Status of the Advanced Encryption Standard (AES) Development Effort

James Foti *
National Institute of Standards and Technology

Keywords: AES, Advanced Encryption Standard, cryptography, encryption.

[Due to the evolving nature of the AES development effort, this paper does not contain the complete information that will be presented at NISSC 1999. During the spring, NIST has been considering public comments and analysis, and during the summer NIST will be making the selection of the AES candidate algorithm finalists. Although this paper does not include many specifics, it presents some general topics that can be elaborated upon in greater detail at NISSC 1999.]

Introduction

The purpose of this presentation is to articulate the status of NIST's Advanced Encryption Standard (AES) development effort. This presentation will include a description of the overall AES development effort, a summary of comments and analysis from the first round of analysis (Round 1), and a discussion of the rationale for NIST's selection of the AES candidate algorithm finalists. Additionally, the author will present some of the analysis activities planned for the second round of evaluation and analysis (Round 2).

In January 1997, NIST announced its intention to develop a Federal Information Processing Standard (FIPS) for an Advanced Encryption Standard (AES). The culmination of this multi-year, multi-stage effort will be a FIPS specifying an Advanced Encryption Algorithm (AEA) - an unclassified, symmetric, block-cipher algorithm accommodating multiple key sizes, which is intended to be available royalty-free worldwide. NIST and the public have completed their first round of evaluation of the fifteen candidate algorithms for security, efficiency, and other properties. At the time of NISSC 1999, the finalist algorithms (approximately five) will be undergoing their second round of evaluation and analysis by NIST and the global cryptographic community.

Background

For over twenty years, NIST's Data Encryption Standard (DES) has been the Federal Government's standard for encrypting unclassified information. In addition, it has gained wide acceptance in the private sector and is found in countless Internet and banking applications. The DES algorithm has evolved from a U.S. Government algorithm into one that is used globally. Consequently, in the spirit of DES's success, NIST's goal in the AES development effort is to

* NIST, 100 Bureau Drive, STOP 8930, Gaithersburg, MD 20899-8930, U.S.A. Email: jfoti@nist.gov

specify an algorithm that will 1) have a usable lifetime of at least thirty years, 2) be available royalty-free worldwide, and 3) be used extensively throughout the U.S. Government and private sectors.

Recognizing the need to transition to a new algorithm, NIST began the AES development effort in early 1997 by proposing some basic criteria that candidate algorithms would have to meet, in addition to required elements in the nomination packages to be submitted to NIST. In response to an official call for comments on the proposed criteria and requirements, over thirty sets of comments were submitted to NIST, from U.S. Government agencies, vendors, academia, international interests, and individuals. Additionally, NIST sponsored an AES workshop on April 15, 1997 to discuss the comments and obtain additional feedback, to better define the request for candidate algorithms.

In the September 12, 1997 Federal Register, NIST announced its "Request for Candidate Algorithm Nominations for the Advanced Encryption Standard (AES)" [AESFR97]. This request solicited candidate algorithms during a nine-month submission period. All algorithm submissions had to meet the following *minimum acceptability criteria*:

- Symmetric (secret-key) algorithm
- Block cipher
- Support key sizes of 128, 192, and 256 bits, and a block size of 128 bits.

NIST required the submitted algorithm packages to meet numerous additional requirements, including the submission of reference and optimized algorithm code, complete algorithm specifications, and statements regarding security, efficiency, and flexibility. All requirements were detailed in [AESFR97].

Twenty-one submission packages were sent to NIST, and a subsequent review of the packages yielded fifteen that met the specified minimum criteria and requirements.

First AES Candidate Conference (AES1)

On August 20-22, 1998, NIST sponsored the First AES Candidate Conference (AES1) in Ventura, California to announce the fifteen AES candidate algorithms. There were five U.S.-based and ten international submissions. The submitters ranged from large computer and computer security corporations to smaller, lesser-known organizations; from groups of collaborating academicians to single individuals; and from world-renowned to up-and-coming cryptographers. See Table 1 for a complete list of the algorithms and their submitters.

