**AES ALGORITHM**

The Advanced Encryption Standard, or AES, is a symmetric [block cipher](https://searchsecurity.techtarget.com/definition/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.

***Specification***

Key sizes: 128, 192 or 256 bits

Block sizes: 128 bits

Rounds: 10, 12 or 14 (depending on key size)

Designers: Vincent Rijmen, Joan Daemen

Structure: Substitution–permutation network

First published: 1998

Fig.2. Advanced Encryption Standard Algorithm Procedure

***AES Image Encryption***

Conversion of original image i.e plain image into encrypted image i.e cipher image is known as image encryption. The round consists of the following stages for image encryption

* Substitute Bytes
* Shift Row
* Mix Columns
* Add Round Key

# Algorithm to Encrypt an Image using AES Algorithm

1: Select an Image to Encrypt.

2: Declare a dynamic binary array of size = height of image \* width of image \* RGB\_size.

The RGB\_ size is 3.

3: Calculate Binary Value of each pixel of an Image.

4: Store all the RGB values of the pixel into the array.

5: Divide the binary array into blocks of size 256 bits and then create 16 sub blocks of 16 bits. This process will repeat till end of file.

6: Apply the Key Generation function to Select Key Value of 256 bits. And create 16 sub blocks of 16 bits.

7: Select 64 bits from transformation table. And create 4 blocks of 16 bits.

8: Apply Logical operation XOR between first 8 block of selected image and second 8 block of selected key. Result will stored in image blocks of

9: Apply Logical operation XOR between last 4 blocks of selected images and 4 blocks of transformation table. Result will store in image blocks.

10: Apply Circular Shift Operation on last 4 block of selected key and second last 4 block of selected image.

11: Apply logical XOR operation between selected image and key which is output of step 8. Result will store in image block.

12: Apply Circular Shift Operation on 4 blocks of transformation table and second last 4 block of selected key.

13: Apply logical XOR operation between transformation table and selected key, which is output of step 10. Result will store in key block.

14: Combine output of step 6, 7, 9, and 11 in such that it should be produced 256 bits total.

15: output of step 12 will become input for next round.

16: Repeat step-7 to step-15, 10 times.

17: After 16thround, cipher text will produce of selected image.. The cipher text obtained is in an array of bits.

18. Declare a dynamic binary array of size = height of image \* width of image \* RGB\_size. Now arrange the cipher values into the image .

19. The image now formed is the encrypted image file

20: Exit.