Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

Институт кибербезопасности и цифровых технологий
Кафедра КБ-8 «Информационное противоборство»

Отчёт по лабораторной работе №3

по дисциплине «Криптографические методы защиты информации»
«Сеть Фейстеля»

Студент: Усков К.А.

Шифр учебной группы: БАСО-03-20

Руководитель: Ермакова А.Ю.

Москва 2023г.

Содержание

1. Шифрование

Зашифруем исходную информацию, длинной 8 байт «67 2D 8E 3B D7 8D BD 51» с помощью сети Феистеля с ключом длинной 8, записанным по байтам в hex «DD C9 03 C4BA 88 42 C4».

На рисунке 1.1 показан первый раунд цикла шифрования.

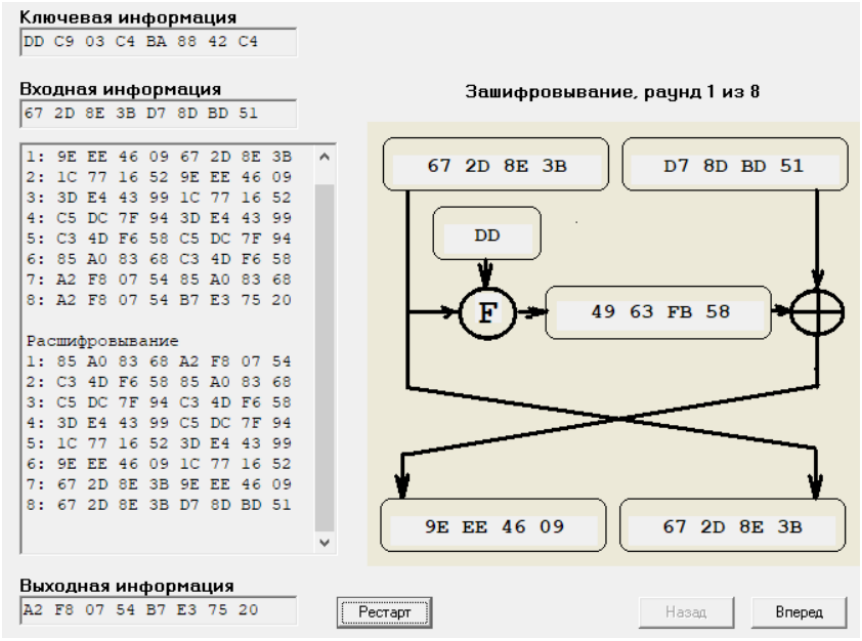

Рисунок 1.1 — Шифрование шаг 1.

Информация «67 2D 8E 3B D7 8D BD 51» преобразовалась с использованием функции F и раундового ключа «DD», в информацию «9E EE 46 09 67 2D 8E 3B».

На рисунке 1.2 показан второй раунд цикла шифрования. Информация «9E EE 46 09 67 2D 8E 3B» преобразовалась с использованием функции F и раундового ключа «C9», в информацию «1C 77 16 52 9E EE 46 09».

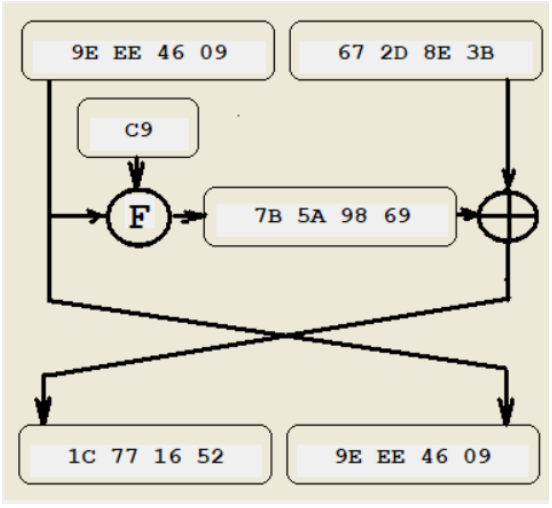

Рисунок 1.2 — Шифрование шаг 2.

