AES:-

**AES**(Advanced encryption standard) or known as **Rijndael**. It is a symmetric key algorithm. There are different types of AES according to the different length of key (128, 192, 256)

Rounds according to the key size

**128 key size -10 rounds.**

192 key size-12 rounds.

256 key size-14 rounds.

Stages of AES(Encryption):-

1. **Key expansion**: Creating keys for each rounds from the original key using Rijndael key schedule.

Means for 10 round 10 keys will generated.

1. **Add round key** :Here the original chiper key will be add to the plaintext .
2. Next 9 rounds will be as follows:

**SubBytes** :Substituting each byte according to the S box

**ShiftRow** :Rows will be shifted according to the row number in horizontal left side rotation manner

**MixColumn** :In this step each column will go through a invertible linear transformation

**AddRoundKey** :Here addition of next 9 keys will take place 1 for each round.

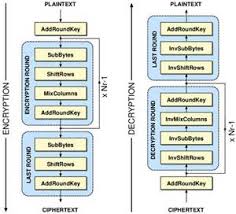
1. For the last round steps are:

**SubBytes** :Substituting each byte according to the S box

**ShiftRow** :Rows will be shifted according to the row number in horizontal left side rotation manner

**AddRoundKey** :Here addition of last key will take place .

***Decryption will takes place in reverse order.***



Sources:

<https://www.ijera.com/papers/Vol3_issue1/IW3116621670.pdf>

<https://en.wikipedia.org/wiki/Advanced_Encryption_Standard>

<https://en.wikipedia.org/wiki/Rijndael_key_schedule>

<https://www.youtube.com/watch?v=gP4PqVGudtg>