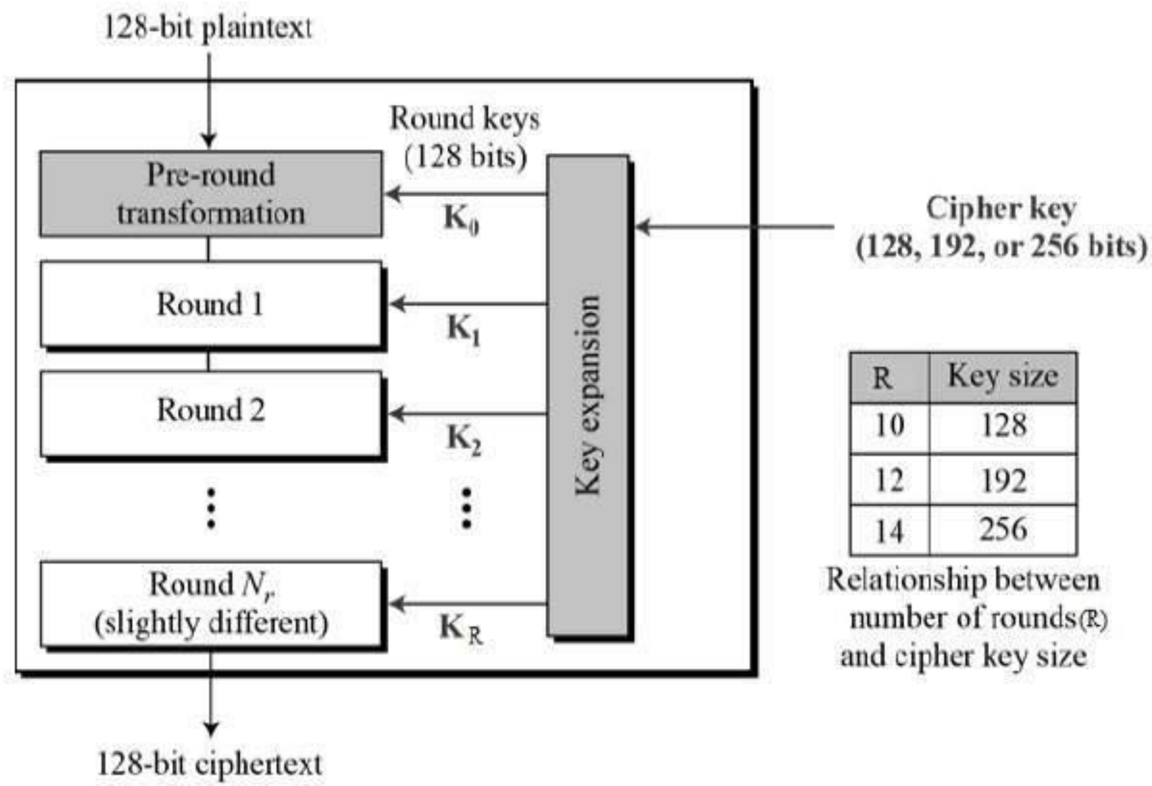
Block Cipher

The Advanced Encryption Standard (AES), also called Rijndael, is a symmetric block cipher with a block length of 128 bits and support for key lengths of 128, 192, and 256 bits. It was published by NIST (National Institute of Standards and Technology) in 2001. Here, we assume a key length of 128 bits, which is likely to be the one most commonly implemented.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

AES Block Cipher

The AES Algorithm:

- AES operates on a 4 × 4 column-wise order array of bytes, called the *state*. For instance, if there are 16 bytes, these bytes are represented as this two-dimensional array:

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

- The key size used for an AES cipher specifies the number of transformation rounds that convert the plaintext into the 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.

- Each round consists of several processing steps, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

AES Block Cipher

The AES Encryption Algorithm:

- The AES algorithm can be broken into three phases: the initial round, the main rounds, and the final round. All of the phases use the same sub-operations in different combinations as follows:

  Initial Round

  AddRoundKey

  Main Rounds (1,2…Nr-1)

