МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение

высшего образования

«Новосибирский национальный исследовательский государственный университет»

(Новосибирский государственный университет)

Структурное подразделение Новосибирского государственного университета –

Высший колледж информатики НГУ

КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

**Информационная безопасность ПК и КС**

«Шифратор и дешифратор»

Руководство пользователя

Научный руководитель

Родионова О.К.

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_2018 г.

Студент 3 курса, Клёц А.П.

гр. 503Б2. «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_2018 г.

Новосибирск

2018

СОДЕРЖАНИЕ

[Введение 3](#_Toc515239502)

[Установка программного продукта 3](#_Toc515239503)

[Способ запуска программного продукта 3](#_Toc515239504)

[Примечания к программному продукту 3](#_Toc515239505)

[1 Руководство пользователя 4](#_Toc515239506)

[1.1 Главное меню 4](#_Toc515239507)

[1.2 Алгоритм простой подстановки 5](#_Toc515239508)

[1.3 Алгоритм Цезаря 8](#_Toc515239509)

[1.4 Алгоритм шифрования xor 11](#_Toc515239510)

[1.5 Алгоритм простой блочной перестановки 14](#_Toc515239511)

# Введение

Вам предоставлена программа для шифрования с помощью таких видов шифрования как: алгоритм простой подстановки, алгоритм Цезаря, алгоритм xor,агоритм простой блочной перестановки.

## Установка программного продукта

Программный продукт не требует каких либо дополнительных программ для запуска. Установка или распаковка не требуются. Достаточно скопировать программу с запоминающего устройсва.

## Способ запуска программного продукта

Программный продукт запускается с иконки на рабочем столе с наименованием “ШИФРАТОР”.

## Примечания к программному продукту

При некорректном вводе исходных данных выводится сообщение об ошибке и описанием этой ошибки.

.Все результаты шифрования/расшифрования сохраняются в файл. После чего могут быть использованы как исходные данные.

# Руководство пользователя

## Главное меню

После того как вы запустили программу перед вами откроется главное меню со списком алгоритмов шифрования. У вас есть возможность выбрать алгоритм шифрования. Нажав на кнопку вы перейдете на тот алгоритм который выбрали. При нажатии на кнопку ВЫХОД программа заканчивает свою работу и закрывается. На рисунке 1 представлен скриншот гланого меню.

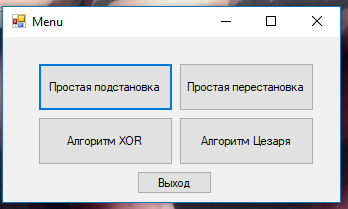


Рисунок 1

## Алгоритм простой подстановки

Для того чтобы запустить алгоритм вам нужно нажать на кнопку с названием «Шифр простой замены».

Вам откроется окно этой шифровки. На рисунке 2 представлен скриншот формы Шифр простой замены.

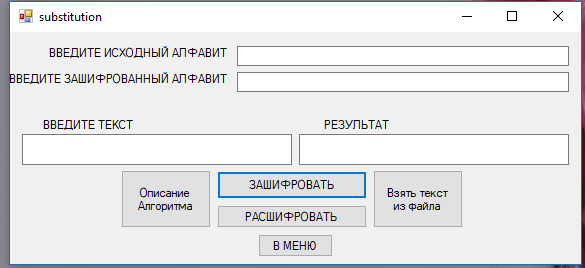


Рисунок 2

Для построения шифра простой замены необходимо выписать буквы алфавита(поле «ВВЕДИТЕ ИСХОДНЫЙ АЛФАВИТ») и под ними подписываются произвольно переставленные буквы этого алфавита, цифры или различные символы(поле «ВВЕДИТЕ ЗАШИФРОВАННЫЙ АЛФАВИТ»). Само шифрование заключается в замене букв согласно таблице. На рисунке 3 представлен скриншот того, куда нужно вводить данные.

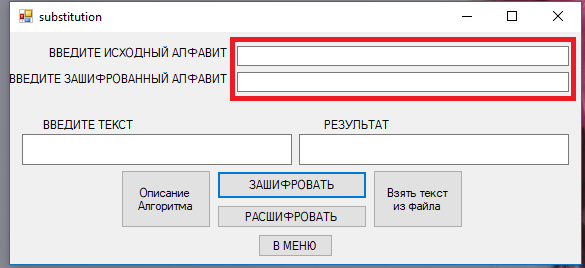


Рисунок 3

Далее неободимо в поле «Введите текст» ввести текст который будет зашифрован или расшифрован. На рисунке 4 представлен скриншот того куда нужно вводить данные.

