Rivest, Shamir, and Adleman Receive 2002 Turing Award

Ronald L. Rivest   Adi Shamir   Leonard M. Adleman

The Association for Computing Machinery (ACM) has named RONALD L. RIVEST, ADI SHAMIR, and LEONARD M. ADLEMAN as winners of the 2002 A. M. Turing Award, considered the "Nobel Prize of Computing", for their contributions to public key cryptography. The Turing Award carries a $100,000 prize, with funding provided by Intel Corporation.

As researchers at the Massachusetts Institute of Technology in 1977, the team developed the RSA code, which has become the foundation for an entire generation of technology security products. It has also inspired important work in both theoretical computer science and mathematics. RSA is an algorithm—named for Rivest, Shamir, and Adleman—that uses number theory to provide a pragmatic approach to secure transactions. It is today's most widely used encryption method, with applications in Internet browsers and servers, electronic transactions in the credit card industry, and products providing email services.

Rivest is the Viterbi Professor of Computer Science in MIT's Department of Electrical Engineering and Computer Science. He is a founder of MIT's Cryptography and Information Security Group. He received a B.A. in mathematics from Yale University and a Ph.D. in computer science from Stanford University.

Shamir is the Borman Professor in the Applied Mathematics Department of the Weizmann Institute of Science in Israel. He received a B.S. in mathematics from Tel Aviv University and a Ph.D. in computer science from the Weizmann Institute.

Adleman is the Distinguished Henry Salvatori Professor of Computer Science and Professor of Molecular Biology at the University of Southern California. He earned a B.S. in mathematics at the University of California, Berkeley, and a Ph.D. in computer science, also at Berkeley.

The ACM presented the Turing Award on June 7, 2003, in conjunction with the Federated Computing Research Conference in San Diego, California. The award was named for Alan M. Turing, the British mathematician who articulated the mathematical foundation and limits of computing and who was a key contributor to the Allied cryptanalysis of the German Enigma cipher during World War II. Since its inception in 1966, the ACM's Turing Award has honored the computer scientists and engineers who created the systems and underlying theoretical foundations that have propelled the information technology industry.

—*From an ACM news release*