Letters to the Editor

Misleading Mathematicians

In his article "Encryption and the NSA Role in International Standards" (February 2015 *Notices*) Dr. Michael Wertheimer works hard to leave the impression that the NSA did not place a backdoor in the DUAL_EC_DRBG algorithm. He never issues a direct denial, and indeed doing so would be difficult, in view of the overwhelming evidence of the backdoor. Instead, he misleads through selective omission of evidence, including evidence that:

- the NSA considered it a "challenge in finesse" (tinyurl.com/n5aqlzh) to get the standard accepted
- the NSA paid a leading industry player a large sum to make this standard (with NSA's curve points) the default option (tinyurl.com/qc6c8qq)
- the NSA suppressed discussion of how the curve points should be generated (tinyurl.com/oaaava7), and
- the standard makes no mathematical sense unless you were designing it for the backdoor.

The NSA needs to address the actual question of the backdoor, or provide an explanation of why it will not.

Dr. Wertheimer is rightly concerned that this incident may lead people to believe that "NSA has a broader agenda to 'undermine Internet encryption,'" and asks for a "fair reading of our track record." This track record includes reducing the key length of the block cipher DES in the 1970s to make it breakable (tinyurl.com/lsfbszt), blacklisting an inventor of DES (Horst Feistel) from cryptography jobs (tinyurl.com/psqbsez), advocating for control of cryptographic research in the 1980s, and, according to NSA's 2013 budget request (tinyurl.com/n5aqlzh), covertly influencing "commercial products' designs" and "policies, standards and specifications for commercial public key technologies" for the purposes of exploitation. Indeed, the track record speaks for itself.

Dr. Wertheimer writes that he feels "a connection to the mathematics community that goes beyond scholarship." If so, his attempt to mislead this community—the community that "encouraged and supported his studies"—is even more shameful.

A slightly different version of this letter is posted on the web at www.cs.bu.edu/~reyzin/wertheimer-letter.html, with thirty signatories.

—Matthew Green
Johns Hopkins University

—Ethan Heilman
Boston University

—Bruce Schneier, Fellow
Berkman Center for Internet and Society
Harvard Law School

(Received February 9, 2015)

Getting it Right and the Shapes of India's Zero

After reading the excellent review of Mazur's book *Enlightening Symbols* (*Notices*, February 2015), I ordered it. I would have liked the book more than I did if the author's information on India had been better.

William Jones (p. 84) was the mathematician-father of the philologist-son Sir William Jones (a judge in India).

Brahmagupta's birthplace (now Bhinmal) is in Gujarat, not south India (regarded the "linguistic south").

Like the *Iliad*, the *Vedas* (all of *Rig Veda*'s 10,500 hymns) were an oral (not written, p. 35) composition, beginning about 3,000 years ago, in archaic, accented Sanskrit (now termed Vedic), and written down long after writing had evolved. Eventually, Vedic morphed into accent-less (classical) Sanskrit (the book's "Sanskrit"), still studied in India and elsewhere.

The relationship between present-day Devnagari (now just Nagari) and the extinct Brahmi script(s) (lasting for about a thousand years) baffles the author. Consulting Jensen's *Sign, Symbol and Script* and Coulmas's *The Writing Systems of the World* might help. All present-day Indian scripts have descended from some Brahmi version, which was then discarded and forgotten.

In Brahmi, the Anuswaara, a dot placed to a letter's right, imparted to it a terminal "um" sound. To secure this sound, this dot was placed above the letter for Indo-European scripts. But in the Dravidian Old-Kannada script (derived from an earlier northern Brahmi), so as not to puncture the palm leaf (the writing materials used being palm leaf and steel stylus), a small circle, instead, was placed to the letter's right. (It is still so in Modern Kannada.) I believe this was how the "dot" and "small circle" representing the Indian "zero" originated.

The present-day Hindu numerals come from Brahmi numerals. Nagari "4" is Brahmi "ma", closely resembling Brahmi "4". More could be said.

People always mention the scarcity of "hard" evidence regarding earlier Indian numerals. Could this be due to the five-century-long razing in North India of Hindu, Buddhist, and Jain temples that fell before the iconic fury of the pseudo-Islamic conquerors who demolished them wherever found? Who knows what Babylonian, Greek, Hindu, and Islamic accomplishments were lost when the pseudo-Muslim Genghis Khan invaded Mesopotamia?

Also, why couldn't the place-value notation (of which a place-holder zero is a sine qua non) have come to India from Mesopotamia? The lion-headed eagle, Imdugud (first depicted during Ur's Third Dynasty), after becoming double-headed (as seen in the thirteenth century BCE meeting of the supreme Hittite gods, Yazilikaya) did get around to several countries including India.

—Padmini Joshi
Professor Emerita
Ball State University
Muncie, Indiana

(Received February 19, 2015)