**ADVANCED ENCRPTION STANDARD :**

**Description :**

The Advanced Encryption Standard (AES), also known by its original name Rijndael is a specification for the [encryption](https://en.wikipedia.org/wiki/Encryption) of electronic data established by the U.S. [National Institute of Standards and Technology](https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology) (NIST) in 2001.

AES is a subset of the Rijndael [block cipher](https://en.wikipedia.org/wiki/Block_cipher)developed by two [Belgian](https://en.wikipedia.org/wiki/Belgium) cryptographers, [Vincent Rijmen](https://en.wikipedia.org/wiki/Vincent_Rijmen) and [Joan Daemen](https://en.wikipedia.org/wiki/Joan_Daemen), who submitted a proposal to NIST during the [AES selection process](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard_process). Rijndael is a family of ciphers with different key and block sizes.

AES has been adopted by the [U.S. government](https://en.wikipedia.org/wiki/Federal_government_of_the_United_States) and is now used worldwide. It supersedes the [Data Encryption Standard](https://en.wikipedia.org/wiki/Data_Encryption_Standard) (DES), which was published in 1977. The algorithm described by AES is a [symmetric-key algorithm](https://en.wikipedia.org/wiki/Symmetric-key_algorithm), meaning the same key is used for both encrypting and decrypting the data.

AES is based on a design principle known as a [substitution–permutation network](https://en.wikipedia.org/wiki/Substitution%E2%80%93permutation_network), and is efficient in both software and hardware. AES is a variant of Rijndael which has a fixed [block size](https://en.wikipedia.org/wiki/Block_size_(cryptography)) of 128 [bits](https://en.wikipedia.org/wiki/Bit), and a [key size](https://en.wikipedia.org/wiki/Key_size) of 128, 192, or 256 bits. By contrast, Rijndael 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.

The key size used for an AES cipher specifies the number of transformation rounds that convert the input, called the [plaintext](https://en.wikipedia.org/wiki/Plaintext), into the final output, called the [ciphertext](https://en.wikipedia.org/wiki/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.

**Operation of AES**

AES is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix AES operates on a 4 × 4 [column-major order](https://en.wikipedia.org/wiki/Column-major_order) array of bytes, termed the state.Most AES calculations are done in a particular [finite field](https://en.wikipedia.org/wiki/Finite_field_arithmetic).

For instance, if there are 16 bytes b0 , b1 , b2 , ………….,b15 {\displaystyle b\_{0},b\_{1},...,b\_{15}} , these bytes are represented as this two-dimensional array:

|  |  |  |  |
| --- | --- | --- | --- |
| b0 | b1 | b2 | b3 |
| b4 | b5 | b6 | b7 |
| b8 | b9 | b10 | b11 |
| b12 | b13 | b14 | b15 |

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration –

**Img**

## Encryption Process :

## Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below –

## Img

### Byte Substitution (Sub-Bytes) :

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

### Shift rows :

Each of the four rows of the matrix is shifted to the left. Any entries that ‘fall off’ are re-inserted on the right side of row. Shift is carried out as follows −

* First row is not shifted.
* Second row is shifted one (byte) position to the left.
* Third row is shifted two positions to the left.
* Fourth row is shifted three positions to the left.
* The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

### Mix Columns :

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

### Add round key :

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round

## Decryption Process :

## The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

* Add round key
* Mix columns
* Shift rows
* Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.