  SubBytes

  ShiftRows

  MixColumns

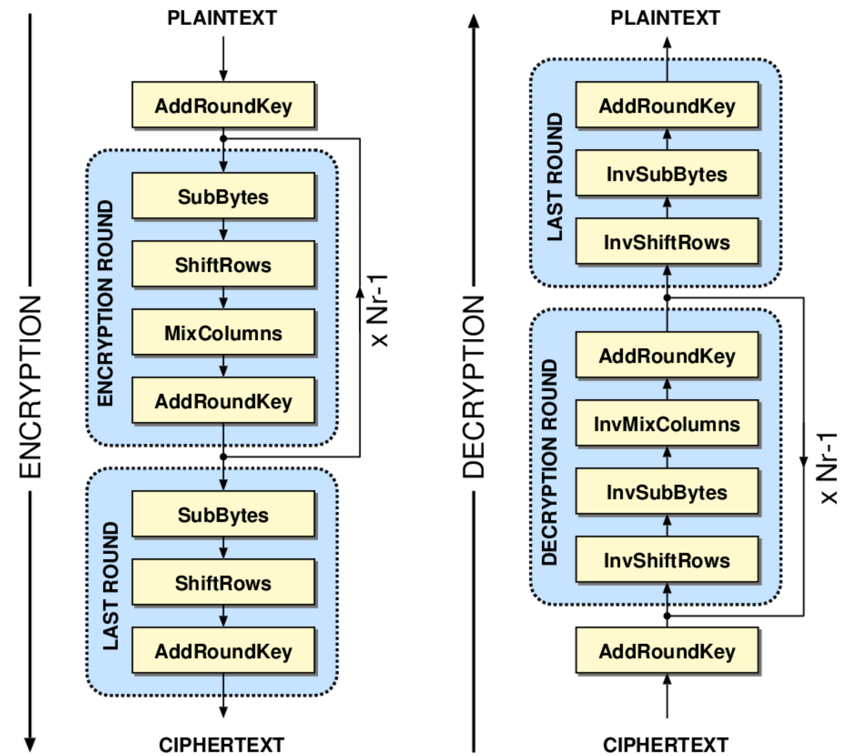
  AddRoundKey

  Final Round (Nr)

  SubBytes

  ShiftRows

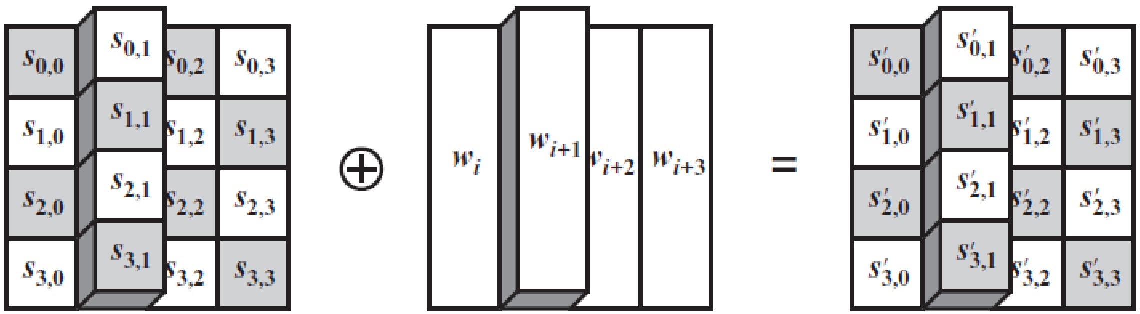
  AddRoundKey



Note that in the above figure, KeyExpansion: round keys are derived from the cipher key using key expansion algorithm. AES requires a separate 128-bit round key block for each round plus one more.

AES Block Cipher

AddRoundKey: In this operation, the 128 bits of **State** are bitwise XORed with the 128 bits of the round key. Here is an example where the first matrix is State, and the second matrix is the round key.



e.g.

$$\begin{pmatrix} 54 & 4F & 4E & 20 \\ 77 & 6E & 69 & 54 \\ 6F & 65 & 6E & 77 \\ 20 & 20 & 65 & 6F \end{pmatrix} \oplus \begin{pmatrix} 54 & 73 & 20 & 67 \\ 68 & 20 & 4B & 20 \\ 61 & 6D & 75 & 46 \\ 74 & 79 & 6E & 75 \end{pmatrix} = \begin{pmatrix} 00 & 3C & 6E & 47 \\ 1F & 4E & 22 & 74 \\ 0E & 08 & 1B & 31 \\ 54 & 59 & 0B & 1A \end{pmatrix}$$

