**Шифр с управляемыми подстановками**

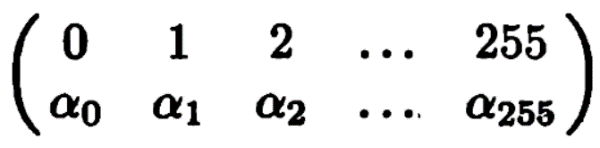
Шифр с управляемыми подстановками является еще одной возможностью реализации управляемых операций с целью внесения для противника дополнительной неопределенности в процесс преобразования сообщения при его шифровании. Один из вариантов построения такого шифра заключается в использовании набора из ***N*** таблиц подстановки, половина из которых являются таблицами прямой подстановки, а другая - таблицами обратной подстановки. То есть, каждой таблице прямой подстановки соответствует таблица обратной подстановки. Следует отметить, что такое деление довольно условно (которую из таблиц считать таблицей прямой подстановки, а какую обратной подстановки). Важно только, чтобы каждая таблица прямой подстановки имела (единственную) таблицу, взаимно обратную именно ей. Каждая таблица подстановки содержит две строки.

Рассмотрим пример построения шифра с управляемыми подстановками.

Положим, что всего имеются ***N* = 32** таблицы подстановки (16 + 16). Положим также, что таблице прямой подстановки Т0 соответствует таблица обратной подстановки Т31, таблице прямой подстановки Т1 - таблица обратной подстановки Т30, таблице прямой подстановки Т2 - таблица обратной подстановки Т29 и т.д. симметрично.

Используем режим блочного шифрования, для определенности положим, что размер шифруемого блока В равен 64 бита. Каждый блок В разобьем на 8 подблоков (в данном примере на 8 байтов): b0, b1, ... , b7. На каждом i-м раунде шифрования используется свой "набор" из 8-и (байтовых) раундовых секретных подключей: к0i, к1i, ... , к7i.

В этом случае в таблицах прямой (и обратной) подстановки должны находиться числа из диапазона от 0 до 255:



В данной таблице в нижней строке присутству­ют все возможные числа из верхнего ряда, но расставленные в другом порядке. Очередность расположения чисел в нижней строке определяет конкретный вариант таблицы подстановки, а, следовательно, и конкретный вариант опера­ции подстановки, выполняемой этой таблицей. Выполнение операции подстановки сводится к выбору по значению числа в верхней строке (вход таблицы подстановки - значение входного блока) числа, находящегося под этим числом в нижней строке. Оно и берется в качестве выходного блока.

Структура i-го раунда шифрования с управляемыми подстановками представлена на рис. 1.