На рисунке 1.3 показан раунд шаг цикла шифрования.

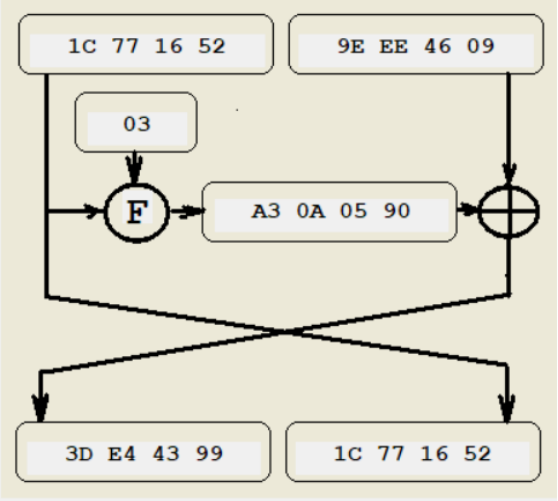

Рисунок 1.3 — Шифрование шаг 3.

Информация «1C 77 16 52 9E EE 46 09» преобразовалась с использованием функции F и раундового ключа «03», в информацию «3D E4 43 99 1C 77 16 52».

На рисунке 1.4 показан четвёртый раунд цикла шифрования.

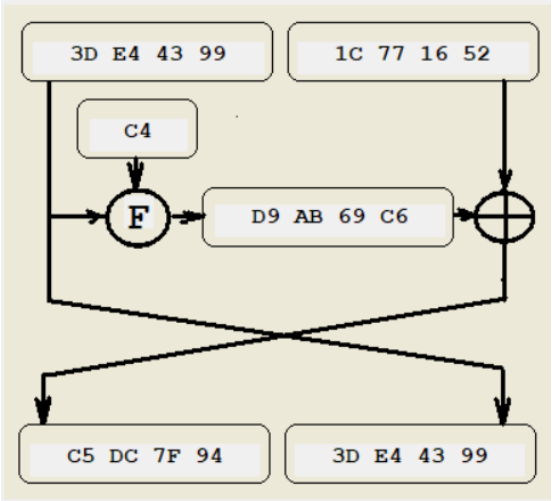

Рисунок 1.4 — Шифрование шаг 4.

Информация «3D E4 43 99 1C 77 16 52».преобразовалась с использованием функции F и раундового ключа «C4», в информацию «C5 DC 7F 94 3D E4 43 43 99».

На рисунке 1.5 показан пятый раунд цикла шифрования. Информация «C5 DC 7F 94 3D E4 43 43 99».преобразовалась с использованием функции F и раундового ключа «BA», в информацию «C3 4D F6 58 C5 DC 7F 94».

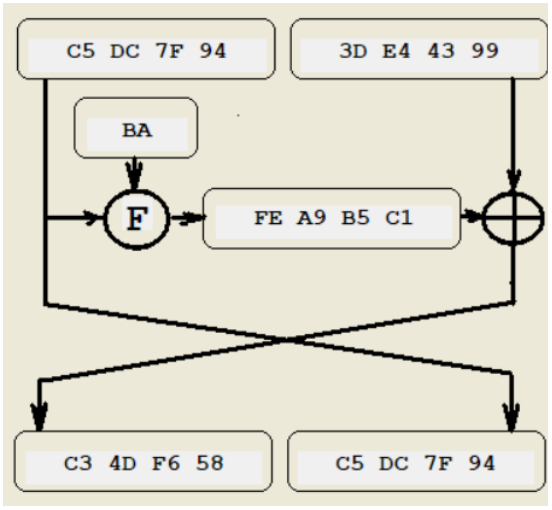

Рисунок 1.5 — Шифрование шаг 5.

На рисунке 1.6 показан шестой раунд цикла шифрования.

