The Strange Relation of Mathematics to Cryptography

Professor Neal Koblitz
University of Washington

Starting in 1984, when Hendrik Lenstra introduced his elliptic curve factoring algorithm, the level of sophistication of the mathematics used in cryptography has risen dramatically. Many concepts from number theory and algebraic geometry have been applied to the study of elliptic and hyperelliptic curve cryptosystems, the number field sieve method for factoring, and other topics.

More recently, though, mathematics has been used to give formal assurances of security, and this has raised some difficult questions and some suspicions that math is being misused. I will discuss the controversy surrounding “provable security” and give some examples that illustrate the need for caution and skepticism.

Neal Koblitz received his Ph.D. in mathematics at Princeton in 1974 with a thesis on arithmetic algebraic geometry. Since 1979 he has been at the University of Washington in Seattle. In 1985 he was co-inventor of Elliptic Curve Cryptography. Since then his research interests have centered around applications of number theory in cryptography. He has written five books, dealing with p-adic analysis, elliptic curves, modular forms, and cryptography.

Neal’s main nonmathematical activity is assisting his wife Ann in running the Kovalevskia Fund for women in science in developing countries, of which she is Director. In addition, he is chair of the mathematical sciences subcommittee of the U.S. Committee for Scientific Cooperation with Vietnam. In these connections he travels extensively, and uses the opportunity to give demonstration math classes and talk with school teachers in various parts of the world.