

# Алгоритм шифрования ~~DES~~

DES – блочный алгоритм, то есть при шифровании исходное сообщение переводится в двоичный код, а затем разбивается на блоки и каждый блок отдельно зашифровывается (расшифровывается). По стандарту (принят в 1977 году) размер блока DES равен 64 бита, то есть используя 8-ми битовую кодировку ASCII, применяемую в те времена, получим в одном блоке – 8 символов.

Теперь же в основном используется 16-ти битная кодировка Юникода (UTF-16), поэтому, чтобы сохранить длину блока равную 8-ми символам, увеличим размер блока DES до 128 бит.

---

# Алгоритм DES.

## Шаги

Итак, для того, чтобы зашифровать сообщение алгоритмом DES, необходимо выполнить следующую последовательность шагов:

довести исходное сообщение до такого размера (в битах), чтобы оно нацело делилось на размер блока (sizeofBlock = 128 бит);

разделить исходное сообщение на блоки

довести длину ключа до длины половины блока

перевести ключ в бинарный формат (в нули и единицы);

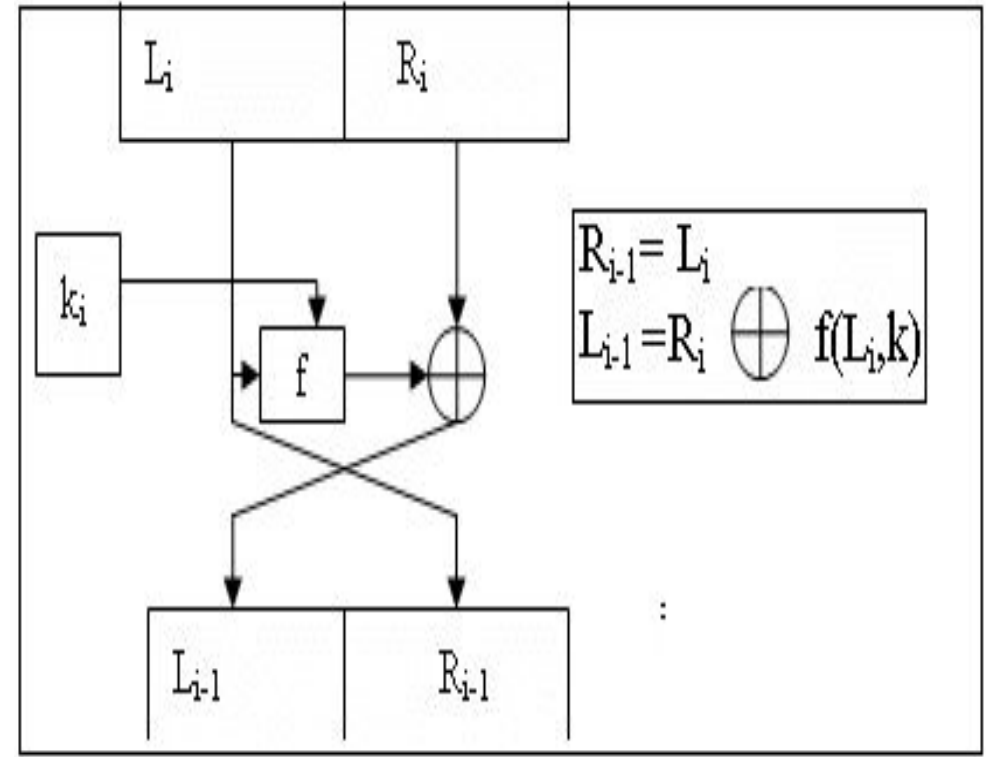
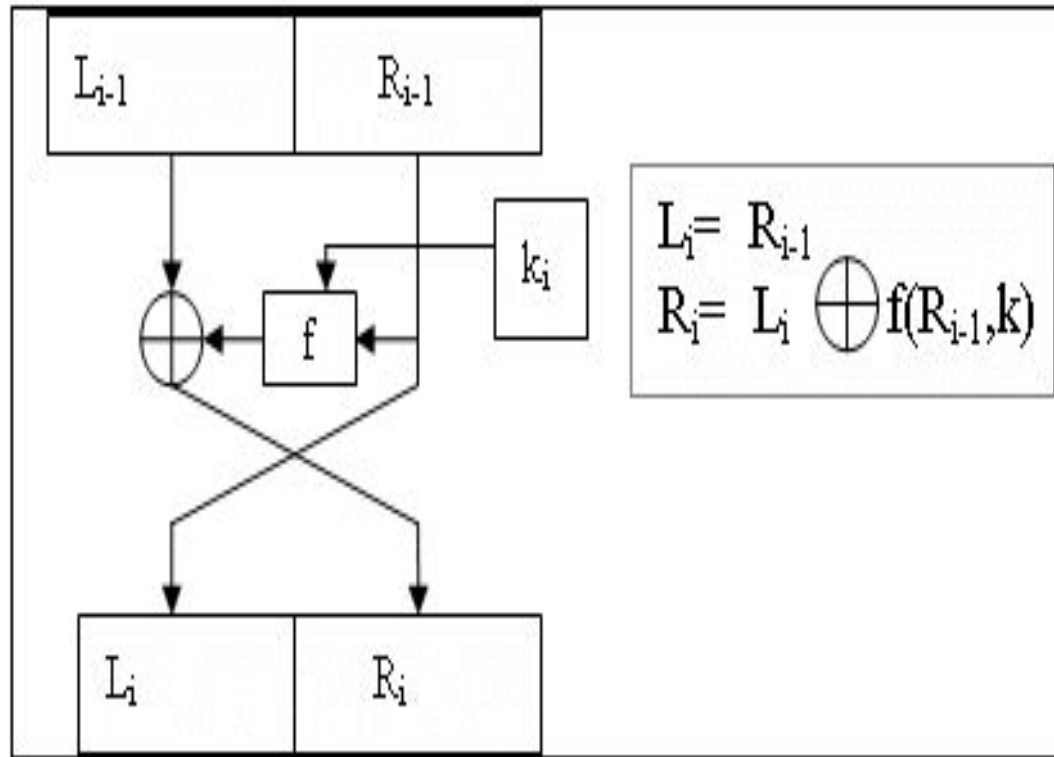
провести над каждым блоком прямое преобразование сетью Фейстеля в течении 16-ти раундов. После каждого раунда необходимо выполнять циклический сдвиг ключа на заданное количество символов);

