 Dec., p. 2041). As was widely reported in the news, computer scientists cracked four critical encryption standards in 1997. A graduate student at the University of California, Berkeley, using a network of 250 workstations, cracked a message encrypted with a 40-bit key in less than 4 hours. The next level of protection, 48 bits, took 13 days to crack by a Swiss-led team of researchers using 3500 personal computers (PCs) spread across Europe.

The most significant encryption standard to fall in 1997 was the government's own 56-bit Data Encryption Standard (DES) algorithm, which has been extensively studied since its publication and is considered to be the world's best known and most widely used secret-key cipher. It took a team of university students, programmers, and scientists 140 days, using thousands of PCs through the Internet, to crack a message encrypted with DES. Most recently, an effort comprising over 4000 teams and tens of thousands of computers processed 72 quadrillion possible keys to decode a message encrypted with the RC5 algorithm and a 56-bit key.

Even though these standards were brought down in response to the RSA Data Security Secret-Key Challenge (*1*), their significance for the security of data encrypted with any of them should not be underestimated. Encryption key sizes up to 56-bits, the only ones currently exportable from the United States without a license, were cracked by researchers armed only with their wits and Internet-accessible PCs. These examples demonstrate both the vulnerability of our most relied upon encryption standards for the near future and the antiquated state of the government's current cryptographic policies.

Alexander Fowler
Scientific Freedom, Responsibility, and Law Program, American Association for the Advancement of Science 1200 New York Avenue, NW, Washington, DC 20005, USA
E-mail: afowler@aaas.org
Web: www.aaas.org/spp/dspp/sfrl/sfrl.htm

References

1. www.rsa.com/rsalabs/97challenge