NISSC 1998

Status of the Advanced Encryption Standard (AES) Development Effort

July 6, 1998

Abstract: The purpose of this presentation will be to articulate the status of NIST's Advanced Encryption Standard (AES) development effort. This will include a description of the overall AES development effort, the identification of the candidate algorithms, initial observations of the various algorithms, a discussion of some of the challenges facing NIST, and a highlight of the next steps in the process.

Author: Jim Foti
Organization: NIST
Security Technology Group
Bldg. 820, Room 417
Gaithersburg, MD 20899
Phone: (301) 975-5237
FAX: (301) 948-1233
E-mail: jfoti@nist.gov

Status of the Advanced Encryption Standard (AES) Development Effort

Jim Foti, NIST

July 6, 1998

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 1998. Between July and October, NIST will learn what the official AES candidate algorithms will be, NIST will hold the First AES Candidate Conference, and the evaluation/analysis process of candidate algorithms will begin. Although this paper cannot include many specifics, it presents some general ideas that can be elaborated upon in greater detail at NISSC 1998.]

Introduction

The purpose of this presentation will be to articulate the status of NIST's Advanced Encryption Standard (AES) development effort. This will include a description of the overall AES development effort, the identification of the candidate algorithms, initial observations of the various algorithms, a discussion of some of the challenges facing NIST, and a highlight of the next steps in the process.

In January 1997, NIST announced its intentions to develop a Federal Information Processing Standard (FIPS) for an Advanced Encryption Standard (AES). The culmination of this multi-year 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 is currently soliciting candidate algorithms from the public at large, and at the time of NISSC 1998, the submitted algorithms will be undergoing the first round of evaluation and analysis by NIST and the general public.

For over twenty years, NIST's Data Encryption Standard (DES) has been the Federal Government's standard method for encrypting unclassified information. In addition, it has gained wide acceptance in the private sector, and is found in countless banking applications. The algorithm specified in the DES standard has evolved from a U.S. Government algorithm into one that is used globally. Consequently, in the spirit of the Data Encryption Standard's success, NIST's goal in the AES development effort is to specify an algorithm that will have a usable lifetime of at least thirty years, and which will also be used extensively throughout the U.S. Government and private sectors.

Request for Candidate Algorithms for the AES

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 packages to be submitted to NIST. Over thirty sets of comments were received, encompassing U.S. Government agencies, vendors, academia, international interests, and individuals. Additionally, NIST sponsored an AES workshop on April 15, 1997 to discuss the comments received and obtain additional feedback, to better define the request for candidate algorithms.

On September 12, 1997, the Federal Register announced NIST's "Request for Candidate Algorithm Nominations for the Advanced Encryption Standard (AES)" [AESFR]. This request solicited candidate algorithms during a fixed submission period, ending on June 15, 1998. In order for a submitted algorithm to be deemed "proper", it must meet certain *minimum acceptability criteria*:

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

In addition, the request specified other information that must be contained in a submission package for it to be deemed "complete". Some of those *submission requirements* are listed here:

1) Complete written specification of the algorithm,
2) Statements of the algorithm's estimated computational efficiency,
3) Known answer test values for the algorithm, and code to generate those values,
4) Statement of the algorithm's expected cryptographic strength,
5) Analysis of the algorithm with respect to known attacks,
6) Statement of advantages and limitations of the algorithm,
7) Reference implementation of the algorithm, specified in ANSI C,
8) Optimized implementations specified in Java and ANSI C,
9) Signed statements that address any applicable patents, and that allow for the algorithm to be used on a worldwide, non-exclusive, royalty-free basis if it is selected for inclusion in the standard, and
10) No proprietary or classified information.

NIST must then review each submission package in detail to determine if it is "complete and proper". It is intended that NIST will then announce all of the submitted candidate algorithms - even including those determined not to be "complete and proper". This announcement will occur in a Federal Register notice and at the First AES Candidate Conference.