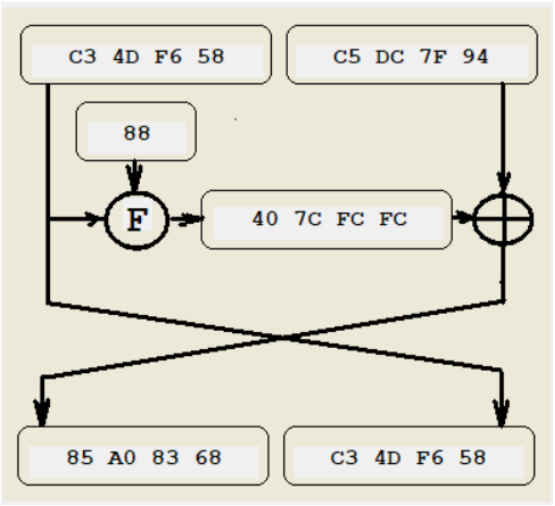

Рисунок 1.6 — Шифрование шаг 6.

Информация «C3 4D F6 58 C5 DC 7F 94» преобразовалась с использованием функции F и раундового ключа «88», в информацию «85 A0 83 68 C3 4D F6 58».

На рисунке 1.7 показан седьмой раунд цикла шифрования. Информация «85 A0 83 68 C3 4D F6 58» преобразовалась с использованием функции F и раундового ключа «42», в информацию «A2 F8 07 54 85 A0 83 68».

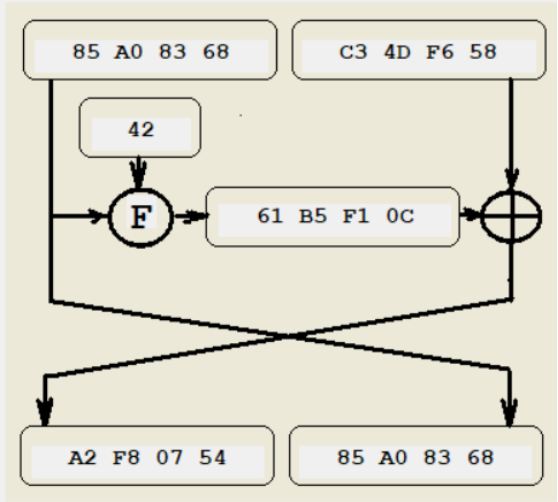

Рисунок 1.7 — Шифрование шаг 7.

На рисунке 1.8 показан последний раунд цикла шифрования. Информация «A2 F8 07 54 85 A0 83 68» преобразовалась с использованием функции F и раундового ключа «C4», в информацию «A2 F8 07 54 B7 E3 75 20». Исходная информация «67 2D 8E 3B D7 8D BD 51» преобразовалась в «A2 F8 07 54 B7 E3 75 20».

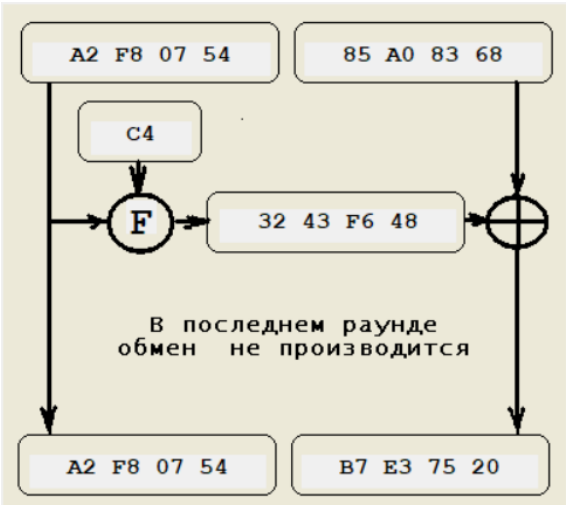

Рисунок 1.8 — Шифрование шаг 8.

2. Расшифровывание

Поскольку на последнем шаге шифрования перестановки левой и правой частей не было, то процесс расшифровки аналогичен процессу шифрования, а именно используется так же функция F и раундового ключи берутся в обратном порядке.

На рисунке 2.1 показан первый раунд цикла расшифровки.

