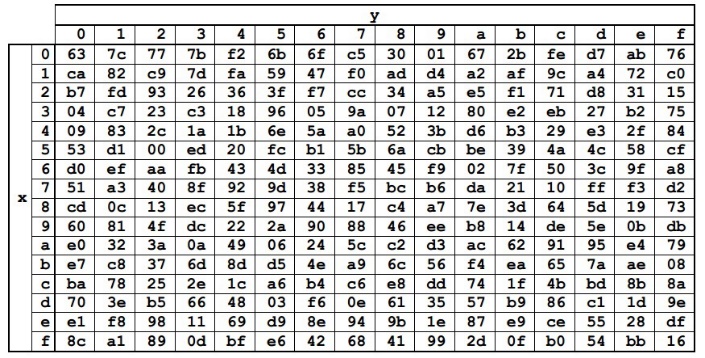
# AESC:\Users\savos\OneDrive\Рабочий стол\1.jpg

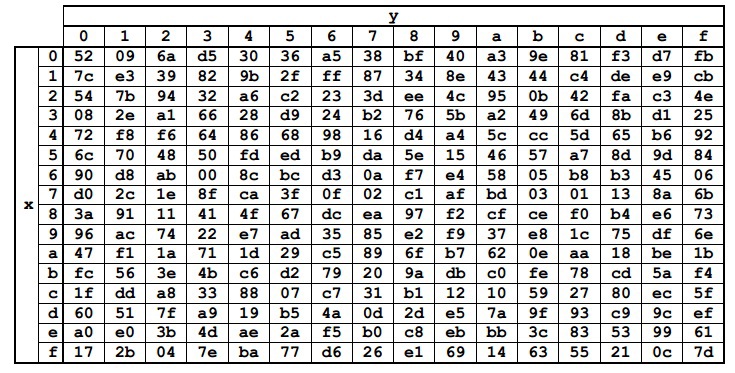


Преобразование представляет собой замену каждого байта из State на соответствующий ему из константной таблицы Sbox.

**SubBytes**

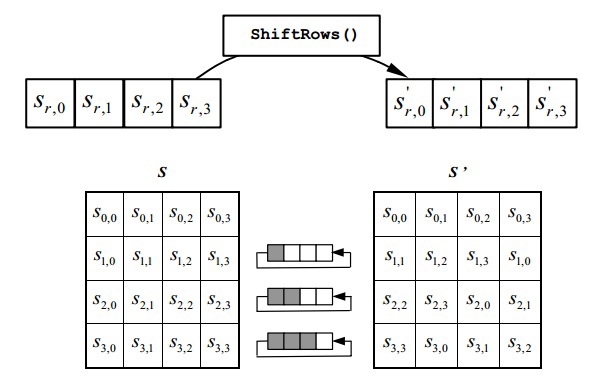


**InvSubBytes**



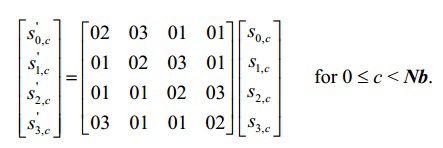
**ShiftRows**

Простая трансформация. Она выполняет циклический сдвиг влево на 1 элемент для первой строки, на 2 для второй и на 3 для третьей. Нулевая строка не сдвигается. Для inv сдвиг вправо.



**MixColumns**

В рамках этой трансформации каждая колонка в State представляется в виде многочлена и перемножается в поле GF(28) по модулю с фиксированным многочленом. .



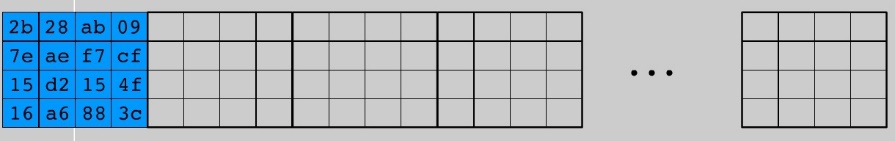
**AddRoundKey**

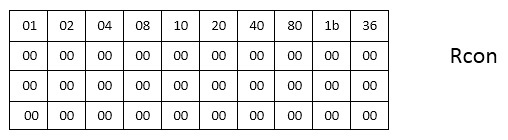
Трансформация производит побитовый XOR каждого элемента из State с соответствующим элементом из RoundKey. RoundKey — массив такого же размера, как и State, который строится для каждого раунда на основе секретного ключа функцией KeyExpansion()

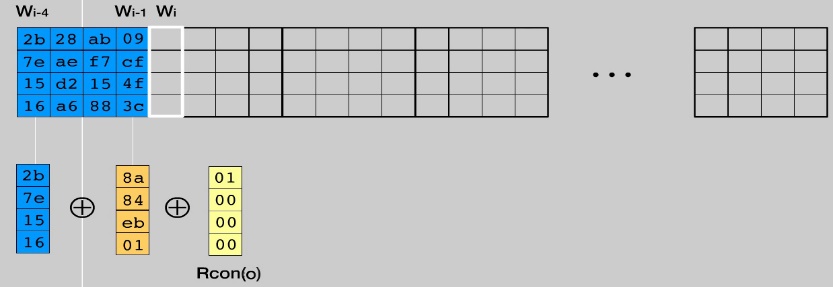
**KeyExpansion**

Эта вспомогательная трансформация формирует набор раундовых ключей — KeySchedule. KeySchedule представляет собой длинную таблицу, состоящую из Nb\*(Nr + 1) столбцов или (Nr + 1) блоков, каждый из которых равен по размеру State.

 Первый раундовый ключ заполняется на основе секретного ключа по формуле



****

****