The Advanced Encryption Standard (AES)

AES is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware.[11] Unlike its predecessor DES, AES does not use a Feistel network.

AES is a variant of Rijndael, with a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, Rijndael *per se* is specified with block and key sizes that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits. Most AES calculations are done in a particular finite field.

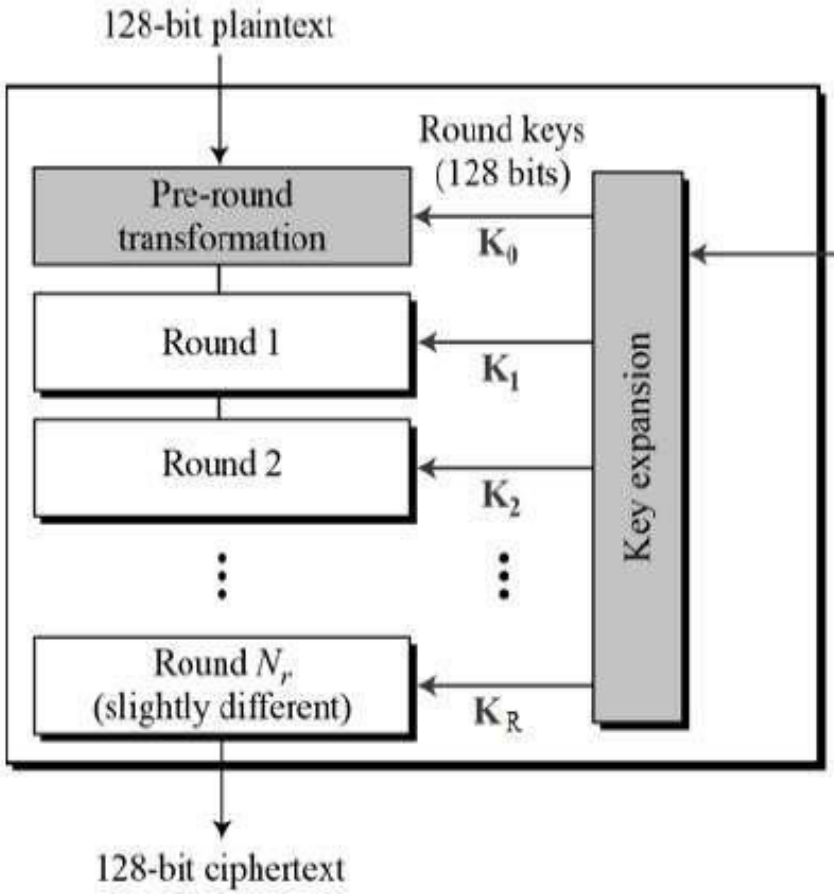
The key size used for an AES cipher specifies the number of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The number of rounds are as follows:

10 rounds for 128-bit keys.
12 rounds for 192-bit keys.
14 rounds for 256-bit keys.

Each round consists of several processing steps, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

High-level description of the algorithm[edit]

`KeyExpansion` – round keys are derived from the cipher key using the AES key schedule. AES requires a separate 128-bit round key block for each round plus one more.
Initial round key addition:
`AddRoundKey` – each byte of the state is combined with a byte of the round key using bitwise xor.
9, 11 or 13 rounds:
`SubBytes` – a non-linear substitution step where each byte is replaced with another according to a lookup table.
`ShiftRows` – a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
`MixColumns` – a linear mixing operation which operates on the columns of the state, combining the four bytes in each column.
`AddRoundKey`
Final round (making 10, 12 or 14 rounds in total):
`SubBytes`
`ShiftRows`
`AddRoundKey`



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size