Размер блока 128 = 16 \* 8 бит. Размер ключа 512 = 16 \* 16 бит. Число основных шагов – 32. Ключ является массивом из восьми 64-битовых элементов кода (64-разрядные целые числа без знака). Ключ делится на 8 частей по 64 бита (i от 0 до 7).

|  |  |
| --- | --- |
| # Алгоритм **шифрования** для ЛР5  1. Блок данных делится пополам:       **DATA** [128] -> [64] + [64]  2. Определяется подключ раунда в соответствии с последовательностью из ГОСТа. Для зашифрования это 32-З: 0-7, 0-7, 0-7, 7-0. Правая часть складывается по модулю 264 с подключом (т.е. простое сложение).  **KEY** [512] -> делится на массив из 8 подключей по [64] бита                  temp = Ki ^ Ri-1          3. 64-битный блок делится на 16 подблоков по 4 бита. Каждый подблок заменяется по таблице замен, размер которой [16] x [16] (число блоков x 2^(размер блока в битах)).           Строка = номер блока.          Столбец = значение Si как числа от 0 до 15.  4. Объединение 16 подблоков в один 64-битный блок. Побитовый циклический сдвиг влево на 11.                  temp = temp << 11          5. Сложение по модулю 2^64 результата предыдущего шага с нетронутой доселе старшей частью блока данных L:          temp = temp ^ Li-1  6. Запись в R числа temp, а в старшую часть нового числа изначальное R.                  Ri = temp         Li = Ri-1 | # Алгоритм **расшифрования** для ЛР5  1. На вход функции расшифрования подаётся Li и Ri. Поскольку Li = Ri-1, то заменив R в алгоритме шифрования на L, получим изначальное значение |