What is AES encryption?

AES or Advanced Encryption Standard is a cipher, i.e., a method for encrypting and decrypting information. Whenever you transmit files over secure file transfer protocols like HTTPS, FTPS, SFTP, WebDAVS, OFTP, or AS2, there's a good chance your data will be encrypted by some flavor of AES - either AES 256, 192, or 128.

AES features

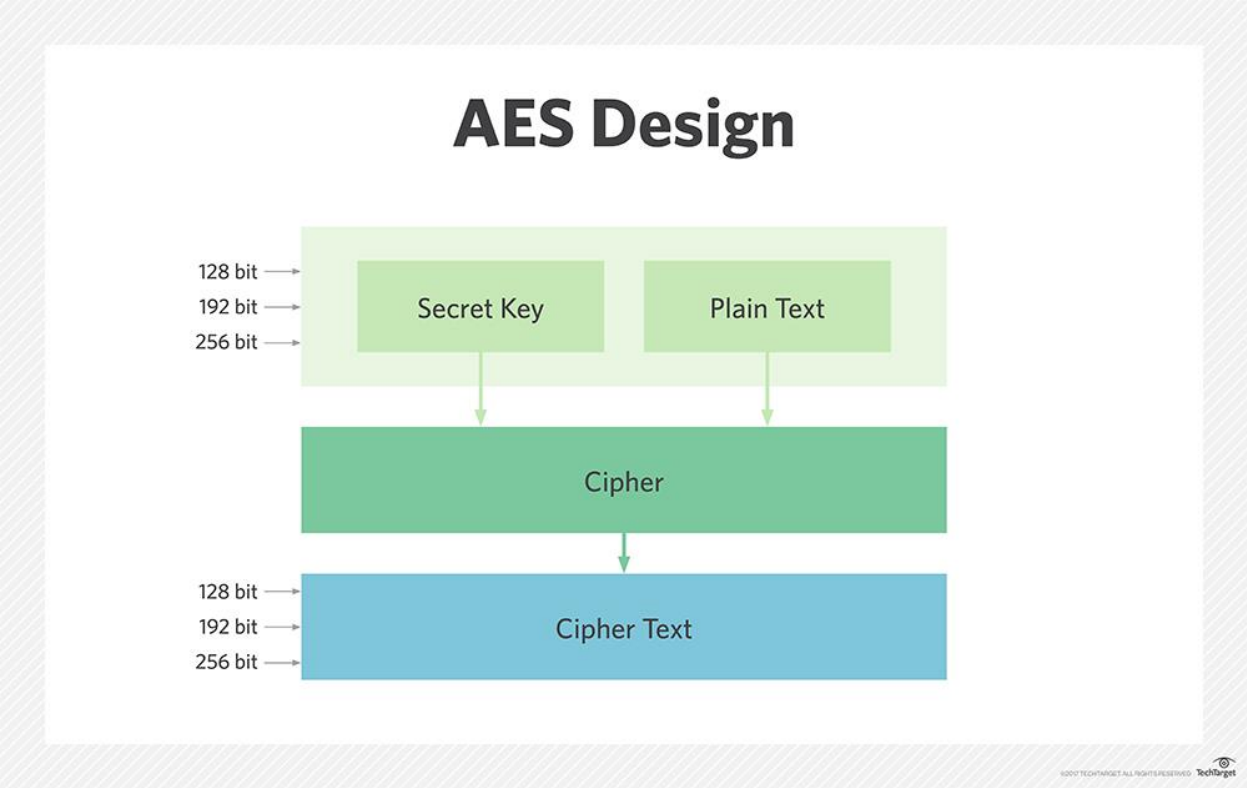
The selection process for this new symmetric_key_algorithm was fully open to public scrutiny and comment; this ensured a thorough, transparent analysis of the designs submitted.

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.

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.

