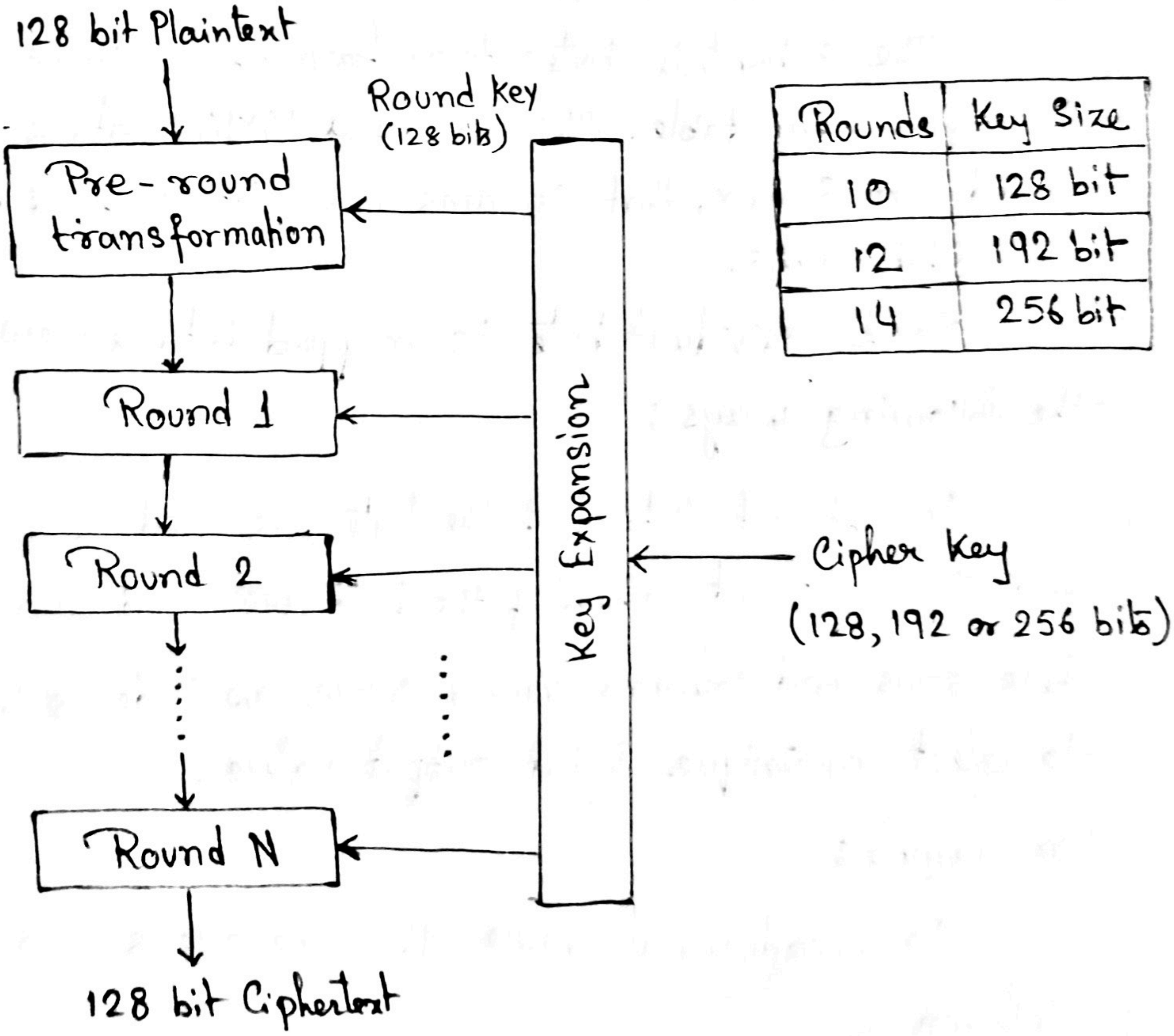
AES (Advanced Encryption Standard) Algorithm:

AES is an iterative rather than Feistel cipher. It is based on 'Substitution - permutation network'. AES performs all its computations on bytes rather than bits Hence AES treats the 128 bits of plaintext block as 16 bytes. These 16 bytes are arranged in a 4 rows and 4 columns matrix.