соединить все блоки вместе; таким образом получим сообщение, зашифрованное алгоритмом DES.);

# Алгоритм DES.

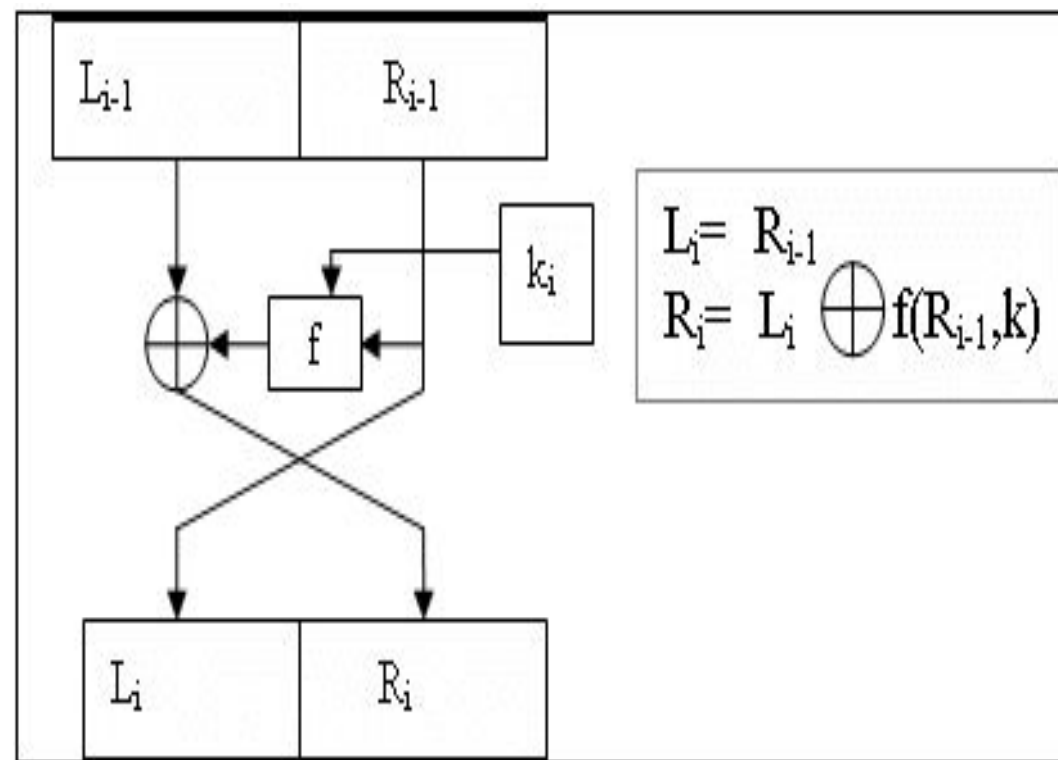
## Сеть Фейстеля

Сеть Фейстеля используется в алгоритме DES для зашифрования (прямое преобразование сетью) и расшифрования (обратное преобразование). Эти преобразования изображены на рисунках 1 и 2 соответственно.



Рассмотрим один раунд прямого преобразования сетью Фейстеля.

На  $i$ -й итерации исходный блок делится пополам – левая часть обозначается  $L$ , правая  $R$ . Над  $R$  и ключом  $k_i$  вычисляется какая-либо выбранная логическая функция  $f$  (мы будем использовать XOR). Затем выполняется вычисление логической операции “исключающее или” над  $L$  и вычисленным ранее значением функции ( $L \text{ xor } f$ ). Старое значение  $R$  переносится в левую часть блока, а в правую часть заносится значение  $L \text{ xor } f$ . И последняя операция раунда – нужно выполнить циклический сдвиг ключа:  $\text{key}_{i+1} = \text{key}_i \gg \text{shiftKey}$  (при расшифровке  $\text{key}_{i-1} = \text{key}_i \ll \text{shiftKey}$ );  $\text{shiftKey}$  – количество символов, на которое необходимо циклически сдвинуть ключ.



# Задание

создать программную реализацию криптографической системы, основанной на алгоритме шифрования DES, которая должна быть оформлена как некоторая программная оболочка.

В программной реализации должен быть разработан интерфейс, удобный для эксплуатации программы, в интерфейсе следует предусмотреть:

1. Два режима формирования ключа – ключ задан, ключ формируется по умолчанию;
2. Ввод начальной информации из сформированного заранее файла и из файла, который создается в оболочке программы;
3. Режимы шифрования, которые предусмотрены в DES;

# Шифрование по алгебре матриц

***ЗАШИФРОВАТЬ СЛОВО ВАСИЛЬЕВА***

***Ключ: матрица***

	1	2	3
A=	0	5	6
	4	2	1

1. Задаем нумерацию букв в шифруемом слове в соответствии с порядковым номером в алфавите (т.е. буква А имеет номер 1, буква Б – 2, буква В 3 и т.д.)

