AES Encryption:

- AES is Advanced Encryption Standard (AES). It is a symmetric block cipher used to protect the information.
- AES is better than triple DES.
- AES includes three block ciphers AES - 128, AES-192, AES-256.

Each cipher(AES-128,AES-192,AES-256) encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively. As AES is a symmetric block cipher the 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 for encryption and decryption.

There are 10 rounds for 128-bit keys. A round consists of several processing steps that include:

1. Substitution
2. ShiftRows (Transposition)
3. Mixing (Plain Text) to transform it into cipher text.
4. AddRoundKey

Substitution:

AES works with bytes rather than bits. Hence, AES treats 128-bits as a block of 16 bytes.
The 16 input bytes are substituted by looking up a fixed S-box table.
The output of this step is a matrix with four rows and four columns.

ShiftRows:

Each of the four rows obtained in the previous step are shifted to the left. The remaining data is added to the right side of the row thereby making circular loop arrangement.
-> first row not shifted
-> second row shifted by one byte position to left
-> third row shifted by two positions to the left
-> fourth row shifted by three positions to the left.

The result is a new matrix with 16 bytes but shifted with respect to each other.

MixColumns:

Each of the column obtained from the previous step is transformed into a special mathematical function, The function takes as input the four bytes of one column and outputs four completely new bytes that replace the original values. The result is another 16 new bytes.

AddRoundKey:

The 16 bytes of the matrix are considered as bits and then are xored with a 128 bit round key. If this is the last round then the output is the cipher text or else the resulting 128 bits are interpreted as 16 bytes and begin another round.