First AES Candidate Conference

Two months after the close of the submission period, NIST will sponsor the First AES Candidate Conference in Ventura, California from August 20-22, 1998. Not only will NIST announce the various AES submitters and the "complete and proper" submissions, but the submitters will also be given an opportunity to present an overview of their candidate algorithms and answer questions from the attendees. The purpose of the conference is to help familiarize participants in the analysis and evaluation process with the various candidate algorithms. NIST anticipates that many of the cryptographers who will be attending the following week's Crypto '98 conference in Santa Barbara will be able to participate in the AES conference. Crypto is an annual conference sponsored by the International Association for Cryptologic Research (IACR). NIST hopes that many of IACR's members will assist the AES development effort by applying their expertise in cryptography to the analysis of the candidate algorithms.

At the AES conference, NIST will distribute AES Candidate Algorithm Analysis Packages to the attendees, so that they may begin Round 1 of the AES development effort's technical evaluation of the candidate algorithms. Additionally, NIST intends to present attendees with other information related to the Round 1 Technical Evaluation.

Initial Observations of AES Candidate Algorithms

[Since no algorithm submissions will be made public by NIST before the First AES Candidate Conference, there is currently no information for this section of the paper. However, some areas of discussion will include:

- announcement of the algorithms and their submitters,
- possible grouping of algorithms into families, based on obvious characteristics, and
- interesting features of the algorithms, based on information presented at the First AES Candidate Conference.

More detailed information will be available after August.]

The Road Ahead - The Analysis Process

Overall, the evaluation and analysis process of the AES candidate algorithms will last for at least one year - most likely longer. This process will be divided into two stages, or "Rounds" of evaluation and analysis, with the pool of candidates being narrowed down at the end of each Round.

As mentioned above, the First AES Candidate Conference will begin the Round 1 Technical Evaluation of the AES candidate algorithms. 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." [AESFR] Instead, NIST will focus its efforts on the analysis of the efficiency of each algorithm's mathematically optimized implementations. This testing will be done on both the ANSI C and Java optimized implementations, on a specific platform. During the Round 1 Technical Evaluation, NIST's testing will focus on the 128-bit key size, at a minimum measuring the time required to perform 1) Algorithm setup, 2) key setup, 3) key change, and 4) encryption and decryption of data.

After Round 1 is complete (approximately six months), NIST will hold a Second AES Candidate Conference, where all evaluation and analysis results (from both NIST and the public) can be presented and discussed. NIST also intends to invite advice on how the list of candidates can be narrowed.

After the conference, NIST will announce the remaining five (or fewer) candidate algorithms that will be further evaluated and analyzed in Round 2. This Round will last from six to nine months (or longer, if necessary), and NIST's efficiency analysis efforts will be focused on the 192- and 256-bit key sizes of the algorithms. NIST may also pursue having the remaining algorithms specified using a Hardware Description Language, "to compare the estimated hardware efficiency of the candidate algorithms". [AESFR]

At the conclusion of Round 2, NIST will sponsor the Third AES Candidate Conference, which will be similar to the second conference. However, NIST will use the information from this conference to make a final decision and select a single algorithm for inclusion in the Draft AES. Upon the approval of an AES FIPS by the Secretary of Commerce, NIST plans to have a validation program for AES conformance testing in place.

***

In the request for candidate algorithms, NIST listed various characteristics that will be taken into consideration during the evaluation and analysis process:

- *SECURITY*: Each algorithm will be judged on factors such as 1) actual security vs. claimed security, 2) indistinguishability of ciphertext from random data, 3) soundness of the algorithm's mathematical basis, etc.
- *COST*: Cost will cover an algorithm's licensing requirements, computational efficiency, and memory 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.

[At NISSC '98, NIST may be able to present some of the preliminary evaluation and analysis results - both its own results and those that the public will have submitted. However, these will be presented in a brief, general manner, and the audience will be directed to look for more detailed information at the AES homepage, http://www.nist.gov/aes.]

Challenges Facing NIST

During the first part of the AES development effort, NIST encountered some challenges as it defined the submission and analysis process, in addition to requirements for the candidate algorithms. NIST also expects other challenges to arise as it continues this effort. Some of these encountered and anticipated challenges are explained in this section.