Submitters presented an overview of their candidate algorithms and fielded questions from the two hundred attendees. The conference was intended to familiarize participants in the analysis and evaluation process with the various candidate algorithms, and begin the Round 1 Evaluation and Analysis period.

Algorithms	Submitters	Countries
CAST-256	Entrust Technologies, Inc.	Canada
CRYPTON	Future Systems, Inc.	South Korea
DEAL	Richard Outerbridge, Lars Knudsen	Canada, Norway
DFC	CNRS - Centre National pour la Recherche Scientifique – Ecole Normale Supérieure	France
E2	NTT – Nippon Telegraph and Telephone Corporation	Japan
FROG	TecApro Internacional S.A.	Costa Rica
HPC	Richard Schroeppel	U.S.A.
LOKI97	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry	Australia
MAGENTA	Deutsche Telekom AG	Germany
MARS	IBM	U.S.A.
RC6	RSA Laboratories	U.S.A.
Rijndael	Joan Daemen, Vincent Rijmen	Belgium
SAFER+	Cylink Corporation	U.S.A.
Serpent	Ross Anderson, Eli Biham, Lars Knudsen	U.K., Israel, Norway
Twofish	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson	U.S.A.

Table 1: AES Candidate Algorithms

To facilitate Round 1 analysis, at AES1 NIST distributed CD-ROMs containing all of the algorithm documentation provided by the submitters. To date, these CD-ROMs have been distributed to over 1000 people around the world. A second CD-ROM has also been distributed (subject to export controls), which contains algorithm code provided by the submitters.

Round 1 Evaluation and Analysis

After AES1, NIST formally began the Round 1 evaluation and analysis period by publishing another Federal Register announcement [AESFR98]. This announcement asked for general public comments on the algorithms, and called for papers for the Second AES Conference (AES2), held in the spring of 1999. The official comment period for Round 1 closed on April 15, 1999.

In [AESFR97] and [AESFR98], NIST listed various characteristics that will be taken into consideration during the evaluation and analysis process (during both Round 1 and Round 2):

- *SECURITY*: Each algorithm will be judged on factors such as 1) actual security vs. claimed security, 2) indistinguishability of ciphertext from random data, and 3) soundness of the algorithm's mathematical basis.

- *COST*: Cost will cover an algorithm's computational efficiency, memory requirements, and licensing requirements, among other factors.

- *ALGORITHM-SPECIFIC CHARACTERISTICS*: The flexibility of an algorithm - how well it can be implemented in a variety of environments, whether it can be used as hashing algorithm, etc. - will be considered. Also, hardware and software suitability will be evaluated, and the algorithm's relative simplicity ("elegance") will also be judged.

NIST does not intend to perform its own cryptanalysis, but rather "it will review the public evaluations of the candidate algorithms' cryptographic strengths and weaknesses." [AESFR97] In fact, public cryptanalysis of the algorithms began even *prior* to AES1 because most submitters had already publicly announced their algorithms. Two papers, which would later be submitted as Round 1 public comments, described weaknesses in LOKI97 and FROG, respectively. One discussed several high-probability differential characteristics in the round function of LOKI97, and its susceptibility to a linear attack; the second paper described differential and linear attacks (for FROG), which for a small class of keys, recover the keys significantly more quickly than with brute force. At AES1, after hearing the presentation for MAGENTA, six of the conference attendees collaborated to cryptanalyze MAGENTA: they identified several significant attacks based on the symmetry of that algorithm's subkeys.

The cryptographic research community and industry produced additional cryptanalysis papers during Round 1, which propose possible attacks on other algorithms. The above attacks were publicly presented at AES2 in Rome, Italy, on March 22-23, 1999. In total, twenty-one papers were presented at AES2, which discussed security strengths and weaknesses of the algorithms, efficiency on various platforms, potential for use on future platforms, etc.