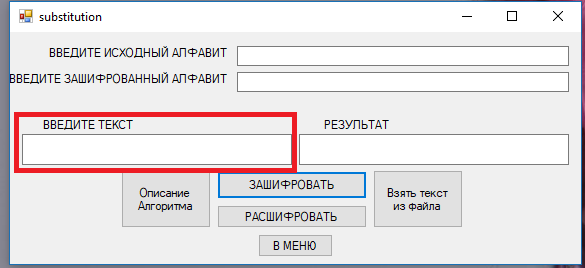


Рисунок 4

После того как исходный алфавит, зашифрованный алфавит и текст введены нужно нажать на кнопку зашифровать или расшифровать. На рисунке 5 представлен скриншот того куда нужно нажать.

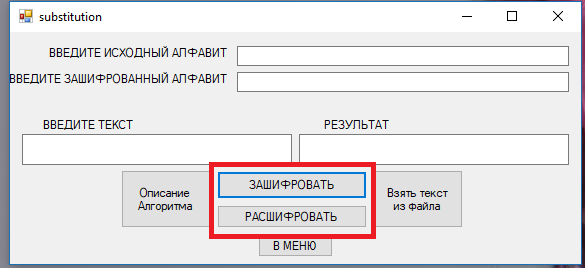


Рисунок 5

Если все исходные данные введены корректно результат зашифровки/расшифровки выведется на соотвествующем поле РЕЗУЛЬТАТ. Все результаты шифрования/расшифрования сохраняются в файл.

Если нажать на кнопку ВЗЯТЬ ТЕКСТ ИЗ ФАЙЛА, то в поле «ВВЕДИТЕ ТЕКСТ» будет записан последний результат работы программы из любого алгоритма шифрования.

Если нажать на кнопку ОПИСАНИЕ АЛГОРИТМА откроется сообщение с кратким описанием данного алгоритма шифрования.

Если нажать на кнопку «В меню» то мы перейдем в главное меню программы.

## Алгоритм Цезаря

Для того чтобы нам попасть в алгоритм цезаря нужно нажать на кнопку «Алгоритм цезаря».

При нажатии на кнопку «Алгоритм Цезаря» вам откроется окно этой шифровки. На рисунке 6 представлен скриншот формы Алгоритма Цезаря.

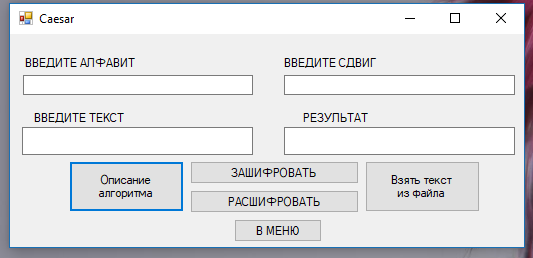


Рисунок 6

Для того зашифровать или расшифровать текст нужно ввести в поле «Введите алфавит» алфавит который будет использоваться. На рисунке 7 представлен скриншот того, куда нужно вводить данные.

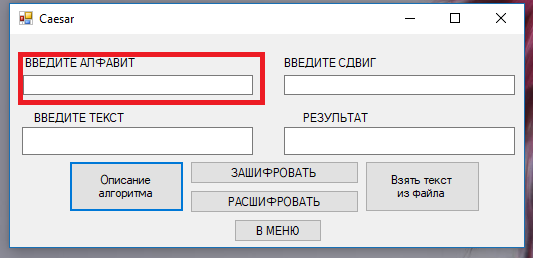


Рисунок 7

После того как вы был введен алфавит нужно ввести в поле «Введите сдвиг» на какое количество символов будет сдвигаться алфавит. Каждый [символ](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%B2%D0%BE%D0%BB) в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в [алфавите](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D1%84%D0%B0%D0%B2%D0%B8%D1%82). Например, в шифре с алфавитом «А Б В Г Д» со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, В станет А, и так далее. На рисунке 8 представлен скриншот того куда нужно вводить данные.

