

# Mathematics and Computer Science

## Cryptography

### Devising a Better Way to Teach and Learn the Advanced Encryption Standard

Cryptographic systems are hard to understand, and that is their point—otherwise hackers would be clearing out bank accounts at will.

*Here is a pedagogical nightmare: How does one describe, explain, and teach the workings of a cryptographic algorithm that was deliberately designed to befuddle would-be code-breakers? Recently, two Santa Clara undergraduates and their math professor developed a much needed approach for introducing an important new encryption standard to students.*



In the world of cryptography, a term like “secure” is relative, and it is easy to see why. When the U.S. National Bureau of Standards developed the first Data Encryption Standard (DES) in the 1970s, it would have taken a lifetime to defeat it using the fastest computers available at that time. Today, with a specially designed supercomputer, an hour would suffice. Fortunately, during the 1990s a more robust cryptographic method called Triple DES was introduced to keep most of the world’s secrets secret. But now its days, too, are numbered.

The U.S. National Institute of Standards and Technology held a competition in 2001 for a new data security algorithm. The winning entry, dubbed the Advanced Encryption Standard (AES), came from a Belgian professor and graduate student. AES is still in the first stages of deployment, but it is proving so hard to defeat that it should serve us well through many generations of ever-speedier new computers.

#### Tougher to Crack, Tougher to Teach

The trouble is, like DES before it, AES is not very easy to explain, or to teach. It is not inordinately complicated, but like many algorithms, it would be best understood if a student could work through an example by hand—and with AES that just is not feasible. Greatly needed was a simpli-

fied version that could be used in traditional teaching and learning environments.

Santa Clara University Associate Professor of Mathematics and Computer Science Ed Schaefer specializes in the field of arithmetic geometry, but he has also earned recognition for work in cryptography. A few years ago a leading data security firm, RSA, hired him to try to crack a new data encryption technique based on elliptic curves. Arithmetic geometry includes the study of elliptic curves—and Schaefer happens to be one of the world’s foremost experts in them. Try as he might, he failed (as others have, since) to defeat elliptic curve codes. The failure had value, however, as it served to increase the perception of elliptic curve cryptography security.

Before the RSA project, Schaefer had become known in cryptography circles for a simplified version of DES that he had developed and described in a 1996 paper. Presented in several textbooks, it is regarded as an effective way to teach the notoriously complicated algorithm to students.

One professor, who uses simplified DES in his own courses, wrote to Schaefer to ask if he had any plans to simplify AES as well. Schaefer did not at the time, but it got him thinking. Then one day Mohammad Musa and Stephen Wedig—two juniors taking Schaefer’s popular introductory cryptography course—walked into his

office and proposed working together on a research project of his choosing. Schaefer had just the thing in mind.

#### The Perfect Team

“The paper that we wrote actually turns out to be more than just a simplified version of AES,” Schaefer says. “We also explain two different attacks against AES that the algorithm was designed to withstand. That makes the attacks, too, much more understandable. Students get to work through examples by hand, and by the end of the paper, they understand why AES is designed as it is.”

Schaefer, Musa, and Wedig all worked together on the paper in what Schaefer describes as a “true collaboration.” Schaefer understood the mathematics and the pedagogical issues, and had the experience of writing papers for publication. But oddly enough, especially for a science professor in Silicon Valley, he’s a self-described technophobe who has never

desired to own either a home computer or a cell phone. (He uses computers, but at work only—and as for telephones, he gets by just fine with a plain land-line.)

By contrast, Schaefer describes Musa and Wedig—computer engineering and computer science majors, respectively—as hardware and software experts. “They’re enormously knowledgeable, much more so than typical undergraduates,” Schaefer says. “They contributed a real depth of background on computers and technology implementation issues that I simply didn’t possess.”

The paper, titled “A Simplified AES Algorithm and Its Linear and Differential Cryptanalyses,” appeared in April 2003 in *Cryptologia*, a well-regarded journal in the field. If it is half as successful as Schaefer’s earlier paper on DES, it should prove to be a feather in the caps of his two undergraduate students as they start their professional careers.

“In order for a computer security system to be considered safe, it must be understood by a large number of scientists. The more scientists who understand it and can not find a weakness, the greater the perceived security.”

Edward F. Schaefer

*associate professor of mathematics and computer science*



Mohammad Musa  
Edward Schaefer