**Математическая постановка задачи**

**Формула для зашифровки текстовых данных с помощью алгоритма XOR:**

### Логическая операция исключающее ИЛИ (XOR).

Обозначение XOR: ^  
Логическая операция исключающее ИЛИ выполняется с двумя битами (a и b). Результат выполнения логической операции XOR будет равен 1 (единице), если один из битов a или b равен 1 (единице), во всех остальных случаях, результат равен 0 (нулю). Смотрим таблицу истинности логической операции исключающее ИЛИ.

|  |  |  |
| --- | --- | --- |
| **a(бит 1)** | **b(бит 2)** | **a(бит 1) ^ b(бит 2)** |
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Таблица 1.

**Формула для зашифровки текстовых данных с помощью алгоритма DES: (Приводить существенную часть кода здесь я не буду т.к. не вижу в этом особого смысла. Поэтому покажу основную функцию Фейстеля которую я использовал и приведу схему шифрования алгоритма des)**

**Основная Формула метода Des:**

Таблица 1: ***Матрица начальной перестановки IP***

58 50 42 34 26 18 10 02

60 52 44 36 28 20 12 04

62 54 46 38 30 22 14 06

64 56 48 40 32 24 16 08

57 49 41 33 25 17 09 01

59 51 43 35 27 19 11 03

61 53 45 37 29 21 13 05

63 55 47 39 31 23 15 07

Затем выполняется шифрование, состоящее из 16 итераций. Результат i-й итерации описывается следующими формулами:

|  |
| --- |
| L(i) = R(i-1)  R(i) = L(i-1) xor f(R(i-1), K(i)) , |

где xor - операция ИСКЛЮЧАЮЩЕЕ ИЛИ

**Объяснение Начальной перестановки**

Исходный текст {\displaystyle T}T (блок 64 бит) преобразуется c помощью начальной перестановки {\displaystyle \mathrm {IP} }IP которая определяется таблицей:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Начальная**[**перестановка**](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B0)**IP** | | | | | | | | | | | | | | | |
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 | 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 | 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 | 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 | 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

Таблица 2.

По таблице первые 3 бита результирующего блока {\displaystyle \mathrm {IP} (T)}IP(T) после начальной перестановки {\displaystyle \mathrm {IP} }IP являются битами 58, 50, 42 входного блока T{\displaystyle T}rr, а его 3 последние бита являются битами 23, 15, 7 входного блока

### Основная функция шифрования (функция Фейстеля)

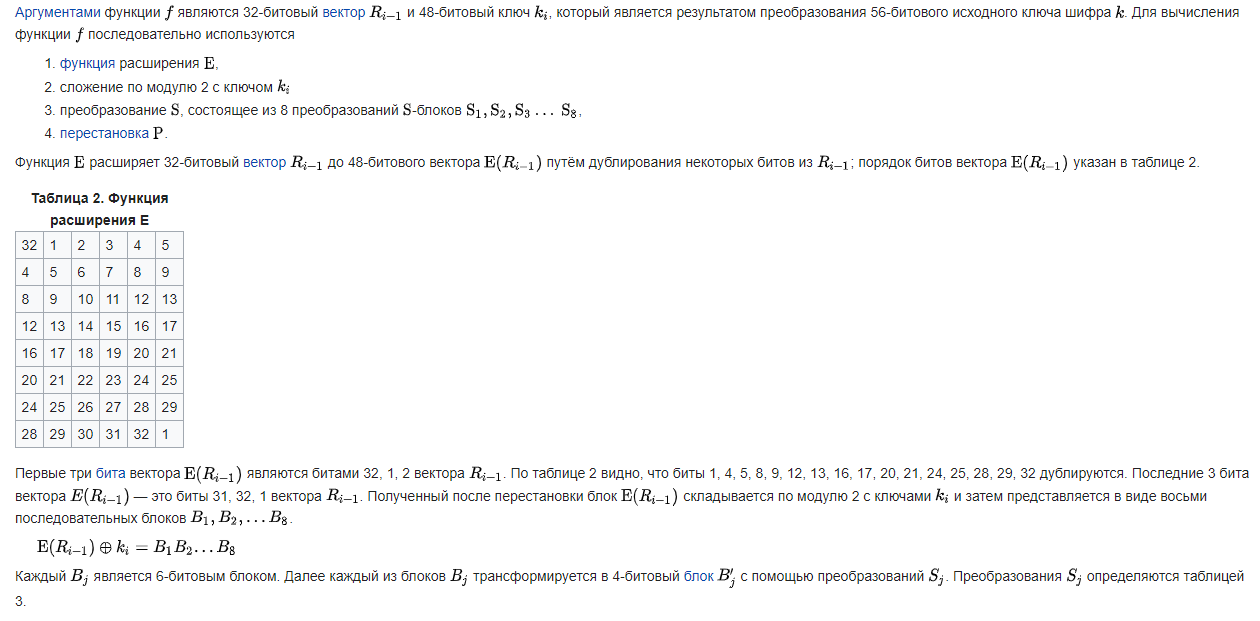


Рис 1.

Источники:

1. <https://ru.bmstu.wiki/DES_(Data_Encryption_Standard)>

2.<https://ru.wikipedia.org/wiki/DES>

3.<https://www.intuit.ru/studies/courses/691/547/lecture/12377?page=2>

4. <http://protect.htmlweb.ru/des.htm>