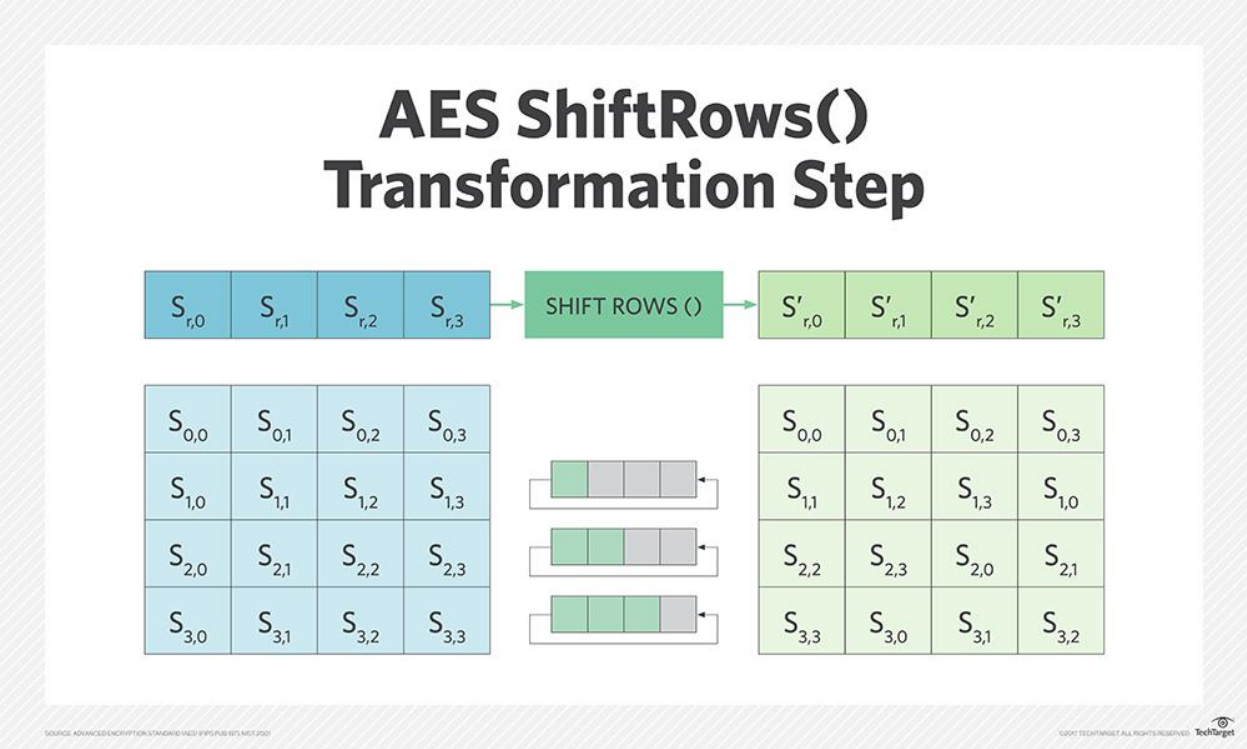


Symmetric (also known as secret-key) ciphers use the same key for encrypting and decrypting, so the sender and the receiver must both know -- and use -- the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information 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 cipher text.

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.



Attacks and Security Breaches Related to AES

AES has yet to be broken in the same way that DES was back in 1999, and the largest successful brute-force attack against *any* block cipher was only against a 64-bit encryption (at least to public knowledge).

The majority of cryptographers agree that, with current hardware, successfully attacking the AES algorithm, even on a 128-bit key would take billions of years and is, therefore, highly improbable.

At the present moment, there isn't a single known method that would allow someone to attack and decrypt data encrypted by AES so long as the algorithm was properly implemented.

However, many of the documents leaked by Edward Snowden show that the NSA is researching whether or not something known as the tau statistic could be used to break AES.

Side Channel Attacks

Despite all of the evidence pointing to the impracticality of an AES attack with current hardware, this doesn't mean that AES is completely secure.

Side channel attacks, which are an attack based on information gained from the physical implementation of a cryptosystem, can still be exploited to attack a system encrypted with AES. These attacks are not based on weaknesses in the algorithm, but rather physical indications of a potential weakness that can be exploited to breach the system.

Here are a few common examples.

- **Timing Attack**: These attacks are based on attackers measuring how much time various computations need to perform.
- **Power-monitoring Attack**: These attacks rely on the variability of power consumption by hardware during computation
- **Electromagnetic Attacks**: These attacks, which are based on leaked electromagnetic radiation, can directly provide attackers with plaintext and other information. This information can be used to surmise the cryptographic keys by using methods similar to those used by the NSA with TEMPEST.

The Anthem Hacking: How AES Could Have Saved 80 Million People's Personal Data

During February of 2015, the database for the Anthem insurance company was hacked, compromising the personal data of over 80 million Americans.

The personal data in question included everything from the names, addresses, and social security numbers of the victims.

And while the CEO of Anthem reassured the public by stating the credit card information of their clients was not compromised, any hacker worth his salt can easily commit financial fraud with the stolen information.

While the company's spokesperson claimed that the attack was unpreventable and that they had taken every measure to ensure the security of their client's information, nearly every major data security company in the world disputed this claim, pointing out that the breach was, in fact, completely preventable.

While Anthem encrypted data in transit, they did *not* encrypt that same data while it was at rest. Meaning that their entire database.