$$\text{e.g.,}\ 69 \oplus 4B = 22$$

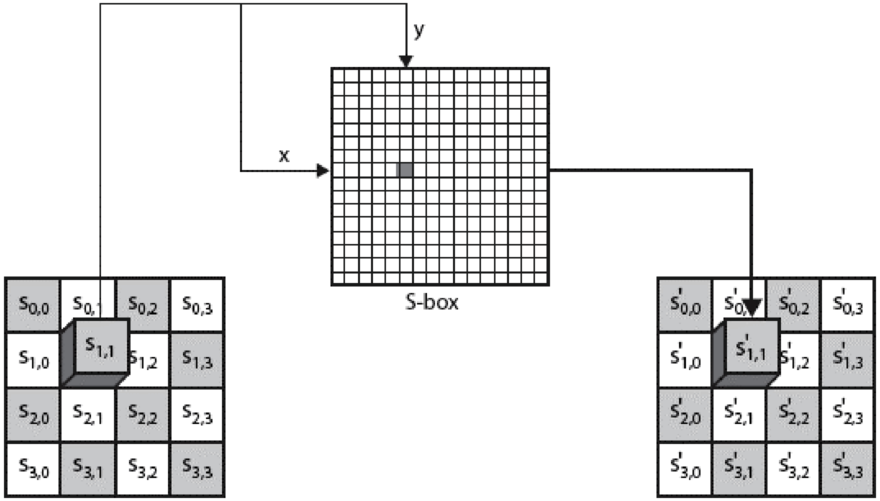
$$\begin{array}{r} 0110\ 1001 \\ 0100\ 1011 \\ \hline 0010\ 0010 \end{array}$$

AES Block Cipher

SubBytes: A nonlinear substitution step where each entry (byte) of the current state matrix is substituted by a corresponding entry in the AES S-Box. For instance: byte (6E) is substituted by the entry of the S-Box in row 6 and column E, i.e., by (9F). (The byte input is broken into two 4-bit halves. The first half determines the row and the second half determines the column).

e.g.:

$$\text{state} = \begin{pmatrix} 00 & 3C & 6E & 47 \\ 1F & 4E & 22 & 74 \\ 0E & 08 & 1B & 31 \\ 54 & 59 & 0B & 1A \end{pmatrix} \Rightarrow \text{S\_box(State)} = \begin{pmatrix} 63 & EB & 9F & A0 \\ C0 & 2F & 93 & 92 \\ AB & 30 & AF & C7 \\ 20 & CB & 2B & A2 \end{pmatrix}$$



AES Encryption Cipher

ShiftRows: A transposition step where the four rows of the state are shifted cyclically to the left by offsets of 0, 1, 2, and 3.

$$\begin{array}{|c|c|c|c|}\hline a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ \hline a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ \hline a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ \hline a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \\ \hline \end{array} \Rightarrow \begin{array}{|c|c|c|c|}\hline a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ \hline a_{1,1} & a_{1,2} & a_{1,3} & a_{1,0} \\ \hline a_{2,2} & a_{2,3} & a_{2,0} & a_{2,1} \\ \hline a_{3,3} & a_{3,0} & a_{3,1} & a_{3,2} \\ \hline \end{array}$$

e.g.:

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ C0 & 2F & 93 & 92 \\ AB & 30 & AF & C7 \\ 20 & CB & 2B & A2 \end{pmatrix} \Rightarrow \begin{pmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{pmatrix}$$

AES Block Cipher

MixColumns: a linear mixing operation which multiplies fixed matrix against current State Matrix:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

$$\begin{aligned} s'_{0,j} &= (2 \bullet s_{0,j}) \oplus (3 \bullet s_{1,j}) \oplus s_{2,j} \oplus s_{3,j} \\ s'_{1,j} &= s_{0,j} \oplus (2 \bullet s_{1,j}) \oplus (3 \bullet s_{2,j}) \oplus s_{3,j} \\ s'_{2,j} &= s_{0,j} \oplus s_{1,j} \oplus (2 \bullet s_{2,j}) \oplus (3 \bullet s_{3,j}) \\ s'_{3,j} &= (3 \bullet s_{0,j}) \oplus s_{1,j} \oplus s_{2,j} \oplus (2 \bullet s_{3,j}) \end{aligned}$$

Unlike standard matrix multiplication, MixColumns performs matrix multiplication as per Galois Field (2^8).

e.g.:

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{pmatrix} = \begin{pmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{pmatrix}$$

AES Block Cipher

The AES Decryption Algorithm:

❑ AddRoundKey:

Add Roundkey transformation is identical to the forward add round key transformation, because the XOR operation is its own inverse.

❑ Inverse SubBytes:

This operation can be performed using the inverse S-Box. It is read identically to the S-Box matrix.

❑ InvShiftRows:

Inverse Shift Rows performs the circular shifts in the opposite direction for each of the last three rows, with a one-byte circular right shift for the second row, and so on.

❑ InvMixColumns:

The inverse mix column transformation is defined by the following matrix multiplication in Galois Field (2^8):

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

Video Link

Video of AES

Another video