**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 |

for (int i = 0; i < inputLength + 1; ++i)

{

Output = input ^ key[ i % keyLenght + 1];

}

где,

* input – массив char с исходными данными,
* inputLength – массив с исходными данными,
* key – ключ в виде массива char,
* keyLength – длинна ключа,
* output – массивы с исходными данными

Здесь я беру индекс вводимых данных и степень ключа по модулю + длины ключа. И на выходе получаю зашифрованные данные. Метод расшифровки идентичен.

**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 концепция метода Des:**

### Двухкратный DES и атака "встреча посередине"(с использованием мат.формулы)

В настоящее время основным недостатком *DES* считается маленькая *длина ключа*. Простейшим способом усложнения процесса криптоанализа является использование *двухкратного шифрования* с помощью одного и того же алгоритма с разными ключами. Если М – сообщение, К1, К2 – *ключ*, f – процесс шифрования по *DES*, а Е – зашифрованное сообщение, то можно записать

E=f(f(M,K1),K2),

то есть сначала блок шифруется одним ключом, затем получившийся шифротекст шифруется вторым ключом. *Расшифрование* проводится в обратном порядке ( f -1 – *расшифрование* по *DES* ):

E=f-1(f-1(E,K2),K1)

В этом случае *длина ключа* равна 56 \* 2 = 112 *бит*, поэтому для обнаружения двойного ключа, которым зашифрован блок, потребуется в общем случае 2112 попыток.

Исследовав эту проблему, американские ученые Меркл и Хеллман придумали способ проведения атаки по открытому тексту, который требует проведения не 2112 попыток, а 257. (Меркл и Хеллман предложили эту схему против *DES*, но можно сделать *обобщение* на все блочные алгоритмы.)

Этот вариант атаки называется *атака "встреча посередине"*. Он основан на следующем свойстве алгоритма. Мы имеем

E=f(f(M,K1),K2)

где М – сообщение, К1, К2 – *ключ*, f – процесс шифрования по *DES*, а Е – зашифрованное сообщение.

Тогда X=f(M,K1)=f-1(E,K2).

Исходный текст — блок 64 бит.

Процесс шифрования состоит из начальной перестановки, 16 циклов шифрования и конечной перестановки.

**Начальная перестановка**

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Таблица. 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 |

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)

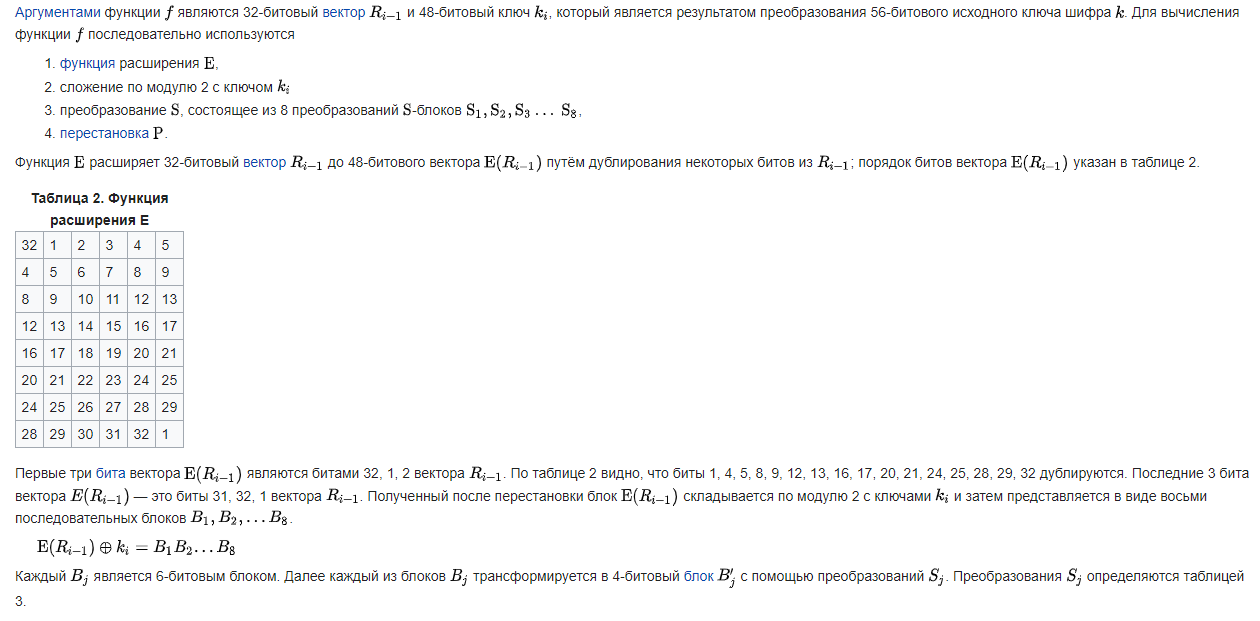


Рис1.

Источники:

1.<http://cppstudio.com/post/500/>

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

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