August 1999

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

THE ADVANCED ENCRYPTION STANDARD: A STATUS REPORT

NIST's Information Technology Laboratory is working with industry and the cryptographic community to develop an Advanced Encryption Standard (AES). The goal is to develop a Federal Information Processing Standard (FIPS) that specifies an encryption algorithm(s) capable of protecting sensitive (unclassified) government information well into the next century. The algorithm(s) is expected to be used by the U.S. Government and, on a voluntary basis, by the private sector. This ITL Bulletin gives a status report on the development of the AES, summarizes the evaluation process, and briefly describes the five finalist algorithms selected in Round 1 of the AES development process.

Background

On January 2, 1997, NIST announced the initiation of an effort to develop the AES and made a formal call for algorithms on September 12, 1997. The call stipulated that the AES must specify an unclassified, publicly disclosed encryption algorithm(s), available royalty-free, worldwide. In addition, the algorithm(s) would implement symmetric key cryptography as a block cipher and (at a minimum) support a block size of 128-bits and key sizes of 128-, 192-, and 256-bits.

On August 20, 1998, NIST announced its acceptance of fifteen AES candidate algorithms at the First AES Candidate Conference (AES1). These algorithms had been submitted by members of the cryptographic community from around the world. At that conference and in a published *Federal Register* notice, NIST solicited public comments on the candidates. A Second AES Candidate Conference (AES2) was held in March 1999 to discuss the results of the analysis conducted by the global cryptographic community on the candidate algorithms. The public comment period on the initial review of the algorithms closed on April 15, 1999.

Evaluation Criteria

In the call for candidate algorithms, NIST specified the evaluation criteria that would be used to compare the candidate algorithms. These criteria were developed from public comments to the proposed criteria and from the discussions at a public AES workshop held on April 15, 1997, at NIST. The evaluation criteria are divided into three major categories: Security, Cost, and Algorithm and Implementation Characteristics.

Security is the most important factor in the evaluation. Security encompasses features such as resistance of the algorithm to cryptanalysis, soundness of its mathematical basis, randomness of the algorithm output, and relative security as compared to other candidates.

Cost is a second important area of evaluation that encompasses licensing requirements, computational efficiency (speed) on various platforms, and memory requirements. Since one of NIST's goals is that the final AES algorithm(s) be available worldwide on a royalty-free basis, intellectual property claims and potential conflicts must be consid-

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and address to this office.

Bulletins issued since March 1998

- ❒ *Management of Risks in Information Systems: Practices of Successful Organizations*, March 1998
- ❒ *Training Requirements for Information Technology Security: An Introduction to Results-Based Learning*, April 1998
- ❒ *A Comparison of Year 2000 Solutions*, May 1998
- ❒ *Training for Information Technology Security: Evaluating the Effectiveness of Results-based Learning*, June 1998
- ❒ *Cryptography Standards and Infrastructures for the Twenty-first Century*, September 1998
- ❒ *Common Criteria: Launching the International Standard*, November 1998
- ❒ *What Is Year 2000 Compliance?*, December 1998
- ❒ *Secure Web-based Access to High Performance Computing Resources*, January 1999
- ❒ *Enhancements to Data Encryption and Digital Signature Federal Standards*, February 1999
- ❒ *Measurement and Standards for Computational Science and Engineering*, March 1999
- ❒ *Guide for Developing Security Plans for Information Technology Systems*, April 1999
- ❒ *Computer Attacks: What They Are and How to Defend Against Them*, May 1999

ered in the selection process. The speed of the algorithms on a variety of platforms must also be considered. During Round 1, the focus was primarily on the speed associated with 128-bit keys. Additionally, memory requirements and constraints for software implementations of the candidates are important considerations.

The third area of evaluation is *algorithm and implementation characteristics* such as flexibility, hardware and software suitability, and algorithm simplicity. Flexibility includes the ability of an algorithm:

- to handle key and block sizes beyond the minimum that must be supported,
- to be implemented securely and efficiently in many different types of environments, and
- to be implemented as a stream cipher, hashing algorithm, and to provide additional cryptographic services.

It must be feasible to implement an algorithm in both hardware and software, and efficient firmware implementations are advantageous. The relative simplicity of an algorithm's design is also an evaluation factor.

