Web address: **http://www.sciencedaily.com/releases/2007/08/070807172333.htm**

ScienceDaily
Your source for the latest research news

Source: American Mathematical Society
Date: August 8, 2007

Keywords: Mathematics, Math Puzzles, Hacking, Information Technology, Mathematical Modeling, Computer Modeling

Math Plus Cryptography Equals Drama And Conflict

Science Daily — Cryptography is just about as old as written communication itself, and mathematics has long supplied methods for the cryptographic toolbox.

Starting in the 1970s, increasingly sophisticated mathematics began to make inroads into cryptography, changing the nature of the field and bringing new perspectives on what it means to keep communications secure.

Neal Koblitz is a mathematician who, starting in the 1980s, became fascinated by mathematical questions in cryptography. In his article "The Uneasy Relationship Between Mathematics and Cryptography", to appear in the September 2007 issue of the Notices of the AMS, Koblitz recalls some of the drama and conflict that he witnessed while doing research in mathematical cryptography in the past two decades. His article discusses how mathematics has been used in cryptography research and also comments on the cultural aspects of the mixing of the two fields.

Just before Koblitz got interested in cryptography, the National Security Agency had carried out a heavy-handed but ultimately unsuccessful attempt to restrict open research in the field. As a result, research in cryptography carried a whiff of "forbidden fruit", and the launching of a series of cryptography conferences in the 1980s became an act of defiance. As Koblitz describes, the conferences were dominated by colorful, iconoclastic figures, and the corporate influence was much less than it is today.

It was around that time that Koblitz and others originated a new approach to cryptography called "elliptic curve cryptography", or ECC. The approach uses elliptic curves, which are planar curves that have special properties and are central to modern number theory (elliptic curves played a key role, for example, in Andrew Wiles's proof of Fermat's Last Theorem).

Commercial systems using ECC were developed and marketed by a company now called Certicom Corporation. Koblitz describes the development of ECC and the ways that elliptic and other curves have been used in cryptography. He also talks about an algorithm called "xedni calculus" ("xedni" is "index" spelled backwards) that seemed initially to provide a way to crack ECC systems, but ultimately proved to be an ingenious but impractically slow method of attack.

The mixture of mathematics and cryptography is a heady one, as it brings abstract research at the frontiers of mathematics to bear on difficult and fascinating questions where the answers can have a big impact on the outside world. Koblitz describes two pernicious effects of this mixing of the two fields. One he calls the "bandwagon effect", in which mathematicians have distorted their research grant proposals in an effort to appeal to funding entities like the National Security Agency.

The other is the effort by various cryptographers to add an aura of reliability to their cryptographic systems by claiming the systems are "provably" secure---that is, by claiming there exists an ironclad mathematical proof of the system's security. Koblitz and a colleague have written several papers critiquing claims of "provable security", and he describes the heated and sometimes bizarre reactions that greeted their critique.

Koblitz's article "The Uneasy Relationship Between Mathematics and Cryptography" will appear on the Notices website.

Note: This story has been adapted from a news release issued by American Mathematical Society.