**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