

# Отчёт по Лабораторной Работе

## **«Аффинная система перестановок Цезаря»**

Выполнил: Кремер Илья, НИ-501

Преподаватель: Кулябов Дмитрий Сергеевич

Москва, РУДН – 2012

## Название и цель работы

Шифр Цезаря. Аффинная система перестановок Цезаря. Разобраться в алгоритме, привести пример реализации.

## Описание алгоритма

Способ шифрования, рассматриваемый в этой работе основывается на отображении каждого символа исходного текста в некоторый другой из того же алфавита. Формула, по которой шифруется каждый символ, выглядит следующим образом:

$$y = (K \cdot x + A) \bmod N$$

Где  $x$  – позиция шифруемого символа в алфавите,  $N$  – количество символов в алфавите,  $K$  и  $A$  – два числа, которые составляют ключ,  $y$  – полученная позиция символа в зашифрованном тексте.

Чтобы зашифровать текст, необходимо применить данную формулу ко всем символам из текста, для символов, которых нет в алфавите, можно не применять формулу.

Чтобы расшифровать текст, необходимо применить формулу:

$$x = (K^{-1} \cdot (y + N - A)) \bmod N$$

Где  $y$ ,  $N$ ,  $A$  – значения из формулы шифрования, а  $K^{-1}$  – обратное число для  $K$  (по модулю  $N$ ). Напомним, что обратное число  $K^{-1}$  по модулю  $N$ , это такое число, что

$$(K^{-1} \cdot K) \bmod N = 1$$

Стоит заметить, что данный алгоритм накладывает некоторые ограничения на входные данные:

1.  $K$  и  $A$  не могут быть отрицательными
2.  $K$  не должно быть равным нулю
3.  $K$  и  $N$  должны быть взаимно простыми числами

Всё дело в том, что отображение должно быть однозначным. Ситуация, когда два различных символа из текста шифруются одинаково, недопустима, ведь в таком случае правильная расшифровка станет невозможной – произойдёт потеря данных.

В связи с последним ограничением становится удобно использовать такой алфавит, чтобы количество его символов было простым числом. Тогда можно использовать больше различных ключей.

Шифр Цезаря – это частный случай такого способа шифрования, когда  $K$  равна единице, а  $A$  – трём.

## Реализация алгоритма

Реализуем алгоритм на JavaScript. Для этого создадим страничку с формой, в которую можно будет вводить алфавит, ключ и тексты.

```
var n = this.alphabet.value.length;
var text = this.src.value.toLowerCase();
var encryptedT = "";
for (var i = 0; i < text.length; i++) {
    var c = text.charAt(i);
    var pos = this.alphabet.value.indexOf(c);
    if (pos < 0) {
        encryptedT += c; // не шифруем данный символ
        continue;
    }
    var newPos = (parseInt(pos) * k + a) % n;
    var newC = this.alphabet.value.charAt(newPos);
    encryptedT += newC;
}
this.dst.value = encryptedT;
```

В приведённом фрагменте кода `text` – это изначальный текст. Видно, что в данном случае регистр букв потеряется при шифровании. С другой стороны никто не мешает удваивать алфавиты. Шифрование таким способом не допускает повторяющихся символов в алфавите. Хотя это и очевидно, но в то же время требует проверки.

Дешифровка будет происходить аналогично:

```
var n = this.alphabet.value.length;
var kInverse = this.calcInverse(k, n);
var text = this.dst.value.toLowerCase();
var decryptedT = "";
for (var i = 0; i < text.length; i++) {
    var c = text.charAt(i);
    var pos = this.alphabet.value.indexOf(c);
    if (pos < 0) {
        decryptedT += c; // не шифруем данный символ
        continue;
    }
    var newPos = (kInverse * (parseInt(pos) + n - a)) % n;
    var newC = this.alphabet.value.charAt(newPos);
    decryptedT += newC;
}
this.src.value = decryptedT;
```

Напишем различные вспомогательные функции для проверки входных данных и реализация готова.

## Примеры работы

Используем сначала только латинский алфавит.

К:

A:

Зашифровать

Длина алфавита (26) и К не должны быть взаимно простыми.

Встречаемся с ограничением на входные данные. 26 и 6 являются взаимно простыми, т.к. оба делятся на 2.

Алфавит:

abcdefghijklmnopqrstuvwxyz

Исходный текст:

attack at dawn

Зашифрованный текст:

lqqlrp lq ulzy

К: 3

А: 11

Выберем другое  $K$  и зашифруем текст. Дешифровка вернёт нам правильное «attack at dawn».

Пробелы не поддались шифрованию, т.к. они не встречаются в алфавите.

Используем теперь алфавит большей длины. Возьмём 71 символ – это простое число. С таким алфавитом можно использовать любые ключи с  $K$  от 1 до 70, от 72 до 141, от 143 до 212 и т.д.

Шифрование с помощью [аффинной системы подстановок Цезаря](#)

Алфавит:

abcdefghijklmnopqrstuvwxyzабвгдеёжзийклмнопрстуфхцчщъыьэюя 0123456789-

Исходный текст:

Шифрование с помощью аффинной системы подстановок Цезаря

Зашифрованный текст:

жіјэскзліѷк2кчсёсмю9kzјіілсok2і28ьёшкчсц28злсксukѵьсзэе

K:  A:

Зашифровать

Расшифровать

Подстановка при шифровании:  $y = (K * x + A) \% n$ , где

$K$  и  $A$  задаются на форме,  $x$  – позиция шифруемого символа в алфавите, а  $n$  – количество символов в алфавите. Символы, не встречающиеся в алфавите не шифруются.

Дешифровка осуществляется по формуле  $x = (inv[K] * (y + n - A)) \% n$ , где

$inv[K]$  – такое число, что  $(inv[K] * K) \% n = 1$ .

### Ответы на теоретические вопросы

1. Какой шифр называется шифром подстановки?

Шифром **подстановки** называется шифр, в котором каждый символ заменяется на какой-либо другой. Чтобы расшифровать данные, необходимо произвести обратную подстановку.

Подстановка может быть полностью замкнута на одном и том же алфавите, т.е. каждому символу алфавита соответствует другой символ из этого алфавита. Кроме того, подстановка может производиться не только над символами, а над группами символом (последовательности соответствует

последовательность), а также для подстановки может быть использовать несколько алфавитов.

2. Какой шифр называется шифром перестановки?

Шифр, который основывается только на изменении порядка следования символов, называется **перестановочным**.

3. Какой шифр называется поворотной решёткой?

Шифрование **поворотной решёткой** – это такой способ шифрования, при котором используется решётка  $2m$  на  $2k$  клеток с  $m * k$  «пустых» клеток. Чтобы зашифровать с её помощью данные, необходимо сначала вписать в пустые клетки первые  $m * k$  букв, затем развернуть решётку на 180 градусов и снова вписать в появившиеся пустые клетки следующие символы из массива данных. Затем необходимо положить решётку на другую сторону и совершить ещё две таких же итерации.

4. Какой шифр называется шифром вертикальной перестановки?

Шифрование с помощью **вертикальных перестановок** – это частный случай маршрутной перестановки. Для этого способа используется таблица, в которой символы из массива данных вписываются обычным способом (заполняя таблицу слева направо и сверху вниз), а зашифрованное сообщение составляется путём выписывания букв по вертикали, при том, что столбцы берутся в порядке, определяемом ключом. То есть ключ – это нумерация столбцов.

5. К какому классу шифров относится шифр Цезаря?

**Шифр Цезаря** является шифром перестановок.