

ADVANCED ENCRYPTION STANDARD (AES) Questions and Answers

Background Information

1. What is the Advanced Encryption Standard (AES)?

The Advanced Encryption Standard (AES) is a Federal Information Processing Standard (FIPS), specifically, [FIPS Publication 197](#), that specifies a cryptographic algorithm for use by U.S. Government organizations to protect sensitive, unclassified information. NIST anticipates that the AES will be widely used on a voluntary basis by organizations, institutions, and individuals outside of the U.S. Government - and outside of the United States - in some cases.

2. What algorithm did NIST select for the AES, and how do you pronounce it?

NIST selected Rijndael as the AES algorithm. The algorithm's developers have suggested the following pronunciation alternatives: "Reign Dahl", "Rain Doll", and "Rhine Dahl".

3. Who submitted the algorithm, and where are they from?

The two researchers who developed and submitted Rijndael for the AES are both cryptographers from Belgium: Dr. Joan Daemen (Yo'-ahn Dah'-mun) of Proton World International and Dr. Vincent Rijmen (Rye'-mun), a postdoctoral researcher in the Electrical Engineering Department (ESAT) of Katholieke Universiteit Leuven. Both gentlemen have been very active in the cryptographic community.

4. Is there a document that provides details on NIST's selection for the AES?

NIST's *ad hoc* AES selection "team" wrote a [Report on the Development of the Advanced Encryption Standard \(AES\)](#). It is a comprehensive report that discusses various issues related to the AES, presents analysis and comments received during the public comment period, summarizes characteristics of the five finalist AES algorithms, compares and contrasts the finalists, and presents NIST's selection of Rijndael.

Complete AES-related information is available on the [AES home page](#). The site includes NIST's Report on the Development of the Advanced Encryption Standard (AES); Rijndael specifications, test values, and code; all public comments, including analysis papers from the various AES conferences; and other "historical" AES information.

5. Why is this approval of the AES FIPS significant?

This announcement marks the culmination of a four-year effort involving the cooperation between the U.S. Government, and private industry and academia from around the world to develop an encryption technique that has the potential to be used by millions of people in the years to come. NIST anticipates that this algorithm will be used widely - both domestically and internationally.

6. Is the AES now an official U.S. Government standard?

Yes. The Secretary of Commerce approved the adoption of the AES as an official Government standard, effective May 26, 2002.

NIST's Selection of the AES Algorithm

7. Why did NIST select Rijndael to propose for the AES?

When considered together, Rijndael's combination of security, performance, efficiency, ease of implementation and flexibility make it an appropriate selection for the AES.

Specifically, Rijndael appears to be consistently a very good performer in both hardware and software across a wide range of computing environments regardless of its use in feedback or non-feedback modes. Its key setup time is excellent, and its key agility is good. Rijndael's very low memory requirements make it very well suited for restricted-space environments, in which it also demonstrates excellent performance. Rijndael's operations are among the easiest to defend against power and timing attacks.

Additionally, it appears that some defense can be provided against such attacks without significantly impacting Rijndael's performance. Rijndael is designed with some flexibility in terms of block and key sizes, and the algorithm can accommodate alterations in the number of rounds, although these features would require further study and are not being considered at this time. Finally, Rijndael's internal round structure appears to have good potential to benefit from instruction-level parallelism.

8. What about the other four algorithms that were not selected?

In terms of security, NIST states in its report that "all five algorithms appear to have adequate security for the AES." NIST is not saying that there is anything "wrong" with any of the other four algorithms. However, when all of the analysis and comments were taken into consideration, the NIST team felt that Rijndael was the best selection for the AES.

9. Why did NIST select only one algorithm to propose for the AES?

NIST considered the possibility of selecting multiple algorithms for the AES, since that was a topic of discussion during the public evaluation periods. Many arguments were made both for and against the inclusion of multiple algorithms in the standard, and NIST's AES selection team considered those comments prior to evaluating the algorithms.

Briefly, NIST's AES selection team decided to select only one algorithm for several reasons. First, other FIPS-approved algorithms (e.g., Triple DES) offer a degree of systemic resiliency, should a problem arise with the AES. Second, multiple AES key sizes provide for increased levels of security. Third, a single algorithm AES will promote interoperability and decrease the complexity of implementations that will be built to comply with the AES specifications, hopefully promoting lower implementation costs than a multiple algorithm AES. Fourth, a single AES algorithm addresses vendors' concerns regarding potential intellectual property costs.

NIST's [report](#) offers more details.

10. Is NIST designating a backup algorithm?

No. Based on public comments and discussion, NIST's AES selection team decided not to designate a "backup" algorithm from among the other four finalists. Some vendors expressed concerns that a backup algorithm would become a *de facto* requirement in products (for immediate availability in the future), leading to higher implementation costs and a potential decrease in the interoperability of AES products. Also, given the uncertainty of the potential applicability of future breakthroughs in cryptanalysis, it would be unclear whether a designated backup would actually provide any resiliency for the main algorithm selection. Finally, NIST's AES selection team anticipated that other algorithms (whether specified in Government standards or not) will continue to be available in commercial products.

NIST's [report](#) offers more details.

11. How has the public been involved in the development of the AES?

From the beginning of the AES development effort, NIST has relied on the public's participation, including:

- a. assisting NIST in the design of submission requirements and evaluation criteria (including minimum key and block size requirements and intellectual property requirements);
- b. developing and submitting candidate algorithms;
- c. analyzing the candidates and sharing those results with the public and NIST;
- d. actively participating in several international conferences; and
- e. commenting on the the Draft FIPS for the AES.

