# ЗАДАНИЕ 1

Найти значение входного вектора данных после прохождение через преобразование P-box.

P-box

25 61 21 45 23 9 24 62

36 48 39 20 17 38 6 37

22 53 54 35 12 7 51 29

32 43 27 41 44 28 3 10

46 40 47 2 31 55 14 49

19 8 58 16 26 63 13 50

4 34 33 52 42 0 57 30

11 56 18 1 59 5 60 15

Значение входного вектора: 0x0a16df83c09675ac88ad907012d093a2

Так как размерность p-box 64 бита, а длина входного вектора бит, то разделим его на два блока: 0x0a16df83c09675ac и 0x88ad907012d093a2.

Выполним преобразование для первого блока.

Переведём в двоичное представление: 0000101000010110110111111000001111000000100101100111010110101100.

Переставим значения двоичного вектора согласно заданной перестановке.

0 1 1 1 1 0 1 0

0 0 0 1 1 0 1 0

1 1 0 0 0 0 1 0

1 1 0 0 0 0 0 0

1 1 0 0 1 1 1 1

1 0 1 1 0 0 1 1

1 0 1 0 0 0 0 1

1 1 0 0 0 0 1 0

Запишем в виде строки: 0111 1010 0001 1010 1100 0010 1100 0000 1100 1111 1011 0011 1010 0001 1100 0010.

Переведём обратно в шестнадцатеричное значение: 0x7A1AC2C0CFB3A1C2.

Выполним преобразование для второго блока.

Переведём в двоичное представление: 1000100010101101100100000111000000010010110100001001001110100010.

Переставим значения двоичного вектора согласно заданной перестановке.

1 0 0 0 0 0 0 1

0 1 0 0 0 1 0 0

0 0 1 1 1 0 1 0

0 1 1 1 0 0 0 1

0 1 0 0 0 1 0 0

1 1 1 1 1 0 1 0

1 0 0 0 0 1 0 0

0 1 0 0 0 0 0 1

Запишем в виде строки: 1000 0001 0100 0100 0011 1010 0111 0001 0100 0100 1111 1010 1000 0100 0100 0001

Переведём обратно в шестнадцатеричное значение: 0x81443A7144FA8441.

Окончательно получим 0x7A1AC2C0CFB3A1C281443A7144FA8441

# ЗАДАНИЕ 2

Определить корректный (логичный, согласно представленному преобразованию) размер входного и выходного значений и выполнить преобразование S-box.

S-box

13 5 12 6 14 9 10 15 3 2 0 8 7 11 1 4

2 8 3 9 13 15 2 1 6 4 5 7 14 0 10 11

15 10 4 6 5 13 9 11 12 14 3 1 0 8 2 7

15 5 14 11 10 6 12 0 4 2 3 8 9 1 13 7

Значение входного вектора: 0x0a16df83c09675ac88ad907012d093a2

Так как размер s-box 64, то размер входного значения 6 бит.

Так как максимальное значение в s-box 15, то размер выходного значения 4 бита.

То есть это сжимающий s-box.

Переведём входной вектор в двоичное представление: 00001010000101101101111110000011110000001001011001110101101011001000100010101101100100000111000000010010110100001001001110100010.

Поделим на подвектора по 6 бит. Перед этим нужно убедиться, что длина вектора кратна 6, и если это не так, то дописать нули в начале. В данном случае допишем 4 нуля.

000000 001010 000101 101101 111110 000011 110000 001001 011001 110101 101011 001000 100010 101101 100100 000111 000000 010010 110100 001001 001110 100010

Переведём в десятеричные числа: 0 10 5 45 62 3 48 9 25 53 43 8 34 45 36 7 0 18 52 9 14 34.

Проведём замену согласно s-box: 13 0 9 8 13 6 15 2 4 6 1 3 4 8 5 15 13 3 10 2 1 4.

Переведём в четырёхзначные двоичные числа: 1101 0000 1001 1000 1101 0110 1111 0010 0100 0110 0001 0011 0100 1000 0101 1111 1101 0011 1010 0010 0001 0100.

Переведём полученный вектор в шестнадцатеричное значение: 0xD098D6F24613485FD3A214.