AES стандарт в США с 2001 года

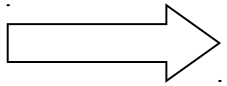
Advanced Encryption Standard

- Схема - квадрат из байтов,
  - Длины ключей N=128, 192, 256 бит
  - Длина блока данных n= 128,
  - d=f(N,n): d=10(N=128),12(N=192),14(N=256)

- Преимущества AES:
  - относительно высокая стойкость и скорость,
  - небольшая стоимость,
  - возможность эффективной программной и аппаратной реализации,
  - гибкость (переменная длина ключей)
  - реализуемость в системах с ограниченным количеством памяти.
- RIJNDAEL (Rijmen and Daemen) «Рейндолл»

1-ое преобразование

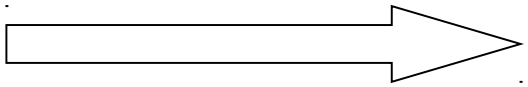
S_{00}	S_{01}	S_{02}	S_{03}
S_{10}	S_{11}	S_{12}	S_{13}
S_{20}	S_{21}	S_{22}	S_{23}
S_{30}	S_{31}	S_{32}	S_{33}



$\boldsymbol{S}_{00}^{-1}$	$\boldsymbol{S}_{01}^{-1}$	$\boldsymbol{S}_{02}^{-1}$	$\boldsymbol{S}_{03}^{-1}$
$\boldsymbol{S}_{10}^{-1}$	$\boldsymbol{S}_{11}^{-1}$	$\boldsymbol{S}_{12}^{-1}$	$\boldsymbol{S}_{13}^{-1}$
$\boldsymbol{S}_{20}^{-1}$	$\boldsymbol{S}_{21}^{-1}$	$\boldsymbol{S}_{22}^{-1}$	$\boldsymbol{S}_{23}^{-1}$
$\boldsymbol{S}_{30}^{-1}$	$\boldsymbol{S}_{31}^{-1}$	$\boldsymbol{S}_{32}^{-1}$	$\boldsymbol{S}_{33}^{-1}$

$$\boldsymbol{S}_{ij}^{-1} = \begin{bmatrix} b_0 & b_1 & \cdots & b_6 & b_7 \end{bmatrix}$$

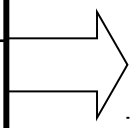
2-ое преобразование



$$\begin{bmatrix} \boldsymbol{b}_0' \\ \boldsymbol{b}_1' \\ \boldsymbol{b}_2' \\ \boldsymbol{b}_3' \\ \boldsymbol{b}_4' \\ \boldsymbol{b}_5' \\ \boldsymbol{b}_6' \\ \boldsymbol{b}_7' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} \boldsymbol{b}_0 \\ \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \\ \boldsymbol{b}_3 \\ \boldsymbol{b}_4 \\ \boldsymbol{b}_5 \\ \boldsymbol{b}_6 \\ \boldsymbol{b}_7 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \boldsymbol{C}_{ij}$$

3-ье преобразование

C_{00}	C_{01}	C_{02}	C_{03}
C_{10}	C_{11}	C_{12}	C_{13}
C_{20}	C_{21}	C_{22}	C_{23}
C_{30}	C_{31}	C_{32}	C_{33}



C_{00}	C_{01}	C_{02}	C_{03}
C_{11}	C_{12}	C_{13}	C_{10}
C_{22}	C_{23}	C_{20}	C_{21}
C_{33}	C_{30}	C_{31}	C_{32}

Матрица D

=

d_{00}	d_{01}	d_{02}	d_{03}
d_{10}	d_{11}	d_{12}	d_{13}
d_{20}	d_{21}	d_{22}	d_{23}
d_{30}	d_{31}	d_{32}	d_{33}

Следующее преобразование является перемешиванием столбцов матрицы D

На этом шаге каждый К-ый столбец матрицы D представляется в 16-ричной системе счисления как вектор над полем $GF(2^8)$ с образующим многочленом

$$p(x) = 1 + x + x^3 + x^4 + x^8$$

с дальнейшим умножением на определенную матрицу с элементами из этого же поля:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} D_{0K} \\ D_{1K} \\ D_{2K} \\ D_{3K} \end{bmatrix} = \begin{bmatrix} D'_{0K} \\ D'_{1K} \\ D'_{2K} \\ D'_{3K} \end{bmatrix}$$

Например, 02 = (0000 0010)

Наконец производится сложение всех 128 элементов полученной на предыдущем шаге матрицы D' с раундовым ключом. После завершения одного раунда все описанные выше операции повторяются с использованием других ключей. Количество раундов – 10, 12,14.