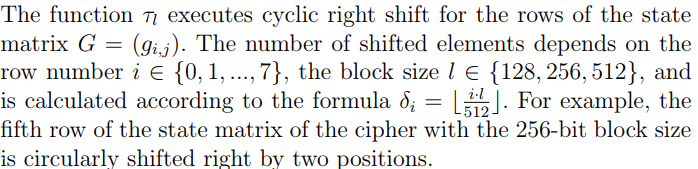
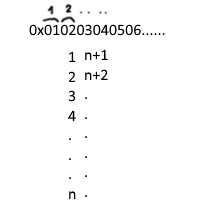
20:37 06.03.2018

Предполагают, что матрица промежуточного состояния в шифре кузнечик имеет ширину всегда 8 байт (столбцов), а строк в зависимости от размерности шифротекста/ключа.

21:13 06.03.2018

Читал вид второго блока. Блока сдвига. Там было сказано, что строк 8 штук.

22:29 06.03.2018

Протестировал 512/512 s\_row и оказалось, что если заполнять по столбам как показано на рисунке, то всё верно. В данном случае “row” – это строка в матрице.

22:57 06.03.2018

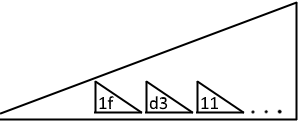
Протестировал s\_row в файле тест и выявил, что примеры в документе работают когда столбец должен быть 8 байт постоянно. Значит c – это кол-во столбцов.

23:48 06.03.2018

Такс! s\_row предполагает сдвиг на позицию (т.е. на 8 бит), а вот просто сдвиг – это сдвиг на биты. В m\_col тож как в s\_row.

15:37 07.03.2018

Входное значение для деления ключа в классе cKey будет иметь вид массива одномерного. Меньше индекс в массиве менее значимые байты в значении. Каждый байт представляется в big-ending виде, а массив в little-ending. В итоге:



2:46 08.03.2018

Предполагаю, что в моменте описания доп. блока для генерации использовалась константа

с форматом big-ending. Что соответствует в примере.

3:04 08.03.2018

При изучении генерации подключей было выявлено, что tmv подтверждает представление значений в примере как на рисунке выше.

2:13 11.03.2018

Переделываю всё. Более правильно и красиво.

16:33 11.03.2018

Циклический сдвиг при производстве подключей нечётный имеет вид побитовый циклический сдвиг. Результат получен и можно сказать, что матрица имеет размер столбца 8 значений, но кол-во столбцов c.

17:35 11.03.2018

Не очень понятно что блять в этой документации происходит. Если посмотреть на генерацию подключей при k=2l, то можно увидеть что чётное не делимое на 4 поворачивает на право на 16\*i и это как id отображается в их логах. В то же время должно быть и для чётного делимого на 4 такое – же (но поворот на другое значение). А этого дерьма нет. И при повороте циклически вправо в сторону более значимых битов в id на 4 в 128\_256 поворот идёт не в право а в лево. Чушь…..

18:03 11.03.2018

Я для рофла изменил в параметрах заметки выше всё на шифт в лево и норм остаток от деления сделал. Всё заработало для 128\_256, но не для 256\_256. Поехал к жеке.

2:39 16.03.2018

Начал делать дешифрование.

4:38 16.03.2018

В дешифровании то же происходит чушь с поворотами. В m\_col дешифрования нужно принимать поворот не в лево а в право.