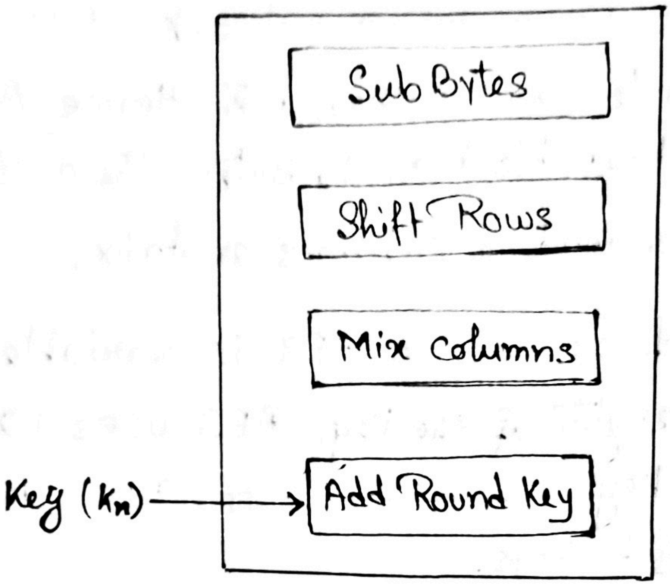
The number of rounds in AES is variable and depends on the length of the Key. AES uses 10 rounds for 128 - bit key, 12 rounds for 192 - bit Keys and 14 rounds for 256 - bit Keys.

The Schematic of AES structure is given as follows:



Rounds	Key Size
10	128 bit
12	192 bit
14	256 bit

Schematic of each round of AES:



Round N

Substitute Bytes Transformation:

The substitute bytes transformation called SubBytes is a simple lookup table. AES defines a 16X16 matrix of byte values called an S-box, that contains permutation of all possiable 256 8 bit values.

Each individual byte is mapped into a new byte in the following ways:

The leftmost 4 bits of the byte aree used as a row value and the rightmost 4 bits of the byte aree used as a column value These rows and columns values serve as indexes into the S-box to select an unique 8 bit output value.

For example:

The hexadecimal value 95 references row 9 and column 5.

Shift Rows Transformation :

The shift row Transformation is known as ShiftRows. In this the first row is not altered. For the Second row, a 1 byte circular left shift is performed. For the third row a 2 byte circular left shift is performed. For the fourth row a 3 byte circular left shift is performed.

For example,

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

→

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

Mix Columns Transformation :

The mix columns transformation also known as MixColumns, operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in that column. The transformation can be defined by the following matrix multiplication.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{00} & S_{01} & S_{02} & S_{03} \\ S_{10} & S_{11} & S_{12} & S_{13} \\ S_{20} & S_{21} & S_{22} & S_{23} \\ S_{30} & S_{31} & S_{32} & S_{33} \end{bmatrix} = \begin{bmatrix} S'_{00} & S'_{01} & S'_{02} & S'_{03} \\ S'_{10} & S'_{11} & S'_{12} & S'_{13} \\ S'_{20} & S'_{21} & S'_{22} & S'_{23} \\ S'_{30} & S'_{31} & S'_{32} & S'_{33} \end{bmatrix}$$

The MixColumn transformation on a single column can be expressed as,

$$s'_{0,j} = (2 \cdot s_{0,j}) \oplus (3 \cdot s_{1,j}) \oplus s_{2,j} \oplus s_{3,j}$$

$$s'_{1,j} = s_{0,j} \oplus (2 \cdot s_{1,j}) \oplus (3 \cdot s_{2,j}) \oplus s_{3,j}$$

$$s'_{2,j} = s_{0,j} \oplus s_{1,j} \oplus (2 \cdot s_{2,j}) \oplus (3 \cdot s_{3,j})$$

$$s'_{3,j} = (3 \cdot s_{0,j}) \oplus s_{1,j} \oplus s_{2,j} \oplus (2 \cdot s_{3,j})$$

For example,

$$\begin{bmatrix} 87 & F2 & 4D & 97 \\ 6E & 4C & 90 & EC \\ 46 & E7 & 4A & C3 \\ A6 & 8C & D8 & 95 \end{bmatrix} \longrightarrow \begin{bmatrix} 47 & 40 & A3 & 4C \\ 37 & D4 & 70 & 9F \\ 94 & E4 & 3A & 42 \\ ED & A5 & A6 & BC \end{bmatrix}$$

Add Round Key Transformation:

- In the Add Round key Transformation also Known as AddRoundKey, the 128 bits aree bitwise XORed with the 128 bits of the Round key. The operation is viewed as a columnwise operation between the 4 bytes of a column and one word of the round key. It can be viewed as a byte-level operation.

For example:

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

⊕

AC	19	28	57
77	FA	D1	5C
66	DC	29	00
F3	21	41	6A

=

EB	59	8B	1B
40	2E	A1	C3
F2	38	13	42
1E	84	E7	D6

128 bits value

round Key

Application of AES Algorithm:

AES is widely used in many applications.

i) Wireless Security: AES is used in securing wireless network such as wifi network, to ensure data confidentiality.

ii) Database Encryption: AES can be applied to encrypt Sensitive data stored in database.

iii) Secure Communication: AES is widely used in protocols like internet communications, emails, instant messaging and voice/video calls.

iv) Virtual Private Networks: AES is commonly used in VPN protocols to secure the communication between a user's device and a remote server.