Results from Round 1

The Round 1 public review extended from the official announcement of the fifteen AES candidates on August 20, 1998, at AES1 until the official close of the comment period on April 15, 1999. During Round 1, many members of the global cryptographic community supported the AES development effort by analyzing and testing the fifteen AES candidates.

NIST facilitated and focused the discussion of the candidate algorithms by providing an electronic discussion forum that was used to comment on the candidates, discuss relevant AES issues, inform the public of new analysis results, etc. This discussion forum is located at **http://aes.nist.gov**. The AES home page **http://www.nist.gov/aes** has served as a tool to disseminate information such as papers for AES2 and other Round 1 public comments.

Twenty-eight papers were submitted to NIST for consideration for AES2. Twenty-one of those papers were presented at AES2 as part of the formal program, and several of the remaining seven were also presented during an informal session at that conference. All of the submitted papers were posted on the AES home page several weeks prior to AES2 in order to promote informed discussions at the conference.

AES2 gave members of the global cryptographic community a chance to present and discuss the analysis that had been performed on the AES candidates during Round 1, as well as other important topics relevant to the AES development effort. In addition to the AES2 papers, NIST received fifty-six sets of public comments on the candidate algorithms during Round 1. All of these comments were made publicly available on the AES home page on April 19, 1999.

NIST performed an analysis of mathematically optimized ANSI C and Java™ implementations[*] of the candidate algorithms that were provided by the submitters prior to the beginning of Round 1. Additionally, NIST performed extensive statistical testing on all of the candidates. The testing of ANSI C implementations focused on the speed of all fifteen candidates on various desktop systems, using different combinations of processors, operating systems, and compilers. The submitters' Java™ code was tested for speed and memory usage on a desktop system, and other features of the code were measured as well. Statistical testing was performed on all fifteen candidates to determine if the algorithms generate output that is statistically indistinguishable from truly random data. Testing results are available on the AES home page.

Selection Process Prior to Round 2

At the conclusion of the Round 1 public review, NIST established an AES technical review team to recommend algorithms for Round 2 evaluations. The team was composed of NIST employees who had been engaged in reviewing the algorithms, reviewing the public comments on the candidates, selecting papers for AES2, conducting NIST's efficiency and randomness testing, attending and presenting information at the AES conferences, and managing the AES development process. The team met several times over the course of two months to develop their consensus position.

During the evaluation process, the NIST team considered all comments, papers, verbal comments at conferences, NIST studies, reports, and proposed modifications. The team discussed each candidate relative to the announced evaluation criteria and other pertinent criteria suggested during the public analysis.

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message to listproc@nist.gov with the message **subscribe itl-bulletin**, and your proper name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

[*] Certain commercial equipment, instruments or materials are identified in this paper to foster understanding. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the materials or the equipment identified is necessarily the best available for the purpose.

The review of each algorithm included a methodical evaluation of the following factors:

- security (including any known attacks or weaknesses),
- efficiency (both speed and memory usage),
- flexibility (implementation on low- and high-end smart cards; support of additional key and block sizes, including whether the reference code actually supported the additional key sizes; suitability for use as a pseudo-random number generator, hashing algorithm, etc.; and whether or not encryption and decryption were the same procedure),
- algorithm simplicity, and
- other issues that were discussed in the received public comments.

Although it was considered, the team readily agreed that it was not possible to conduct a quantitatively based selection of the finalists. For example, comments were not received regarding the security analysis of some candidates, whereas other algorithms were reported as "broken." Since security is considered the most important evaluation criteria, the AES review team made a first cut of the candidates based on security, then proceeded with the other selection criteria. This evaluation process resulted in the team selection of five candidates with superior characteristics as finalists for Round 2 evaluation.

It is important to note that the selection of an algorithm as a finalist does not constitute endorsement by NIST of the algorithm or its security. Similarly, the non-selection of an algorithm is not necessarily to be taken as a statement about the algorithm's quality, security, efficiency, or other characteristics.

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today.

Round 2 AES Finalists

Using the analyses and comments received, NIST selected five finalist algorithms: **MARS**, **RC6™**, **Rijndael**, **Serpent,** and **Twofish**. No significant security vulnerabilities were found for these candidates during the Round 1 analysis, and each of these algorithms constitutes potentially superior technology. Below is a summary of each of the finalist candidates in alphabetical order. Profiles and overall assessments for all fifteen Round 1 candidates can be found in the NIST Round 1 Report (from which this summary is extracted), which is available on the AES home page.

