DEFINITION

Advanced Encryption Standard (AES)

Posted by: Margaret Rouse WhatIs.com

Follow:

Contributor(s): Michael Cobb, GEM100, Borys Pawliw

The Advanced Encryption Standard, or AES, is a symmetric block cipher chosen by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.

The National Institute of Standards and Technology (NIST) started development of AES in 1997 when it announced the need for a successor algorithm for the Data Encryption Standard (DES), which was starting to become vulnerable to brute-force attacks.

This new, advanced encryption algorithm would be unclassified and had to be "capable of protecting sensitive government information well into the next century," according to the NIST announcement of the process for development of an advanced encryption standard algorithm. It was intended to be easy to implement in hardware and software, as well as in restricted environments (for example, in a smart card) and offer good defenses against various attack techniques.

AES features

The selection process for this new symmetric key algorithm was fully open to public scrutiny and comment; this ensured a thorough, transparent analysis of the designs submitted.

NIST specified the new advanced encryption standard algorithm must be a block cipher capable of handling 128 bit blocks, using keys sized at 128, 192, and 256 bits; other criteria for being chosen as the next advanced encryption standard algorithm included:

- **Security:** Competing algorithms were to be judged on their ability to resist attack, as compared to other submitted ciphers, though security strength was to be considered the most important factor in the competition.
- **Cost:** Intended to be released under a global, nonexclusive and royalty-free basis, the candidate algorithms were to be evaluated on computational and memory efficiency.
- **Implementation:** Algorithm and implementation characteristics to be evaluated included the flexibility of the algorithm; suitability of the algorithm to be implemented in hardware or software; and overall, relative simplicity of implementation.

Choosing AES algorithms

Fifteen competing symmetric key algorithm designs were subjected to preliminary analysis by the world cryptographic community, including the National Security Agency (NSA). In August 1999, NIST selected five algorithms for more extensive analysis. These were:

- MARS, submitted by a large team from IBM Research
- RC6, submitted by RSA Security
- Rijndael, submitted by two Belgian cryptographers, Joan Daemen and Vincent Rijmen
- Serpent, submitted by Ross Anderson, Eli Biham and Lars Knudsen
- Twofish, submitted by a large team of researchers from Counterpane Internet Security, including noted cryptographer Bruce Schneier

Implementations of all of the above were tested extensively in ANSI C and Java languages for speed and reliability in encryption and decryption; key and algorithm setup time; and resistance to various attacks, both in hardware- and software-centric systems. Members of the global cryptographic community conducted detailed analyses (including some teams that tried to break their own submissions).

After much feedback, debate and analysis, the Rijndael cipher -- a mash of the Belgian creators' last names Daemen and Rijmen -- was selected as the proposed algorithm for AES in October 2000 and published by NIST as U.S. FIPS PUB 197. The Advanced Encryption Standard became effective as a federal government standard in 2002. It is also

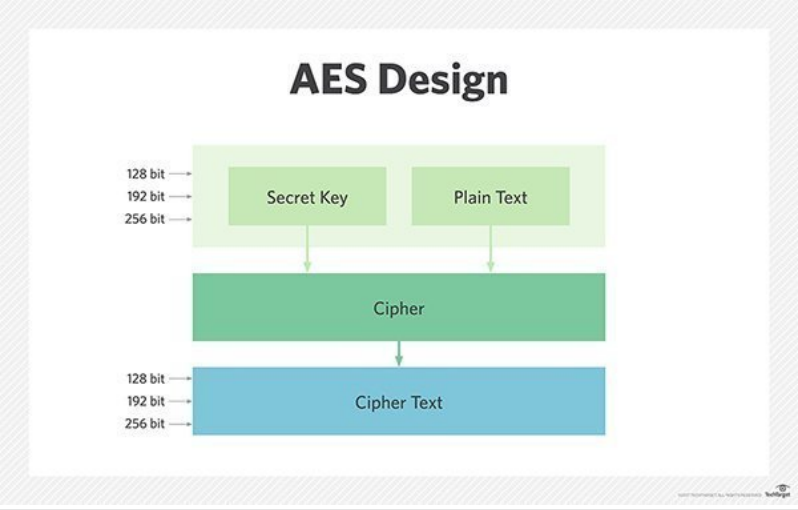
included in the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 18033-3 standard, which specifies block ciphers for the purpose of data confidentiality.