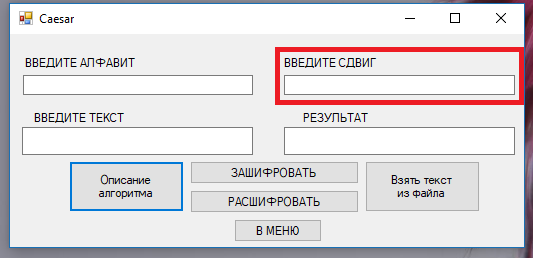


Рисунок 8

Далее неободимо в поле «Введите текст» ввести текст который будет зашифрован или расшифрован. На рисунке 9 представлен скриншот того куда нужно вводить данные.

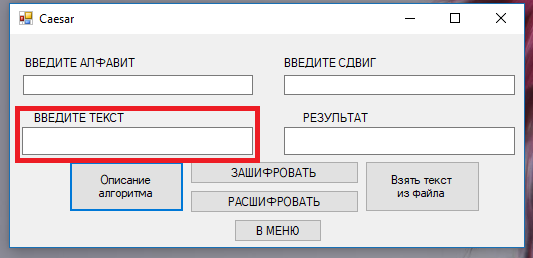


Рисунок 9

Шифрованный текст получается путём замены каждой буквы оригинального текста соответствующей буквой шифрованного алфавита

Если все исходные данные введены корректно результат зашифровки/расшифровки выведется на соотвествующем поле РЕЗУЛЬТАТ. Все результаты шифрования/расшифрования сохраняются в файл.

Если нажать на кнопку ВЗЯТЬ ТЕКСТ ИЗ ФАЙЛА, то в поле ВВЕДИТЕ ТЕКСТ будет записан результат предыдущей работы программы из любого алгоритма шифрования.

Если нажать на кнопку ОПИСАНИЕ АЛГОРИТМА откроется сообщение с кратким описанием данного алгоритма шифрования.

Если мы нажмем на кнопку «В меню» то мы перейдем в главное меню программы.

## Алгоритм шифрования xor

Для того чтобы нам попасть в алгоритм шифрования xor нужно нажать на кнопку «Алогритм xor».

При нажатии на кнопку «Алгоритм xor» откроется форма с этим алгоритмом. На рисунке 10 представлен скриншот алгоритма шифрования xor.

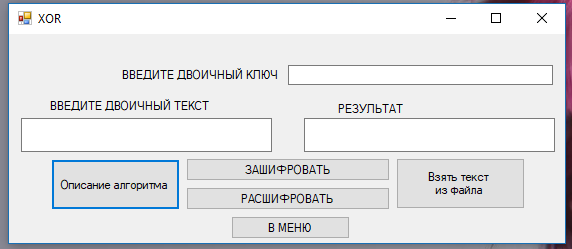


Рисунок 10

Для того зашифровать или расшифровать текст нужно ввести в поле «Введите двоичный ключ» двоичный ключ с помощью которого будет зашифровываться или расшифровываться текст. Алгоритм XOR-шифрования основан на применении бинарной логической операции исключающего или. Идея алгоритма заключается в том, что к каждому символу исходного текста и очередному символу строки пароля применяется логическая операция XOR. Например,если ввести текст 0101 и ключ 0100 то в результате получится 0010, то есть если символ ключа и текста совпадают то в результат записывется 0, в противном случае записывается 1. На рисунке 11 представлен скриншот, того куда нужно вводить.

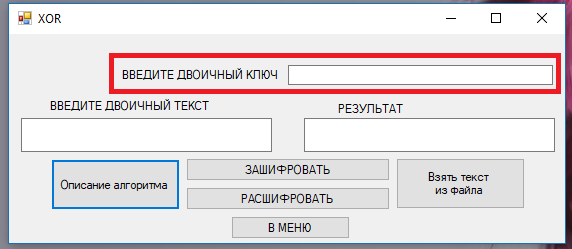


Рисунок 11

После того как был введен ключ нужно ввести в поле «Введите двоичный текст» текст который нужно зашифровывать или расшифровывать, текст должен быть двоичный. На рисунке 12 представлен скриншот, того куда нужно вводить.