**В А С И Л Ь Е В А**

**3 1 19 10 13 30 6 3 1**

2. Умножаем матрицу на вектор

$$C1 = \begin{vmatrix} 1 & 2 & 3 \\ 0 & 5 & 6 \\ 4 & 2 & 1 \end{vmatrix} * \begin{vmatrix} 3 \\ 1 \\ 19 \end{vmatrix} = \begin{vmatrix} 1*3 + 2*1 + 3*19 \\ 0*3 + 5*1 + 6*19 \\ 4*3 + 2*1 + 1*19 \end{vmatrix} = \begin{vmatrix} 62 \\ 119 \\ 33 \end{vmatrix}$$

**Т.е. буква В это 62, буква А это 119, буква С это 33**



Те же самые действия проделываем с другими буквами

$$C2 = \begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline \end{array} * \begin{array}{|c|} \hline 10 \\ \hline \end{array} = \begin{array}{|c|} \hline 1*10+2*13+3*30 \\ \hline \end{array} = \begin{array}{|c|} \hline 126 \\ \hline \end{array}$$
$$\begin{array}{|c|c|c|} \hline 0 & 5 & 6 \\ \hline \end{array} * \begin{array}{|c|} \hline 13 \\ \hline \end{array} = \begin{array}{|c|} \hline 0*10+5*13+6*30 \\ \hline \end{array} = \begin{array}{|c|} \hline 245 \\ \hline \end{array}$$
$$\begin{array}{|c|c|c|} \hline 4 & 2 & 1 \\ \hline \end{array} * \begin{array}{|c|} \hline 30 \\ \hline \end{array} = \begin{array}{|c|} \hline 4*10+2*13+1*30 \\ \hline \end{array} = \begin{array}{|c|} \hline 96 \\ \hline \end{array}$$

⊕

$$C3 = \begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline \end{array} * \begin{array}{|c|} \hline 6 \\ \hline \end{array} = \begin{array}{|c|} \hline 1*6+2*3+3*1 \\ \hline \end{array} = \begin{array}{|c|} \hline 15 \\ \hline \end{array}$$
$$\begin{array}{|c|c|c|} \hline 0 & 5 & 6 \\ \hline \end{array} * \begin{array}{|c|} \hline 3 \\ \hline \end{array} = \begin{array}{|c|} \hline 0*6+5*3+6*1 \\ \hline \end{array} = \begin{array}{|c|} \hline 21 \\ \hline \end{array}$$
$$\begin{array}{|c|c|c|} \hline 4 & 2 & 1 \\ \hline \end{array} * \begin{array}{|c|} \hline 1 \\ \hline \end{array} = \begin{array}{|c|} \hline 4*6+2*3+1*1 \\ \hline \end{array} = \begin{array}{|c|} \hline 31 \\ \hline \end{array}$$

3. Записываем ответ

$$T = [62 \ 119 \ 33 \ 126 \ 245 \ 96 \ 15 \ 21 \ 31]$$

ЗАШИФРОВАТЬ ФРАЗУ

**1 ВАРИАНТ**

ВАЛЛИУЛОВ ТИМУР РУСТАМОВИЧ

Ключ: матрица

$$A = \begin{vmatrix} 10 & 3 & 2 & 1 \\ 5 & 6 & 7 & 3 \\ 4 & 2 & 1 & 0 \\ 5 & 1 & 6 & 7 \end{vmatrix}$$

ГАВРИЛОВА ЛАРИСА АЛЕКСАНДРОВНА

Ключ: матрица

$$A = \begin{vmatrix} 0 & 8 & 5 \\ 7 & 5 & 4 \\ 0 & 3 & 6 \end{vmatrix}$$

---

---

## 2 ВАРИАНТ

МАДИЛОВ АРТЁМ СЕРГЕЕВИЧ

Ключ: матрица

$$A = \begin{vmatrix} 1 & 2 & 5 \\ 4 & 7 & 8 \\ 0 & 5 & 1 \end{vmatrix}$$

АРСЕНОВА ЛИЛЯ ФРАНЦЕВНА

Ключ: матрица

$$A = \begin{vmatrix} 5 & 4 & 8 \\ 7 & 2 & 1 \\ 0 & 6 & 2 \end{vmatrix}$$