1026-94-3 **Neal Koblitz*** (koblitz@math.washington.edu), University of Washington, Department of Mathematics, Box 354350, Seattle, WA 98195-4350. *Stormy Marriage – A Periodization of the History of the Relationship between Mathematics and Cryptography.*

Most applications of mathematics to cryptography are relatively recent. Since the 1980's concepts from number theory and algebraic geometry have been applied to the study of elliptic and hyperelliptic cryptosystems, the number field sieve for factoring, pairing-based cryptosystems, and other topics. In the 1990's some mathematicians tried, with varying degrees of success, to use a connection (real or imagined) with cryptography to get more support and funding. Often their claims of cryptographic relevance were viewed as far-fetched by people who actually work in cryptography. Analogously, many researchers in cryptography started to use mathematical formalism as a way to establish the reliability of their protocols. However, the reliance on the theorem-proof paradigm of mathematics to give assurances of security has raised some tricky questions and some suspicions that math is being misused. I will give some examples that illustrate the need for skepticism about "provable security." I will also make some comments about the sociology of cryptographic research in comparison with the traditions and culture of mathematical research. (Received February 10, 2007)