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»

Отчет заказчику

Научный руководитель

Родионова О.К.

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_2018 г.

Студент 3 курса, Клёц А.П. .

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

Новосибирск

2018

СОДЕРЖАНИЕ

[Введение 3](#_Toc515239286)

[1 ОПИСАНИЕ АЛГОРИТМОВ 5](#_Toc515239287)

[1.1 Алгоритм простой подстановки 5](#_Toc515239288)

[1.1.1 Как работать с программой реализующей алгоритм простой подстановки 5](#_Toc515239289)

[1.2 Алгоритм Цезаря 6](#_Toc515239290)

[1.2.1 Как работать с программой реализующей алгоритм 6](#_Toc515239291)

[1.3 Алгоритм XOR 7](#_Toc515239292)

[1.3.1 Как работать с программой реализующей алгоритм XOR 7](#_Toc515239293)

[1.4 Алгоритм простой блочной перестановки 8](#_Toc515239294)

[1.4.1 Как работать с программой реализующей алгоритм XOR 8](#_Toc515239295)

[Заключение 9](#_Toc515239296)

[Список используемых источников 10](#_Toc515239297)

[Приложение 11](#_Toc515239298)

# Введение

Программа, предназначенная для шифрования или дешифрования информации, использующая классические алгоритмы.

**Рекомендованные системные требования:**

- операционные системы: Windows Vista/XP/XP 98, Windows 7, Windows 8;Windows 10.

- процессор: AMD Phenom II X4 1 Ghz или лучше, Intel Core2 Quad 1 Ghz или лучше;

- видеокарта: 256 мб или лучше

- оперативная память: 256 GB RAM или лучше;

- свободное место на HDD: 70 мб.

**Среда разработки программного продукта**

Разработана система на языке программирования с#, в среде разработки Microsoft Visual Studio 14.0.

**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”.

**Размер программного продукта**

Конечный размер программного продукта без учета размера файла с записанными в него результатами работы программы составляет - 420 КБ (430 424 байт).

**Содержание программного продукта**

Программный продукт включает в себя 4 простых алгоритмов. Программа выполняет функции шифрования/дешифрования, используя для этого следующие классические алгоритмы:

1. Алгоритм простой подстановки.

2. Алгоритм Цезаря.

3. Алгоритм XOR.

4. Алгоритм простой блочной перестановки.

После выполнения шифрования/дешифрования программа сохраняет конечный результат в файл. Последний конечный результат выполнения шифрования/дешифрования можно использовать как исходные данные для дальнейших действий.

# ОПИСАНИЕ АЛГОРИТМОВ

## Алгоритм простой подстановки

В качестве подстановочного шифра был использован шифр простой замены, то есть для каждой буквы открытого текста существует единственный сопоставленный ей символ. Иными словами каждый символ исходного текста заменяется на заранее определенный символ. Все вхождения символа будут заменены на один и тот же символ независимо от контекста.

### Как работать с программой реализующей алгоритм простой подстановки

Работа описана в инструкции. Ссылка

## Алгоритм Цезаря

Шифрование алгоритмом Цезаря происходит следующим образом. Все символы заданного алфавита сдвигаются на заданное число позиций заданную пользователем, называющуюся величиной сдвига.

### Как работать с программой реализующей алгоритм

**Цезаря**

Работа описана в инструкции. Ссылка

## Алгоритм XOR

Заданы две последовательности из 0 и 1(шифруемая информация и ключ произвольной вами длинны). Над шифруемой информацией и ключом производится «сложение по модулю 2» Итак, XOR – результат операции, который принимает значение «истина» только если всего один из аргументов имеет значение «истина».

### Как работать с программой реализующей алгоритм XOR

Работа описана в инструкции. Ссылка.

## Алгоритм простой блочной перестановки

Метод [симметричного шифрования](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D1%8B%D0%B5_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B), в котором элементы исходного [открытого текста](https://ru.wikipedia.org/wiki/%D0%9E%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%B9_%D1%82%D0%B5%D0%BA%D1%81%D1%82) меняют местами. Элементами текста могут быть отдельные символы (самый распространённый случай), пары букв, тройки букв, комбинирование этих случаев и так далее.

### Как работать с программой реализующей алгоритм XOR

Работа описана в инструкции. Ссылка

# Заключение

В рамках курсовой работы была выполнено написание программы для шифрования и дешифрования.

В ходе выполнения задания были выполнены следующие задания.

1.Написан алгоритм для выполнения: Алгоритма простой подстановки, Алгоритма Цезаря, Алгоритма XOR и Алгоритма простой блочной перестановки.

2.Создан пользовательский интерфейс.

3.Написан отчёт заказчику.

4.Написана инструкция пользователя

# Список используемых источников

[[Перестановочный шифр — Википедия](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%BE%D1%87%D0%BD%D1%8B%D0%B9_%D1%88%D0%B8%D1%84%D1%80)]

[[Шифр подстановки — Википедия](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%BF%D0%BE%D0%B4%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B8)]

[[Шифр Цезаря — Википедия](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F)]

[[XOR шифрование - Криптография](http://kriptografea.narod.ru/XOR.html)]

# Приложение