NIST focused its own Round 1 evaluation efforts on the following properties of the candidate algorithms:

- Efficiency (speed) of the algorithms' optimized C code on multiple platforms (Pentium Pro, Pentium II, Sun™, and SGI), using different compilers (Borland C++ 5.0, Microsoft Visual C++ 6.0, DJGPP 2.01, etc.);

- Efficiency (speed) and use of memory of the optimized Java™ implementations; and

- Statistical randomness of output from the algorithms.

During Round 1, NIST's testing concentrated on the algorithms' performance using the 128-bit key size. At a minimum, efficiency testing will include the measurement of 1) algorithm setup, 2) key setup, 3) key change, and 4) the encryption and decryption of data.

In addition to the above information (public cryptanalysis and NIST testing), NIST received numerous official comments regarding algorithm efficiency when coded in different languages (C, Assembly, etc.) on various platforms (8-bit smartcards, 32- and 64-bit processors, and parallelized computers). The public also commented on intellectual property concerns, the

selection process for the Round 2 finalist algorithms, and other important issues of the AES Development Effort. (The author will be able to present an overview of these various results and comments at NISSC 1999.) In total, fifty-six sets of public comments were received by NIST during Round 1, and these were made available at the AES home page [AESHome] immediately after the close of the comment period.

Round 2 Evaluation and Analysis

During the summer of 1999, NIST will announce approximately five candidate algorithms that will be further evaluated and analyzed in Round 2. This round will last approximately nine months (or longer, if necessary), during which the global cryptographic community will be intensely focusing its analysis efforts on these finalists. NIST will concentrate its efficiency analysis efforts on the algorithms' 192- and 256-bit key sizes. The National Security Agency (NSA) has agreed to perform a hardware efficiency analysis of these finalists, by implementing them in a Hardware Description Language [NSA].

In March/April 2000, NIST will sponsor the Third AES Candidate Conference (AES3), which will be similar to AES2. NIST will use the information from this conference to make a final decision and select one or more algorithms for inclusion in the Draft AES. During Round 1, NIST received numerous comments that it should consider including *multiple* algorithms in the AES FIPS, as opposed to a *single* algorithm. In [AESFR97], NIST stated that it would consider the possibility of including multiple algorithms. NIST expects that this issue will receive considerable attention during Round 2.

Upon the approval of an AES FIPS by the Secretary of Commerce, NIST intends to have a validation program in place, to test AES implementations for conformance to the FIPS. Currently, NIST estimates that the AES FIPS and validation program should be available sometime in the year 2001.

Conclusion

The AES development effort is one of the most ambitious and significant efforts that NIST's Computer Security Division has undertaken in recent years. This effort is likely to have a widespread domestic and international impact for many years to come. By relying on public candidate algorithm submissions, soliciting public evaluation of those algorithms, and sharing its own analysis results with the public, NIST hopes that the algorithm(s) for the AES FIPS will have a high degree of public confidence from the very beginning. At the time of NISSC 1999, the author will be prepared to present an overview of Round 1 evaluations and analysis and discuss NIST's selection of the Round 2 finalists. NIST is proceeding relatively rapidly but also prudently, so that within the next two years, U.S. Government agencies and others will have a newer, stronger, and more efficient security technology available to protect sensitive information for the next several decades.

Up-to-date information on the AES Development Effort may be found at [AESHome].

References

[AESFR97] "Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard (AES)", Federal Register, Volume 62, Number 177, September 12, 1997. Pp. 48051-48058.

[AESFR98] "Request for Comments on Candidate Algorithms for the Advanced Encryption Standard (AES)", Federal Register, Volume 63, Number 177, September 14, 1998. Pp. 49091-49093.

[AESHome] AES home page, http://www.nist.gov/aes.

[NSA] "Initial Plans for Estimating the Hardware Performance of AES Submissions", National Security Agency,http://csrc.nist.gov/encryption/aes/round2/nsahardware-aes.pdf, May 1998.