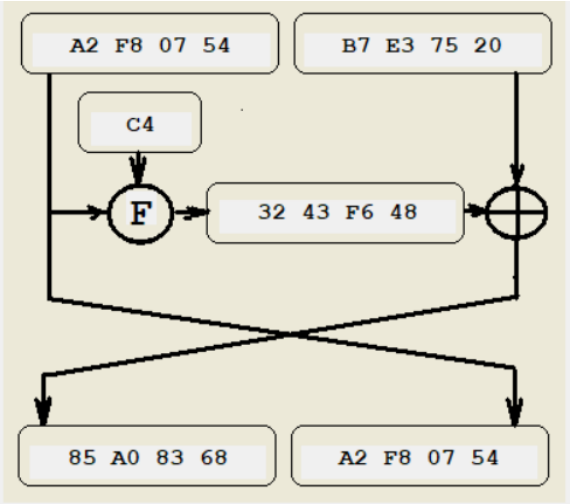

Рисунок 2.1 — Расшифровывание шаг 1.

Информация «A2 F8 07 54 B7 E3 75 20» преобразовалась с использование функции F и раундового ключа «C4», в информацию «85 A0 83 68 A2 F8 07 54».

На рисунке 2.2 показан второй раунд цикла расшифровки. Информация «85 A0 83 68 A2 F8 07 54» преобразовалась с использование функции F и раундового ключа «42», в информацию «C3 4D F6 58 85 A0 83 68».

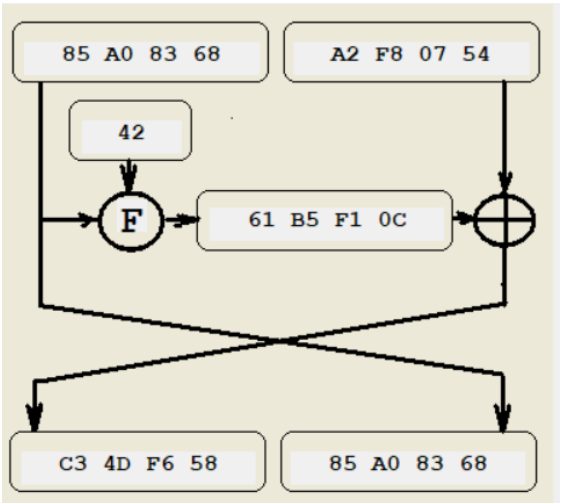

Рисунок 2.2 — Расшифровывание шаг 2.

На рисунке 2.3 показан раунд шаг цикла расшифровки.

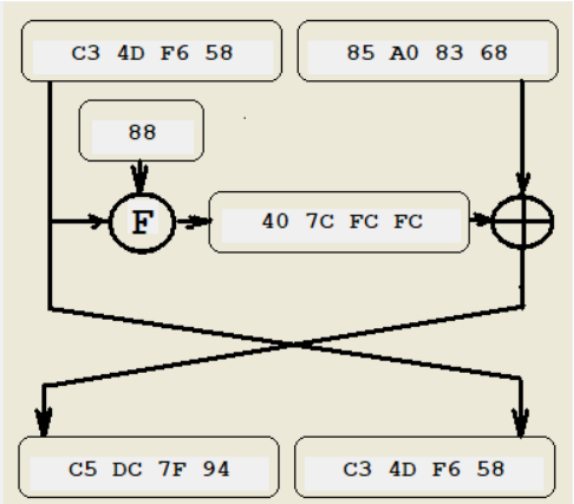

Рисунок 2.3 — Расшифровывание шаг 3.

