I was shocked and dismayed that the AMS agreed to publish Neal Koblitz's recent article ["The Uneasy Relationship Between Mathematics and Cryptography", September 2007] without, apparently, any editorial oversight. As one who works in the field of 'provable security', I vehemently disagree with most of Koblitz's points — more on this below — but this is not my primary complaint. Instead, what I found most abhorrent about the article is that it crosses the line from reasoned academic argument to personal screed, from constructive criticism to belligerent name-calling. I cannot imagine the Notices publishing a similarly disparaging article about any other academic discipline, let alone one so closely allied with mathematics.

By yet another fault of the editors, readers were not given the opportunity to read a companion article containing a countervailing point of view. Without dissecting Koblitz's arguments point-by-point (which I will be happy to do upon request of the editors), let me assure those readers that proofs in modern cryptography are as meaningful as proofs in any other area of mathematics. Can a scheme that has been proven secure still succumb to a real-world attack? Yes, but this does not invalidate the proof. (A proof of security is always given with respect to a particular definition of security; a given definition is not necessarily appropriate for all possible environments in which a scheme may be deployed.) Are most (but not all!) results in cryptography conditional? Yes, but this has also been shown to be inherent until the P vs. NP question (one of the seven "Millennium Problems" of the Clay Mathematics Institute) is settled. Do mistakes happen? Occasionally, and with more frequency then we might like. But this surely does not eradicate the importance of having proofs in the first place.

Frankly, I have never been able to understand why any mathematician would discourage the use of precise definitions, rigorous proofs, and formal reasoning in any field. (Introduction of these elements in cryptography helped the field progress from an art to a science, and also played a large role in the real-world success that cryptography has enjoyed.) Koblitz's article clarifies his motivation: sheer elitism. According to Koblitz, cryptographers generally publish papers of "little originality" and containing "tiny improvements"; when we do publish something of potential interest, it is just as likely to be wrong. According to Koblitz, apparently, cryptographers (in contrast to trained mathematicians) are simply incapable of writing correct proofs; hence his admonition that cryptographers simply give up on the goal rather than focus on better quality control. This is snobbery at its purest.

Publication of Koblitz's article has the real potential to cause serious damage: not to cryptography — which will do just fine with or without Koblitz's support — but to the future involvement of mathematicians in the field of cryptography. In the future, the editors should more carefully weight the pros and cons of publishing 'contributions' of this nature.

Jonathan Katz
University of Maryland
jkatz@cs.umd.edu