rily rain-fed agriculture, we see in the final quarter of the third millennium B.C. an increase in settlement numbers and the growth of a town at Tell Sweyhat. In moister areas near Kurban Hoyuk in southern Turkey, growth in rural sedentary settlements was at the expense of towns. As Frank Hole states ("Wheat domestication," Letters, 16 Jan., p. 303), something was going on at this time, but whether it was culturally or climatically driven, or a combination of both, is unclear (*4*). A case for increased atmospheric moisture in the mid-Holocene can be made from lake sediments and alluvial sediments (*5*). The former record suggests that there was dwindling but fluctuating moisture toward the end of the third millennium B.C., followed by greater drying in the later second millennium B.C., when settlement in northern Mesopotamia did indeed decline, but did not disappear. Although I, too, accept a role for climate, especially in these fragile, highly stressed semiarid agricultural systems, archaeological evidence suggests that not only was settlement decline in one part of this zone counteracted by increases in other areas, but also that there were adjustments within both pastoral and sedentary communities that could absorb some of the stress of climatic shocks.

Tony Wilkinson
Oriental Institute,
University of Chicago,
Chicago, IL 60637, USA
E-mail: t-wilkinson@uchicago.edu

References

1. F. Sirocko, *Paleoecol. Africa* **24**, 65 (1996).
2. N. Roberts and H. E. Wright, in *Global Climates Since the Last Glacial Maximum*, H. E. Wright *et al.* Eds. (Univ. of Minnesota Press, Minneapolis, MN, 1993), pp. 194–220.
3. T. J. Wilkinson, *Geoarchaeology* **12**, 853 (1997).
4. K. Butzer, in *Third Millennium B.C. Climate Change and Old World Collapse*, H. N. Dalfes, G. Kukla, H. Weiss, Eds. (NATO ASI Series, Springer, Berlin, 1997), pp. 245–296.
5. G. Lemcke and M. Sturm, in *ibid.*, pp. 653–678; A. M. Rosen, *Geoarchaeology* **12**, 395 (1997).

■

Gentlemen of Science

In a Special News Report, Jon Cohen describes "Scientists who fund themselves" (9 Jan., p. 178). I would like to add the names of my mentor J. B. S. Haldane (1892–1964) and his father J. S. Haldane (1860–1936). The younger Haldane, in particular, exemplified the amateurish tradition by making significant contributions to genetics, physiology, biochemistry, and biometry, while possessing no academic qualification in any branch of science (*1*). Both Haldanes funded their own research as well as that of their students from their own pockets whenever they could.

Much of our research did not require expensive facilities, but we needed support for salaries, travel, and other expenses to attend scientific meetings, which was partially provided by Haldane. He even edited his own journal, the *Journal of Genetics*, which bypassed the usual peer-review system, but Haldane privately arranged for us to obtain the comments of distinguished colleagues before he accepted a paper for publication. His father, Oxford physiologist J. S. Haldane, built his own laboratory on the ground floor of his sprawling house in Oxford ("Cherwell"), complete with an airtight chamber with a sealable door and observation window. Both father and son conducted physiological experiments, in which they were their own "guinea pigs," that were often painful and involved the testing of the effects of various gaseous mixtures, atmospheric pressures, and temperatures.

Krishna R. Dronamraju
Foundation for Genetic Research,
Post Office Box 27701–0,
Houston, TX 77227, USA

References

1. *Haldane and Modern Biolology*, K. R. Dronamraju, Ed. (Johns Hopkins Univ. Press, Baltimore, MD, 1968).

■

Muon Collider Studies

The article "Physicists dream of a muon shot" by Alexander Hellemans (News, 9 Jan., p. 169) gives a useful account of the 4th International Conference on Muon Colliders (San Francisco, December 1997), which I, with the assistance of others on the program committee, organized.

The concept of a Higgs factory muon collider (*1*) arose (and the name was coined, as I recall) at our first conference in 1992 in Napa, California, but it had little scientific support at that time.

At the 1997 conference, however, there were reports about four independent studies of the parameters of the electroweak theory that suggest the existence of a low-mass Higgs scalar particle (below 200 gigavolts). This is precisely the mass range in which a Higgs factory is designed to operate and that is expected by supersymmetry.

A similar situation happened with the Z particle. Before the Z particle was discovered in 1983 at the European Organization for Nuclear Research (CERN), the mass was known well enough to start the design of the Large Electron-Positron Accelerator (LEP, a Z factory) machine at CERN and the Stanford Linear Collider (SLC). History may

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