Информация «C3 4D F6 58 85 A0 83 68» преобразовалась с использование функции F и раундового ключа «88», в информацию «C5 DC 7F 94 C3 4D F6 58»

На рисунке 2.4 показан четвёртый раунд цикла расшифровки. Информация «C5 DC 7F 94 C3 4D F6 58» преобразовалась с использование функции F и раундового ключа «BA», в информацию «3D E4 43 99 C5 DC 7F 94»

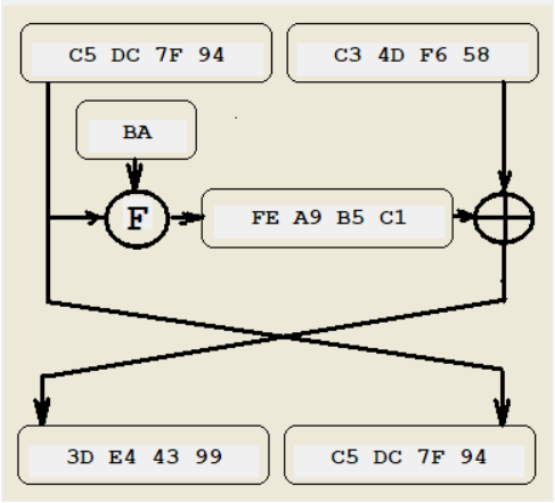

Рисунок 2.4 — Расшифровывание шаг 4.

На рисунке 2.5 показан пятый раунд цикла расшифровки. Информация «3D E4 43 99 C5 DC 7F 94» преобразовалась с использование функции F и раундового ключа «C4», в информацию «1C 77 16 52 3D E4 43 99»

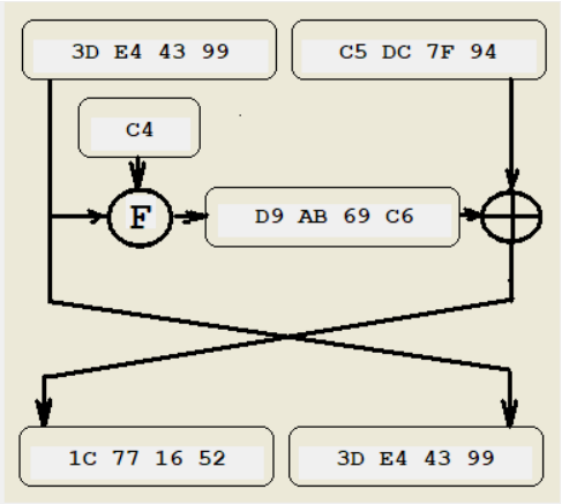

Рисунок 2.5 — Расшифровывание шаг 5.

На рисунке 2.6 показан шестой раунд цикла расшифровки. Информация «1C 77 16 52 3D E4 43 99» преобразовалась с использование функции F и раундового ключа «03», в информацию «9E EE 46 09 1C 77 16 52»

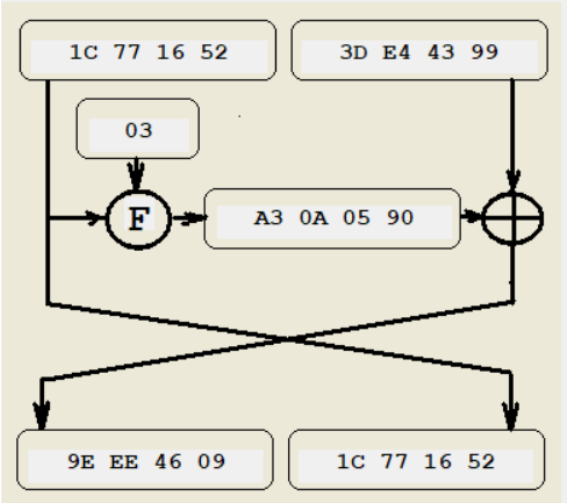

Рисунок 2.6 — Расшифровывание шаг 6.

На рисунке 2.7 показан седьмой раунд цикла расшифровки. Информация «9E EE 46 09 1C 77 16 52»преобразовалась с использование функции F и раундового ключа «C9», в информацию «67 2D 8E 3B 9E EE 46 09»

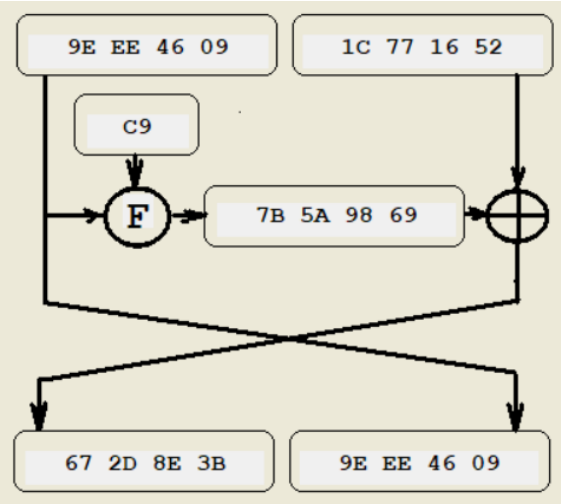

Рисунок 2.7 — Расшифровывание шаг 7.