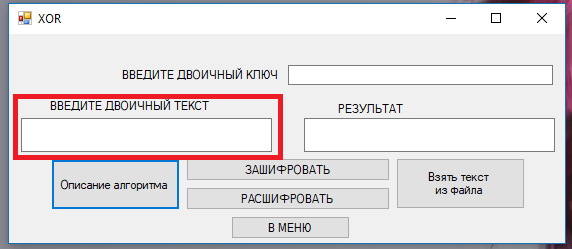


Рисунок 12

Если все исходные данные введены корректно результат зашифровки/расшифровки выведется на соотвествующем поле РЕЗУЛЬТАТ. Все результаты шифрования/расшифрования сохраняются в файл.

Если нажать на кнопку ВЗЯТЬ ТЕКСТ ИЗ ФАЙЛА, то в поле ВВЕДИТЕ ТЕКСТ будет записан результат предыдущей работы программы из любого алгоритма шифрования.

Если нажать на кнопку ОПИСАНИЕ АЛГОРИТМА откроется сообщение с кратким описанием данного алгоритма шифрования.

Если мы нажмем на кнопку «В меню» то мы перейдем в главное меню программы.

## Алгоритм простой блочной перестановки

Для того чтобы нам попасть в алгоритм простой перестановки нужно нажать на кнопку «Простая перестановка».

При нажатии на кнопку «Простая перестановка» откроется форма с этим алгоритмом. На рисунке 13 представлен скриншот алгоритма шифрования xor.

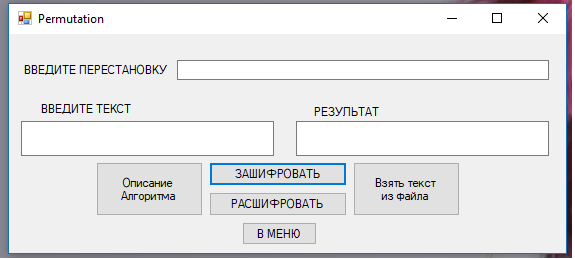


Рисунок 13

Для того зашифровать или расшифровать текст нужно ввести в поле «Ведите перестановку» перестановку, перестановка записывается в поле через знак пробел. Кодирование осуществляется перестановкой букв. Допустим введём перестановку 2413, первый символ из исходного блока должен быть переставлен на второе место, второй на четвертое, третий на первое, четвертый на третье.Если данным ключом зашифровать слово кофе, то получится слово фкео. Дешифрование производится в обратном порядке

На рисунке 14 представлен скриншот того куда нужно вводить данные.

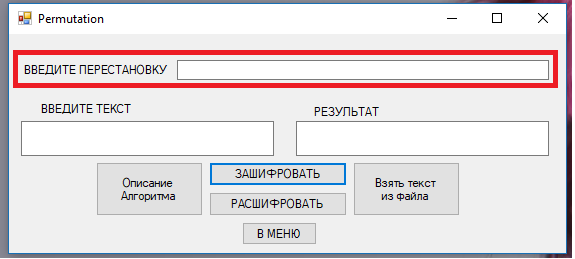


Рисунок 14

После того как была введена перестановка нужно ввести в поле «Введите текст» текст который нужно зашифровывать или расшифровывать. На рисунке 15 представлен скриншот, того куда нужно вводить.

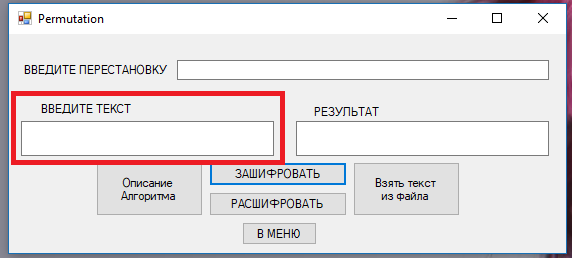


Рисунок 15

Если все исходные данные введены корректно результат зашифровки/расшифровки выведется на соотвествующем поле РЕЗУЛЬТАТ. Все результаты шифрования/расшифрования сохраняются в файл.

Если нажать на кнопку ВЗЯТЬ ТЕКСТ ИЗ ФАЙЛА, то в поле ВВЕДИТЕ ТЕКСТ будет записан результат предыдущей работы программы из любого алгоритма шифрования.

Если нажать на кнопку ОПИСАНИЕ АЛГОРИТМА откроется сообщение с кратким описанием данного алгоритма шифрования.

Если мы нажмем на кнопку «В меню» то мы перейдем в главное меню программы.