NIST expects that the cryptographic community will continue to analyze the AES through various conferences such as CRYPTO, EUROCRYPT, ASIACRYPT, and the Fast Software Encryption Workshop (FSE).

Security and Maintenance of the AES

12. Did NIST consider adding more rounds to Rijndael?

Prior to its evaluation of the five finalists, NIST's AES selection team discussed the issue of whether it should change the number of rounds for one or more of the algorithms, since that issue had been raised by the public during the recent comment period. Some of those public comments offered specific reasons for changing the number of rounds, although many did not, and there seemed to be no agreement regarding which algorithm(s) should be altered (and if so, exactly how that should be done).

NIST's selection team recognized that changing the number of rounds would decrease the utility of the large amount of analysis that has taken place during the last two years. For some algorithms, it is not clear how the algorithm would be fully defined (e.g., the key schedule) with a different number of rounds, or how such a change would impact the security analysis. Another consideration was that none of the algorithms' submitters proposed to change the number of rounds in their algorithms, when they were given an opportunity to propose minor modifications in the summer of 1999. For these reasons, NIST's AES selection team decided it would be most appropriate to base its evaluation and selection on the five algorithms as they were originally submitted (i.e., without changing the number of rounds).

NIST's [report](#) offers more details.

13. Will the AES replace Triple DES and DES?

The AES is being developed to replace DES, but NIST anticipates that Triple DES will remain an approved algorithm (for U.S. Government use) for the foreseeable future. Single DES is being phased out of use, and is currently permitted in legacy systems, only.

Triple DES and DES are specified in [FIPS 46-3](#), while the AES is specified in [FIPS 197](#). The status of the algorithms in each FIPS is handled separately by NIST.

14. Is NIST concerned that the algorithm is of foreign origin?

No. The complete algorithm specification and design rationale was available for review by NIST, NSA, and the general public for more than two years before its selection. From the beginning of the AES development effort, NIST has indicated that the involvement of the international crypto community has been necessary for the development of a high-quality standard.

15. Approximately how big are the AES key sizes?

The AES specifies three key sizes: 128, 192 and 256 bits. In decimal terms, this means that there are

approximately:

3.4×10^{38} possible 128-bit keys;

6.2×10^{57} possible 192-bit keys; and

1.1×10^{77} possible 256-bit keys.

In comparison, DES keys are 56 bits long, which means there are approximately 7.2×10^{16} possible DES keys. Thus, there are on the order of 10^{21} times more AES 128-bit keys than DES 56-bit keys.

16. What is the chance that someone could use the "DES Cracker"-like hardware to crack an AES key?

In the late 1990s, specialized "DES Cracker" machines were built that could recover a DES key after a few hours. In other words, by trying possible key values, the hardware could determine which key was used to encrypt a message.

Assuming that one could build a machine that could recover a DES key in a second (i.e., try 2^{55} keys per second), then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key. To put that into perspective, the universe is believed to be less than 20 billion years old.

17. Will NIST continue to monitor the algorithm's security, and how will it handle security issues that may arise in the future?

Yes. As is the case with its other cryptographic algorithm standards, NIST will continue to follow developments in the cryptanalysis of Rijndael. The AES will be formally reevaluated every five years. Maintenance activities for the standard will be developed at the appropriate time, in full consideration of the situation's particular circumstances. Should an issue arise that requires more immediate attention, NIST will act expeditiously and consider all available alternatives at that time.

18. How long will the AES last?

No one can be sure how long the AES - or any other cryptographic algorithm - will remain secure. However, NIST's Data Encryption Standard (DES) was a U.S. Government standard for approximately twenty years before it was known to be "cracked" by massive parallel network computer attacks and special-purpose "DES-cracking" hardware. The AES supports significantly larger key sizes than what DES supports. Barring any attacks against AES that are faster than key exhaustion, then even with future advances in technology, AES has the potential to remain secure well beyond twenty years.

Implementation, Testing, and Use of the AES

19. Who will be required to implement and use the AES?

The AES algorithm is an approved encryption algorithm that can be used by U.S. Government organizations to protect sensitive (unclassified) information. As is currently the case, those Government organizations will be able to use other FIPS-approved algorithms in addition to, or in lieu of, the AES.

Commercial and other non-U.S. Government organizations are invited - **but not required** - to adopt and implement the AES and NIST's other cryptographic standards.

20. Will NIST test for the conformance of products with the AES?

Conformance testing of the AES will be conducted under the [Cryptographic Module Validation Program \(CMVP\)](#), run jointly by NIST and the [Communications Security Establishment \(CSE\)](#) of the Government of

Canada. Commercial, accredited laboratories test cryptographic implementations for conformance to NIST's standards, and if the implementations conform, then NIST and CSE issue jointly-signed validation certificates for those implementations.

21. Are test values and reference code available for the AES?

Yes, [test values and code](#) provided by the Rijndael submitters are available, in order to assist implementers.

22. Will implementations of the AES be exportable?

Yes, AES implementations will be exportable, and AES implementations in proprietary systems will just need a one-time review prior to export. For full details, please contact the [Department of Commerce's Bureau of Export Administration \(BXA\)](#), which maintains the export regulations related to cryptographic technology. More information on current export regulations is available from [BXA's Information Technology Controls Division](#); TEL: (202) 482-0707, or FAX: (202) 501-0784.

Last Modified: January 28, 2002

[Questions?](#)

[Press Contacts](#)

[Computer Security Division](#)

[National Institute of Standards and Technology](#)