First, writing the Federal Register notice announcing the request for candidate algorithms was a very challenging task. NIST had to consider over thirty sets of comments, plus input from the April 15, 1997 workshop. The comments often conflicted with one another. Many excellent ideas were presented to NIST, and three months were spent selecting what were thought to be the most appropriate criteria and writing the final announcement. NIST wanted to present a challenging - but not impossible - set of requirements, in order to improve the chances that the algorithms received would come from those submitters who were truly serious about the process. Also, NIST felt that the best approach was to specify the analysis and evaluation criteria in as much detail as possible, so that the submitters and others would understand what NIST anticipated doing.

Second, NIST wanted to select two APIs (one for ANSI C, another for Java) to which submitters' algorithm implementations must conform. This would enable NIST to develop only two test suites for the efficiency testing of all submitters' mathematically optimized implementations, rather than having to develop new code for each algorithm. Also, it would help other people and organizations to more easily perform their analysis of the algorithms. NIST had a multitude of APIs from which to choose, but settled on Sun's Java Development Kit (JDK) and Java Cryptography Extension (JCE). This enabled NIST to define specific calls with the appropriate underlying structure, based on a widely used and well-known API specification, for which documentation and a reference implementation were available. However, due to numerous complications with changing versions of the JDK and JCE, along with unanticipated availability problems, NIST decided to specify a simple Java API specifically for the AES submissions. NIST received invaluable assistance from Raif Naffah and the Cryptix Development Team to develop the API and provide submitters with an extremely useful toolkit for the Java portion of their submissions.

Third, NIST must abide by export controls regarding the distribution of AES Candidate Algorithm Analysis Packages, since these packages will contain cryptographic source code. In order to speed up the process of being able to export these packages to international evaluators, NIST worked with the Bureau of Export Administration (BXA) to develop a framework in which export licenses could be applied for and obtained well in advance of the official announcement of candidate algorithms. The goal of this was to be able to distribute the analysis packages to all requesting individuals, with as little delay as possible.

Fourth, NIST must prepare CDs containing the “complete and proper” candidate algorithms and all of the information related to them that was originally submitted to NIST. Some must be generated such that they do not contain code, and can be submitted in a general nature outside of the U.S. and Canada (but in a manner compliant with export controls on cryptography). NIST will have less than two months between the close of the submission period and the First AES Candidate Conference to prepare the AES Candidate Algorithm Analysis Packages.

Fifth, a major part of the selection process will be NIST analysis of the efficiency of the various algorithms. NIST must be very careful to perform testing consistently for each of the algorithms. This information will be made publicly available, and part of NIST's responsibility will be to facilitate the sharing of this information and the dissemination of the results of public evaluation and analysis.

Sixth, there is also the possibility that NIST will be presented with classified analysis results regarding the algorithms. How much that will affect the selection of the algorithms cannot be determined. However, NIST must take into account *all* of the analysis results that it receives and generates, in order to most responsibly select an algorithm that will have an exceptionally high chance of remaining secure and usable by the U.S. Government – and hopefully by many in the private sector - for thirty years.

Finally, the narrowing process at the end of Rounds 1 and 2, when the remaining candidates are reduced from approximately seventeen to five, and then from five to (ideally) one, will likely be difficult for NIST. However, by making analysis public, facilitating the sharing of evaluation information, and sponsoring two conferences to discuss evaluation and analysis results, the selection process will hopefully be less difficult than it otherwise could be.

Conclusion

The AES development effort is one of the most ambitious and significant efforts that NIST's Security Technology Group 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 and private candidate algorithm submissions, soliciting public evaluation of those algorithms, and sharing its own analysis results with the public, NIST hopes to settle on a single algorithm for the AES FIPS that will have a high degree of public confidence from the very beginning. NIST is proceeding carefully but relatively rapidly, so that U.S. Government agencies will soon have a newer, stronger, and more efficient security technology available for protecting unclassified information for the next thirty years.

References

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