In June 2003, the U.S. government announced that AES could be used to protect classified information, and it soon became the default encryption algorithm for protecting classified information as well as the first publicly accessible and open cipher approved by the NSA for top-secret information. The NSA chose AES as one of the cryptographic algorithms to be used by its Information Assurance Directorate to protect national security systems.

Its successful use by the U.S. government led to widespread use in the private sector, leading AES to become the most popular algorithm used in symmetric key cryptography. The transparent selection process helped create a high level of confidence in AES among security and cryptography experts. AES is more secure than its predecessors -- DES and 3DES -- as the algorithm is stronger and uses longer key lengths. It also enables faster encryption than DES and 3DES, making it ideal for software applications, firmware and hardware that require either low latency or high throughput, such as firewalls and routers. It is used in many protocols such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS) and can be found in most modern applications and devices that need encryption functionality.

How AES encryption works

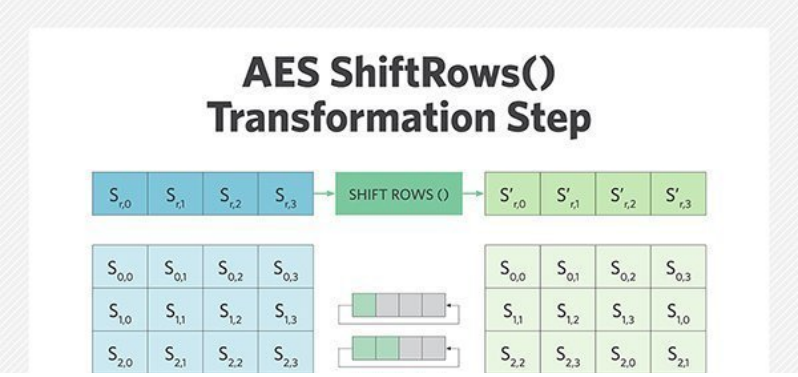
AES comprises three block ciphers: AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. The Rijndael cipher was designed to accept additional block sizes and key lengths, but for AES, those functions were not adopted.



Symmetric (also known as secret-key) ciphers use the same key for encrypting and decrypting, so the sender and the receiver must both know -- and use -- the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of ciphertext.

The AES encryption algorithm defines a number of transformations that are to be performed on data stored in an array. The first step of the cipher is to put the data into an array; after which the cipher transformations are repeated over a number of encryption rounds. The number of rounds is determined by the key length, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

The first transformation in the AES encryption cipher is substitution of data using a substitution table; the second transformation shifts data rows, the third mixes columns. The last transformation is a simple exclusive or (XOR) operation performed on each column using a different part of the encryption key -- longer keys need more rounds to complete.



AES encryption transforms array data by shuffling rows and columns, and substitutions based on the encryption key.

Attacks on AES encryption

Research into attacks on AES encryption has continued since the standard was finalized in 2000. Various researchers have published attacks against reduced-round versions of the Advanced Encryption Standard.

Prev

1

Next

Margaret Rouse asks:

How could the selection process used by NIST for the Advanced Encryption Standard be improved?

Join the Discussion

In 2005, cryptographer Daniel J. Bernstein published a paper, "Cache-timing attacks on AES," in which he demonstrated a timing attack on AES capable of achieving a "complete AES key recovery from known-plaintext timings of a network server on another computer."

A research paper published in 2011, titled "Biclique Cryptanalysis of the Full AES," by researchers Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger, demonstrated that by using a technique called a biclique attack, they could recover AES keys faster than a brute-force attack by a factor of between three and five, depending on the cipher version. However, even this attack does not threaten the practical use of AES due to its high-computational complexity.

