FOR IMMEDIATE RELEASE:
Aug. 9, 1999

Philip Bulman
(301) 975-5661
philip.bulman@nist.gov

G 99-111

NIST Announces Encryption Standard Finalists

You can think of it as the Olympics of information scrambling.

One of the most important competitions in the history of cryptography—and for the future support of secure electronic commerce—entered a new phase today when the Commerce Department's National Institute of Standards and Technology named a handful of finalists in the drive to develop the Advanced Encryption Standard. The AES will be a strong data scrambling formula for protecting the electronic data flow of the 21st century.

Secretary of Commerce William Daley hailed today's announcement as a significant step toward creating a more secure digital economy.

"This is a critical milestone in developing the Advanced Encryption Standard. The AES will serve as an important security tool in support of the dynamic growth of electronic commerce," Daley said.

A year ago, researchers from 12 different countries submitted 15 candidates for the AES—the new encoding method that eventually will be adopted by the federal government. Since that time, cryptographers have tried to find ways to "attack" the different encoding methods, looking for weaknesses that would compromise the encrypted information. Today's decision narrows the field of contenders from 15 candidates to only five.

The five finalists are sophisticated mathematical formulas, called algorithms, which are at the heart of computerized encryption systems. Encryption systems encode everything from electronic mail to the secret personal identification numbers, or PINs, that people use with bank teller machines.

-more-

The AES will be a public algorithm designed to protect sensitive government information well into the next century. It will replace the aging Data Encryption Standard, which NIST adopted in 1977 as a Federal Information Processing Standard used by federal agencies to encrypt information. DES is used widely in the private sector as well, especially in the financial services industry.

NIST's Information Technology Laboratory chose the following five contenders as finalists for the AES:

- MARS—developed by International Business Machines Corp. of Armonk, N.Y.;
- RC6™—developed by RSA Laboratories of Bedford, Mass.;
- Rijndael—developed by Joan Daemen and Vincent Rijmen of Belgium;
- Serpent—developed by Ross Anderson, Eli Biham and Lars Knudsen of the United Kingdom, Israel and Norway respectively; and
- Twofish—developed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall and Niels Ferguson. (Many members of this group are associated with Counterpane Systems of Minneapolis).

No significant security vulnerabilities were found for the five finalists during the initial analysis of the algorithms, and each candidate offers technology that is potentially superior for the protection of sensitive information well into the 21st century.

NIST requested proposals for the AES on Sept. 12, 1997. Each of the candidate algorithms supports cryptographic key sizes of 128, 192 and 256 bits. At a 128 bit key size, there are approximately 340,000,000,000,000,000,000,000,000,000,000,000,000 (340 followed by 36 zeroes) possible keys.

The global cryptographic community has been helping NIST in the AES development process by studying the candidates. NIST used feedback from these analyses and its own assessments to select the finalists. The studies evaluated security and how fast the algorithms could encrypt and decrypt information. The algorithms were tested on everything from large computers to smart cards.

During the evaluation process NIST considered all comments, papers, verbal comments at conferences, reports and proposed modifications, and its own test data. Each candidate algorithm was discussed relative to the announced evaluation criteria and other pertinent criteria suggested during the public analysis. A detailed report on the process, "Status Report on the First Round of the Development of the Advanced Encryption Standard," is available on the AES web site at www.nist.gov/aes.

NIST is making the five finalists available for intensified study and analysis by cryptographers, the public, industry and academia. Analysis of the finalists will be presented at a conference in April 2000. NIST is accepting comments on the candidates through May 15, 2000. Then it will review the comments and draft the proposed AES (incorporating one or more of the algorithms) for public comment. If all goes as planned, the standard should be completed by the summer of 2001.

As a non-regulatory agency of the U.S. Department of Commerce's Technology Administration, NIST strengthens the U.S. economy and improves the quality of life by working with industry to develop and apply technology, measurements and standards through four partnerships: the Measurement and Standards Laboratories, the Advanced Technology Program, the Manufacturing Extension Partnership and the Baldrige National Quality Program.

For more information about NIST, see our web site at www.nist.gov.