На рисунке 2.8 показан последний раунд цикла расшифровки.

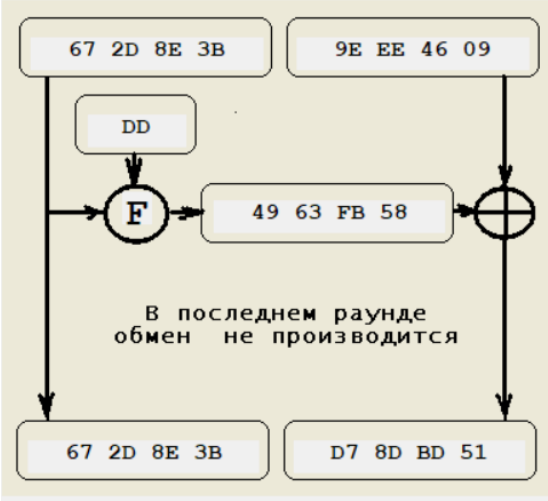

Рисунок 2.8 — Расшифровывание шаг 8.

Информация «67 2D 8E 3B 9E EE 46 09» преобразовалась с использование функции F и раундового ключа «C9», в информацию «67 2D 8E 3B D7 8D 51» Полученная информация совпадает с исходной.

3. Поиск общей функции F

3.1. Порядок поиска

Во время поиска функции F было рассмотрено несколько моделей и лишь последняя из них могла и привела к должному результату. Опишу кратко последовательность действий, которая привела к нахождению функции F.

Вне сомнения первым шагом было исследование функции F(L, K), где K=0. На первых трёх наборах, знания L и F в двоичном представлении имело равное число единиц. Первое значение это L в двоичной записи, второе – F.

а) 00001010010100111010010111010001; 00110100010110100110000110101010

б) 01110110111010101100110100011100; 10011001110000110100111010111101

в) 00010110000011111000101111001011; 01110001110110011110001001100001

Таким образом было выдвинуто предположение, что нулевой раундовый ключ исключает алгоритм замены и остается лишь перестановка. Задача свелась к поиску этого алгоритма перестановки. Были найдены дополнительные пары L и F(L, K), где K = 0. Затем записаны все значения L, а после соответствующие значения F. Таким образом нужно было найти соответствие столбцов, которые обязаны были быть уникальными, для однозначного определения алгоритма, именно поэтому первых трёх пар L и F было не достаточно. Найденная перестановка представлена на рисунке 3.1.

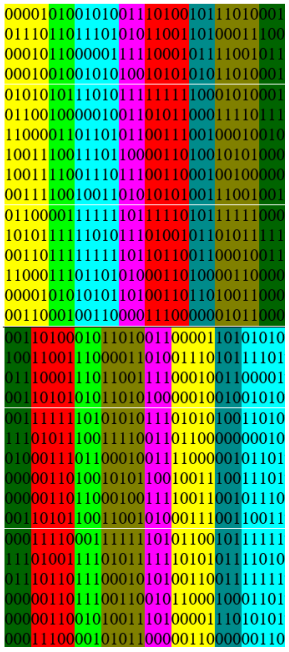

Рисунок 3.1 — Алгоритм перестановки.

Затем было решено исследовать функцию F, когда раундовый ключ является степенью 2. Т.е. в двоичной записи присутствует одна единица. Больше всего наборов было найдено для ключа K=20(hex). Для выделенных групп по алгоритму перестановки можно заметить одинаковую разницу. Однако в некоторых случаях разница отличается, что говорит о переносе значений в старший разряд между группами. На рисунке 3.2 показан промежуточный шаг определения алгоритма замены в функции F.

