DEFINITION

Advanced Encryption Standard (AES)

By Michael Cobb

The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information. AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cybersecurity and electronic data protection.

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

NIST stated that the newer, advanced encryption algorithm would be unclassified and must be "capable of protecting sensitive government information well into the [21st] century." It was intended to be easy to implement in hardware and software, as well as in restricted environments -- such as a smart card -- and offer decent defenses against various attack techniques.

AES was created for the U.S. government with additional voluntary, free use in public or private, commercial or noncommercial programs that provide encryption services. However, nongovernmental organizations choosing to use AES are subject to limitations created by U.S. export control.

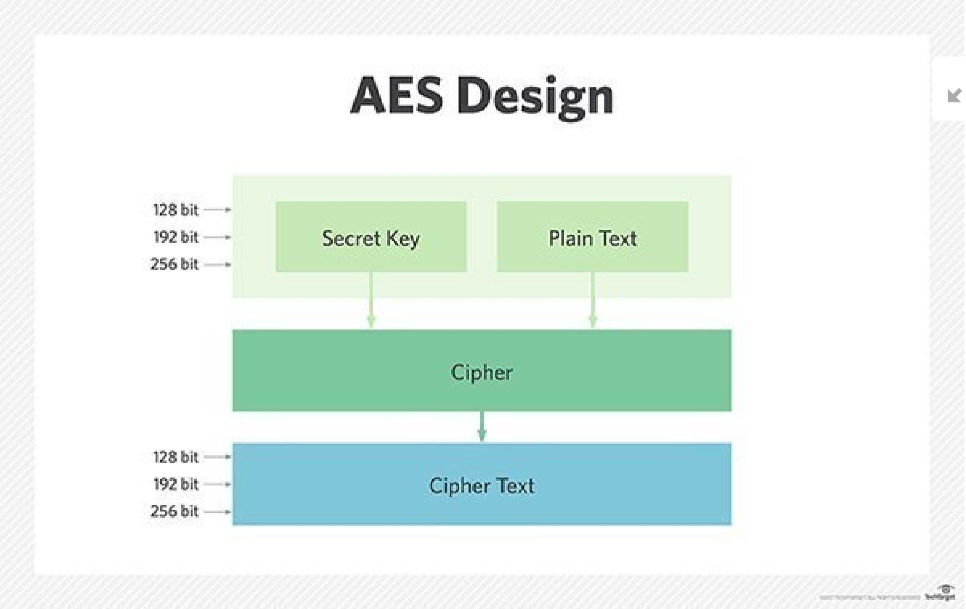
How AES encryption works

AES includes three block ciphers: AES-128, AES-192 and AES-256.

AES-128 uses a 128-bit key length to encrypt and decrypt a block of messages, while AES-192 uses a 192-bit key length and AES-256 a 256-bit key length to encrypt and decrypt messages. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively.

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. The government classifies information in three categories: Confidential, Secret or Top Secret. All key lengths can be used to protect the Confidential and Secret level. Top Secret information requires 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 to transform it into the final output of ciphertext.



A visual chart describing the relationships between secret key, plaintext, cipher and ciphertext

The AES encryption algorithm defines numerous 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 multiple encryption rounds.

The first transformation in the AES encryption cipher is substitution of data using a substitution table; the second transformation shifts data rows, and the third mixes columns. The last transformation is performed on each column using a different part of the encryption key. Longer keys need more rounds to complete.

AES features

NIST specified the new AES 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 AES algorithm included the following:

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

Choosing AES algorithms

Fifteen competing symmetric 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:

1. **MARS**, submitted by a large team from IBM Research;
2. **RC6**, submitted by RSA Security;
3. **Rijndael**, submitted by two Belgian cryptographers, Joan Daemen and Vincent Rijmen;
4. **Serpent**, submitted by Ross Anderson, Eli Biham and Lars Knudsen; and
5. **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 American National Standards Institute (ANSI), C and Java languages for speed and reliability in the encryption and decryption processes, key and algorithm setup time, and resistance to various attacks -- both in hardware- and software-centric systems. Detailed analyses were conducted by members of the global cryptographic community, including some teams that tried to break their own submissions.

After much feedback, debate and analysis, the Rijndael cipher was selected as the proposed algorithm for AES in October 2000. It was published by NIST as U.S. Federal Information Processing Standards (FIPS) PUB 197, which was accepted by the secretary of commerce in December 2001.

AES 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. 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.

The successful use of AES by the U.S. government led to the algorithm's widespread use in the private sector. AES has become the most popular algorithm used in symmetric key cryptography. The transparent selection process established by NIST helped create a high level of confidence in AES among security and cryptography experts.

Difference between AES-128 and AES-256

Overall, security experts consider AES safe against brute-force attacks, in which all possible key combinations are checked until the correct key is found. However, the key size employed for encryption needs to be large enough so that it cannot be cracked by modern computers, even considering advancements in processor speeds based on Moore's law.

A 256-bit encryption key is significantly more difficult for brute-force attacks to guess than a 128-bit key; however, because the latter takes so long to guess, even with a huge amount of computing power, it is unlikely to be an issue for the foreseeable future, as a hacker would need to use quantum computing to generate the necessary brute force.

Still, 256-bit keys also require more processing power and can take longer to execute. When power is an issue -- particularly on small devices -- or where latency is likely to be a concern, 128-bit keys are likely to be a better option.

When hackers want to access a system, they will aim for the weakest point, which is typically not the encryption, regardless of whether it's a 128-bit key or a 256-bit key. Users should make sure the software under consideration does what they want it to do, that it protects user data in the way it's expected to and that the overall process has no weak points.