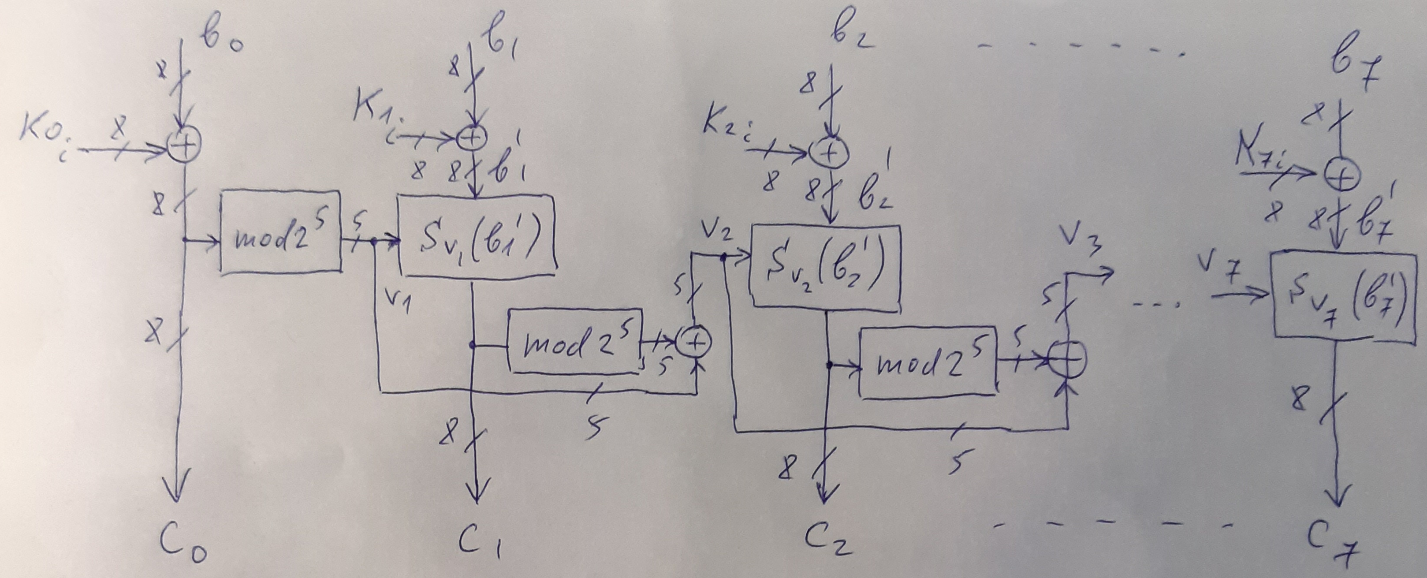


Рис. 1. В данной реализации алгоритма используется 32 таблицы. Размер каждой таблицы – 2 х 256

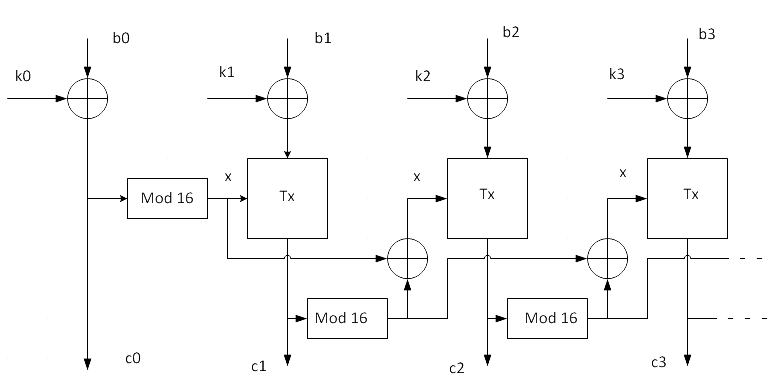


Рис. 1. В данной реализации алгоритма используется всего 16 таблиц.

Входные 8-битные подблоки b0, ... , b1, b7 складываются по модулю 2 с секретными раундовыми подключами к0i, ... ,к1i, к7i. Функциональные блоки mod 25 выделяют из 8-разрядных двоичных чисел пять их младших разрядов. Выделенные разряды используются в дальнейшем для непредсказуемого для противника формирования номеров (используемых 32-х таблиц подстановки). Порядок расчета номеров таблиц подстановки наглядно показан на рис. 1. Поэтому, если даже противнику известны все используемые в шифре таблицы подстановки, он не может правильно определить номер таблицы, используемой на каждом шаге шифрования в данном раунде. В результате для противника вносится дополнительная неопределенность в процесс шифрования сообщения. На рис. 1 с0, с1, ... , с7- это подблоки результата i-го раунда шифрования сообщения.

Для расшифрования сообщения надо правильно рассчитать номера таблиц обратной подстановки, в точности соответствующих использованным при шифровании таблицам прямой подстановки. В рассматриваемом примере таблице подстановки Т**k** (с порядковым номером k) соответствует таблица обратной подстановки с номером 31 - k, где k **=** 0, 1, ... , 31. Это дает возможность при расшифровании сообщения получить на каждом раунде номера соответствующих таблиц обратной подстановки.

С учетом сказанного, нетрудно построить структуру i-го раунда расшифрования.