Рисунок 3.2 — Поиска замены.

Можно заметить, что перенос разрядов происходит не только между двумя группами (по 3 и 5 разрядов). Например в 4 наборе произошёл перенос из тёмно-голубой группы в красную. На других наборах значений L и F(L, K), где K – степень двойки, были найдены дополнительные переносы разрядов. На основе чего был получен алгоритм перестановки, представленный на рисунке 3.3.

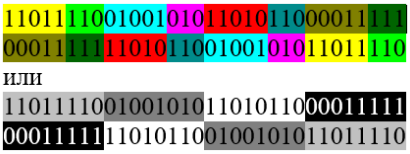

Рисунок 3.3 — Алгоритм перестановки до замены.

Затем была составлена строка, по которой происходит замена между двумя алгоритмами перестановки. Алгоритм замены по найденной строке представлен на рисунке 3.4.

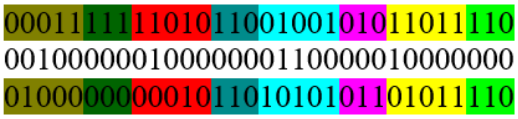

Рисунок 3.4 — Алгоритм замены.

Использовался раундовый ключ K = 00100000 (bin). Не трудно заметить, что строка замены была получена следующим образом: в четвёртом байте записывается ключ, во третьем – ключ со сдвигом влево на 1 разряд, во втором – сумма ключа и его сдвига влево на 1 разряд, в первом – ключ со сдвигом влево на 2 разряда. После этой замены происходит перестановка в состояние, найденное для ключа K=0, перестановка представлена на рисунке 3.5.

Рисунок 3.5 — Алгоритм перестановка после замены.

На других наборах L, F(L, K) и K были отмечены несколько особенностей. При составлении строки для замены происходит перенос разрядов между байтами и все промежуточные сдвиги раундового ключа складываются между собой, а переноса от старшего бита нет т.е. выполняется сумма по модулю 2^{32}.. При наложении строки замены с L после первой перестановки, происходит перенос разрядов между байтами (было определено при подборе алгоритма замены), а разряды при переносе от старшего бита теряются т.е. выполняется сумма по модулю 2^{32}.

Была найдена общая функция F представляющая собой последовательность перестановки, замены по ключу и перестановки.

3.2. Краткое описание функции на примере её проверки

Проверим функцию F для раунда представленного на рисунке 1.2. L = 9E EE 46 09 (hex). K = C9 (hex).

На первом шаге происходит перестановка по байтам: L` = 09 46 EE 9E (hex) = 00001001010001101110111010011110 (bin).

Затем составляется строка по раундовому ключу K = 11001001 (bin) как сумма 5 значений по модулю 2^{32}:

11001001|00000000|00000000|00000000 K<<24
00000001|10010010|00000000|00000000 K<<17
00000000|00000001|10010010|00000000 K<<9
00000000|00000000|11001001|00000000 K<<8
00000000|00000000|00000011|00100100 K<<2
11001010|10010100|01011110|00100100 K`

K`=(K<<24)+(K<<17)+(K<<9)+(K<<8)+(K<<2) (mod 2^{32})

На втором шаге происходит замена как сумма L` и K` по модулю 2^{32}:

00001001|01000110|11101110|10011110 L`
11001010|10010100|01011110|00100100 K`
11010011|11011011|01001100|11000010 L`` = L`+K` (mod 2^{32})

На третьем шаге происходит перестановка L``:

11010011111011011010011001100001010 L``
01111011010110101001100001101001 F

F(L, K) = 01111011010110101001100001101001 (bin) = 7B 5A 98 69 (hex)

Заключение

Раундовый ключ это последовательность из 8 бит, в то время общий ключ сети Фейстеля определяется последовательность 64 бит. Поэтому число ключей: $2^{64} \approx 1{,}8 \cdot 10^{19}$.