AES has proven to be a reliable cipher, and the only practical successful attacks against AES have leveraged side-channel attacks on weaknesses found in the implementation or key management of specific AES-based encryption products.

Side-channel attacks exploit flaws in the way a cipher has been implemented rather than brute force or theoretical weaknesses in a cipher. The Browser Exploit Against SSL/TLS (BEAST) browser exploit against the TLS v1.0 protocol is

a good example; TLS can use AES to encrypt data, but due to the information that TLS exposes, attackers managed to predict the initialization vector block used at the start of the encryption process.

This was last updated in March 2017

Continue Reading About Advanced Encryption Standard (AES)

- Uncover the difference between AES and DES
- What is the difference between symmetric and asymmetric encryption algorithms? Find out here
- Read a lecture on the Advanced Encryption Standard from Purdue University
- Learn more about the Advanced Encryption Standard from the Internet Engineering Task Force (IETF)

Related Terms

cipher

In cryptology, the discipline concerned with the study of cryptographic algorithms, a cipher is an algorithm for encrypting and ...
See complete definition

cryptanalysis

Cryptanalysis is the study of ciphertext, ciphers and cryptosystems with the aim of understanding how they work and finding and ...
See complete definition

email spam

Email spam, or junk email, is unsolicited bulk messages sent through email with commercial, fraudulent or malicious intent. See complete definition

Dig Deeper on Email Security Guidelines, Encryption and Appliances

ALL NEWS GET STARTED PROBLEM SOLVE

Pretty Good Privacy (PGP)

Internet Key Exchange (IKE)

Cisco brings email security appliances closer to SaaS

Diffie-Hellman key exchange (exponential key exchange)

Load More

Join the conversation

6 comments

Share your comment

Send me notifications when other members comment.

Add My Comment

Oldest ▼

[-] **Margaret Rouse**

- 17 Nov 2014 7:33 AM

How could the selection process used by NIST for the Advanced Encryption Standard be improved?

Reply

[-] **Margaret Rouse**

- 17 Nov 2014 7:33 AM

Do you have any concerns about theoretical attacks against AES becoming a reality? Should the industry move to accommodate alternative ciphers such as Threefish or the Salsa20 stream cipher?

Reply

[-] **Ken Harthun**

- 10 Dec 2014 9:05 AM

In this universe, there are no absolutes. Likewise in the world of encryption. As computing power increases at an exponential rate, ciphers become increasingly subject to being broken. There's no question that we have very robust ciphers, per se, but when these are broken, it is usually because

of mistakes in their implementation.

AES will probably eventually be successfully attacked in situ. Someone will figure it out. Simply moving to alternatives will make little difference in the overall scheme of things: Crackers will someday figure out a way to break them, too. The answer to the question, "when is someday?" we have no way of predicting.

Keeping encryption robust is a cat and mouse game just like fighting malware and securing systems and networks.

Read Security Corner for more practical security advice.

Reply

[-] **Johniv**

- 21 May 2017 2:08 PM

What is to prevent someone from coming in a backdoor, leaving a utility like heapmemdump running as a thread and capturing the AES keycode? This has always bothered me, that any PC connected to the Net would be open to this exploit. Why crack the key when you can snatch it right out of memory. Isn't this essentially how the Cisco routers were exploited? A recent article mentioned HP audio drivers were found to have a keylogger embedded that was writing keystrokes to a file. Any PC connected to the Net, or allowing a memory stick to be inserted, is subject to this kind of exploitation. Let me know if I am wrong.

Reply

[-] **venkates**

- 23 Feb 2018 4:24 AM

Is this practically possible by using matlab?

Reply

[-] **asmig23**

- 25 Sep 2018 6:58 PM

Are designer and Advanced Encryption Standard stream ciphers or they use block cipher encryption?

Reply

Understanding the process behind Google's cloud data deletion can help influence stronger enterprise security policies. Expert Ed...

How to configure a vTAP for cloud networks

A vTAP can give enterprises better visibility into their cloud networks. Expert Frank Siemons of InfoSec Institute explains how ...