Additionally, there should be no gray areas or uncertainty about data storage and handling. For example, if data resides in the cloud, users should know the location of the cloud. Most importantly, the security software that has been selected should be easy to use to ensure that users do not need to perform unsecure workarounds to do their jobs.

AES vs. RSA

AES is used widely for protecting data at rest. Applications for AES include self-encrypting disk drives, database encryption and storage encryption. On the other hand, the RSA (Rivest-Shamir-Adleman) algorithm is often used in web browsers to connect to websites, in virtual private network (VPN) connections and in many other applications.

Unlike AES, which employs symmetric encryption, RSA is the base of asymmetric cryptography. Symmetric encryption involves converting plaintext to ciphertext using the same key, or secret key, to encrypt and decrypt it. On the other hand, the term *asymmetric* comes from the fact that there are two related keys used for encryption: a public and a private key. If encryption is performed with the public key, decryption can only happen with the related private key and vice versa. Typically, RSA keys are employed when there are two separate endpoints.

While RSA encryption works well for protecting the transfer of data across geographic boundaries, its performance is poor. The solution is to combine RSA encryption with AES encryption in order to benefit from the security of RSA with the performance of AES. This can be accomplished by generating a temporary AES key and protecting it with RSA encryption.

AES vs. DES

The U.S. government developed DES algorithms more than 40 years ago to ensure government systems all used the same, secure standard to facilitate interconnectivity. DES served as the linchpin of government cryptography for years until 1999, when researchers broke the algorithm's 56-bit key using a distributed computer system. In 2000, the U.S. government chose to use AES to protect classified information. DES is still used in some instances for backward compatibility.

The two standards are both symmetric block ciphers, but AES is more mathematically efficient. The main benefit of AES lies in its key length options. The time required to crack an encryption algorithm is directly related to the length of the key used to secure the communication -- 128-bit, 192-bit or 256-bit keys. Therefore, AES is exponentially stronger than the 56-bit key of DES. AES encryption is also significantly faster, so it is ideal for applications, firmware and hardware that require low latency or high throughput.

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 AES.

Researchers have found a few potential ways to attack AES encryption. In 2009, they discovered a possible related-key attack. This cryptanalysis attempted to crack a cipher by studying how it operates using different keys. The related-key attack proved to be a threat only to AES systems that are incorrectly configured.

In 2009, there was a known-key attack against AES-128. A known key was used to discern the structure of the encryption. However, the hack only targeted an eight-round version of AES-128, rather than the standard 10-round version, making the threat relatively minor.

A major risk to AES encryption comes from side-channel attacks. Rather than attempting a brute-force assault, side-channel attacks are aimed at picking up leaked information from the system. Side-channel attacks, however, may reduce the number of possible combinations required to attack AES with brute force.

Side-channel attacks involve collecting information about what a computing device does when it is performing cryptographic operations and using that information to reverse-engineer the device's cryptography system. These attacks may use timing information, such as how long it takes the computer to perform computations; electromagnetic leaks; audio clues; and optical information -- for example, from a high-resolution camera -- to discover extra information about how the system is processing the AES encryption. In one case, a side-channel attack was used successfully to deduce AES-128 encryption keys by carefully monitoring the cipher's shared use of the processors' cache tables.

Side-channel attacks can be mitigated by preventing possible ways data can leak. Additionally, using randomization techniques can help eliminate any relationship between data protected by the cipher and any leaked data that could be collected using a side-channel attack.

AES security

Security experts maintain that AES is secure when implemented properly. However, AES encryption keys need to be protected. Even the most extensive cryptographic systems can be vulnerable if a hacker gains access to the encryption key.

Use of strong passwords, password managers, multifactor authentication (MFA), firewalls and antivirus software is critical to enterprise security. Employees should also be trained in ways to prevent social engineering and phishing attacks.

This was last updated in April 2020

Continue Reading About Advanced Encryption Standard (AES)

- The difference between AES and DES encryption
- Cryptography basics: Symmetric key encryption algorithms
- How to use data encryption tools and techniques effectively
- Fitting cybersecurity frameworks into your security strategy
- How does AES encryption work?

Related Terms

computer security incident response team (CSIRT)

A computer security incident response team, or CSIRT, is a group of IT professionals that provides an organization with services ... See complete definition ⓘ

cyber espionage

Cyber espionage, also called cyber spying, is a form of cyber attack that is carried out against a competitive company or ... See complete definition ⓘ

National Security Agency (NSA)

The National Security Agency (NSA) is a federal government intelligence agency that is part of the United States Department of ... See complete definition ⓘ

↘ Dig Deeper on Government information security management

block cipher

By: TechTarget Contributor

hard-drive encryption

By: Margaret Rouse

cryptography

By: Kathleen Richards

Symmetric vs. asymmetric encryption: Decipher the differences

By: Michael Cobb

SearchSecurity

Latest TechTarget
resources

- CLOUD SECURITY
- NETWORKING
- CIO
- ENTERPRISE DESKTOP
- CLOUD COMPUTING
- COMPUTER WEEKLY

SearchCloudSecurity

Invest in cloud security to future-proof your organization

The cloud has opened many opportunities for enterprises to maintain operations during the pandemic, but it has also created ...

What are cloud security frameworks and how are they useful?

Cloud security frameworks help CSPs and customers alike, providing easy-to-understand security baselines, validations and ...

- About Us
- Meet The Editors
- Contact Us
- Videos
- Photo Stories
- Definitions
- Guides
- Advertisers
- Business Partners
- Media Kit
- Corporate Site
- Contributors
- CPE and CISSP Training
- Reprints
- Events
- E-Products