Cryptographic Standards and Guidelines

AES Development

AES Overview | NIST Reports | Federal Register Notices | Rijndael Info | Related Publications

AES Overview

Beginning in 1997, NIST worked with industry and the cryptographic community to develop an Advanced Encryption Standard (AES). The overall goal was to develop a Federal Information Processing Standard (FIPS) specifying an encryption algorithm capable of protecting sensitive government information well into the 21st century. The algorithm was expected to be used by the U.S. Government and, on a voluntary basis, by the private sector.

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

On August 20, 1998, NIST announced a group 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 simultaneously-published Federal Register notice, NIST solicited public comments on the candidates ("Round 1"). 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. Using the analyses and Round 1 comments received, NIST selected five algorithms from the fifteen.

The AES finalist candidate algorithms were MARS, RC6, Rijndael, Serpent, and Twofish, and NIST developed a Round 1 Report describing the selection of the finalists.

These finalist algorithms received further analysis during a second, more in-depth review period ("Round 2") prior to the selection of the final algorithm(s) for the AES FIPS. Until May 15, 2000, NIST solicited public comments on the remaining algorithms. Comments and analysis were actively sought by NIST 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, overall recommendations and implementation issues. NIST received numerous Round 2 comments. An informal, online AES discussion forum was also provided by NIST for interested parties to discuss the AES finalists and relevant AES issues.

Near the end of Round 2, NIST sponsored the Third AES Candidate Conference (AES3) - an open, public forum for discussion of the analyses of the AES finalists. AES3 was held April 13-14, 2000 in New York, NY, USA. Submitters of the AES finalists were invited to attend and engage in discussions regarding comments on their algorithms. All papers proposed for AES3 were considered as official Round 2 public comments.

After the close of the Round 2 public analysis period on May 15, 2000, NIST studied all available information in order to make a selection for the AES. On October 2, 2000, NIST announced that it has selected Rijndael to propose for the AES. A report, press release, and AES fact sheet are available with that information.

After the announcement, NIST began preparing a draft Federal Information Processing Standard (FIPS) for the AES, which was published for public review and comment in February 2001. Following the 90-day comment period, the draft standard will be revised by NIST, as appropriate, in response to public comments. A review, approval, and promulgation process then followed.

The Advanced Encryption Standard (AES) was published as FIPS 197 on November 26, 2001. Validation testing for conformance of AES implementations to FIPS 197 then began under the Cryptographic Algorithm Validation Program (CAVP). As of 2020, more than 5700 AES algorithm implementations had been validated by CAVP as conforming to FIPS 197 specifications.

NIST Reports on AES Development

- *First Advanced Encryption Standard (AES) Candidate Conference* (Jan./Feb. 1999)
- *Second Advanced Encryption Standard (AES) Candidate Conference* (Jul./Aug. 1999)
- *Status Report on the First Round of the Development of the Advanced Encryption Standard* (Sep./Oct. 1999)
- *Third Advanced Encryption Standard Candidate Conference* (April 13-14, 2000) [AES3 Proceedings]
- *Report on the Development of the Advanced Encryption Standard (AES)* (May/June 2001)

Federal Register Notices

Jan. 2, 1997	Announcing Development of a FIPS for AES
Sep. 12, 1997	Requesting Candidate Algorithm Nominations for AES
Sep. 14, 1998	Request for Comments on Round 1 Candidates
Sep. 15, 1999	Request for Comments on Round 2 Candidates
Feb. 28, 2001	Request for Comments on Draft FIPS for AES
Dec. 6, 2001	Announcing FIPS 197 (AES)

Rijndael Information

- Specification (amended);
- Supporting Documentation (provided with original submission);
- Intellectual Property statements (original; Round 2 update);
- ANSI C Reference Code (DOS; UNIX);
- Test Values; and
- VHDL implementation, developed by NSA for each of the AES finalists, Aug. 7, 2000 (VHDL README file). NSA also provided NIST a report that was made public in May 2000, *Hardware Performance Simulations of Round 2 Advanced Encryption Standard Algorithms*.

Related NIST Publications

- *The Economic Impacts of the Advanced Encryption Standard, 1996-2017* (September 2018)
- *Development of the Advanced Encryption Standard* (August 2021)

The Internet Archive has an archive copy of NIST's AES Development site (as of December 18, 2001), including links to information on all candidate algorithms, public comments received, conference materials, etc.

Created December 29, 2016, Updated May 08, 2023

PROJECT LINKS
Overview
News & Updates
Publications
Presentations
ADDITIONAL PAGES
Example Values
Crypto-Enabled Applications
Withdrawn Crypto Standards
Archived Crypto Projects
AES Development

CONTACTS
Dr. Lily Chen
lily.chen@nist.gov

GROUP
Cryptographic Technology

RELATED PROJECTS
Block Cipher Techniques
Circuit Complexity
Computer Security Objects Register
Crypto Publication Review Project
Crypto Reading Club
Crypto Standards Development Process
Cryptographic Algorithm Validation Program
Digital Signatures
Elliptic Curve Cryptography
Hash Functions
Key Management
Lightweight Cryptography
Message Authentication Codes
Multi-Party Threshold Cryptography
Pairing-Based Cryptography
Post-Quantum Cryptography
Privacy-Enhancing Cryptography
Random Bit Generation