MARS incorporates its "cryptographic core" into an innovative, heterogeneous overall structure. It also features a variety of operations, including the technique of rotating digits by a varying number of places that is determined by both the data and the secret key. Consequently, while MARS performs well in general, it performs particularly well on computer platforms that support its rotation and multiplication operations efficiently. NIST accepted a modification to MARS for Round 2 (proposed by the submitter) that should improve its ability and flexibility to function in some memory-constrained environments, such as low-end smart cards. MARS was submitted to the AES development effort by the International Business Machines Corporation.

RC6 is an algorithm that is simple enough to memorize and should be easy to implement compactly in both software and hardware. Its simplicity also should facilitate its further security analysis in Round 2, which is assisted by the analysis of its predecessor, RC5. RC6 does not use substitution tables; instead, the principal engine for its security is the technique of rotating digits by a varying number of places that is determined by the data. In general, RC6 is fast and it is particularly fast on platforms that support its rotation and multiplication operations efficiently; its key setup is also fast. RC6 was submitted to the AES development effort by RSA Laboratories.

Rijndael performs excellently across all considered platforms. Its key setup is fast and its memory requirements are low, so it also should perform well in hardware and in memory-constrained environments. The straightforward design and the conservative choice of operations should facilitate its further analysis, and the operations should be relatively easy to defend against certain attacks on physical implementations. Even though parallel processing was not considered during the Round 1 selection process by the AES review team, Rijndael has the potential of benefiting from advances in computer processors that allow many instructions to be executed in parallel. Rijndael was submitted to the AES development effort by Joan Daemen and Vincent Rijmen.

Serpent is ultra-conservative in its security margin; the designers chose to use twice as many iterations as they believed secure against currently known attacks. Consequently, Serpent's performance is relatively slow compared to the other four finalists. In some settings, however, this should be mitigated by the efficiency of optimized implementations using what the submitters call the "bitslice" mode, for which the algorithm was specially designed. Serpent should fit well in hardware (with potential tradeoffs of speed versus space) and in memory-constrained environments. The straightforward design and the conservative choice of operations should facilitate further analysis of this candidate, and the operations should be easy to defend against certain attacks on physical implementations. Serpent was submitted to the AES development effort by Ross Anderson, Eli Biham, and Lars Knudsen.

Twofish exhibits fast and versatile performance across most platforms; it also should perform well both in hardware and in memory-constrained environments. It features variable substitution “tables” that depend on the secret key. The submitters believe that such tables generally offer greater security than tables with fixed values. The possibility of pre-computing these tables to varying degrees helps Twofish offer a wide variety of performance tradeoffs. Depending on the setting, Twofish can be optimized for speed, key setup, memory, code size in software, or space in hardware. Twofish was submitted to the AES development effort by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson.

Next Steps

With the announcement of the finalists, NIST formally opens the "Round 2" public evaluation process and solicits comments on the remaining algorithms through May 15, 2000. Comments can be submitted via the AES home page. NIST actively seeks comments and analysis on any aspect of the candidate algorithms, including but not limited to the following topics:

- cryptanalysis,
- intellectual property,
- crosscutting analyses of all of the AES finalists,
- selection and use of multiple AES algorithms,
- overall recommendations, and
- implementation issues.

NIST is providing an opportunity for the sponsors of the AES finalists to revise the ANSI C and Java™ implementations of their algorithms. NIST intends to make these implementations available (via CD-ROM) within two months of the beginning of Round 2.

Near the end of Round 2, NIST will sponsor the Third AES Candidate Conference (AES3), an open, public forum for discussion of the analyses of the AES finalists. Submitters of the AES finalists will be invited to attend and engage in discussions regarding comments on their algorithms. AES3 will be held April 13-14, 2000, in New York, New York. Registration and logistical information will be posted on the AES home page. Proposed papers for this conference are due to NIST by January 15, 2000.

Following the close of the Round 2 public analysis period on May 15, 2000, NIST intends to study all available information and propose the AES, which will incorporate one or more AES algorithms selected from the finalists. The AES will be announced as a proposed Federal Information Processing Standard (FIPS) that will be published for public review and comment. Following the comment period, the standard will be revised, as appropriate, by NIST in response to those comments. A review, approval, and promulgation process will then follow. If all steps of the AES development process proceed as planned, it is anticipated that the standard will be completed by the summer of 2001.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900

Official Business
Penalty for Private Use $300
Address Service Requested