МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ Федеральное государственное автономное образовательное учреждение высшего образования

«Новосибирский национальный исследовательский государственный университет» (Новосибирский государственный университет, НГУ)

Структурное подразделение Новосибирского государственного университета

Высший колледж информатики Университета (ВКИ НГУ)

КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ЛАБОРАТОРНАЯ РАБОТА

ОТЧЁТ ЗАКАЗЧИКУ ПО ПРИЛОЖЕНИЮ «AgentXResident»

Руководитель Родионова О.К.

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_2018 г.

Студент 3 курса Гайдучик В.В.

гр. 503а1

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_2018 г.

Новосибирск

2018

ВВЕДЕНИЕ

1.1 Область применения

Программное обеспечение предназначено для шифровки и дешифровки заданного текста по ключу. Всего в ПО используется четыре алгоритма шифрования:

* Шифровка простой заменой.
* Шифровка XOR.
* Шифровка Цезаря.
* Блочная шифровка.

1.2 Уровень подготовки пользователя

Пользователь данного программного обеспечения должен иметь опыт работы с ОС MS Windows (XP и выше), а также навык работы с Windows Forms и приложением «Блокнот».

1.3 Перечень эксплуатационной документации, с которой необходимо ознакомиться пользователю

На данный момент – отсутствует.

1.4 Системные требования

* Процессор с тактовой частотой не ниже 1,8 ГГц. Рекомендуется использовать как минимум двухъядерный процессор.
* 2 ГБ ОЗУ; рекомендуется 4 ГБ ОЗУ (минимум 2,5 ГБ при выполнении на виртуальной машине).
* Место на жестком диске: до 40 МБ свободного места.
* Скорость жесткого диска: для повышения производительности используйте твердотельный накопитель (SSD).
* Видеоадаптер с минимальным разрешением 720p (1280 на 720 пикселей); для оптимальной работы ПО рекомендуется разрешение WXGA (1366 на 768 пикселей) или более высокое.

ПОДГОТОВКА К РАБОТЕ

2.1 Состав и содержание дистрибутивного носителя данных

Для работы с ПО, необходимо следующее:

* Windows Проводник.
* Блокнот.

2.2 Порядок загрузки данных и программ

Перед началом работы с ПО, на рабочем месте пользователя необходимо выполнить следующие действия:

* Создать текстовый файл (используя приложение Блокнот или командную строку), в который будет записываться зашифрованная информация.
* Убедиться, что в файле идёт корректное сохранение данных.

2.3 Порядок проверки работоспособности

Для проверки работоспособности ПО, на рабочем месте пользователя нужно выполнить следующие действия:

* Скачать ПО с электронного носителя.
* Запустить файл формата «\*.exe» (\* – название ПО).
* Убедиться, что на рабочем месте пользователя открылось приложение «\*».

В случае, если приложение «\*» не запускается, то следует обратиться к Вашему системному администратору, или в службу поддержки.

КРАТКОЕ ОПИСАНИЕ АЛГОРИТМОВ

3.1 Шифр простой подстановки

В [шифрах](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80) простой подстановки замена производится только над одним-единственным символом. Для наглядной демонстрации шифра простой замены достаточно выписать под заданным [алфавитом](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D1%84%D0%B0%D0%B2%D0%B8%D1%82) тот же алфавит, но в другом порядке или, например, со смещением. Записанный таким образом алфавит называют алфавитом замены.

3.2 Шифр Цезаря

Шифр Цезаря — один из древнейших шифров. При шифровании каждая буква заменяется другой, отстоящей от ней в алфавите на фиксированное число позиций. Шифр назван в честь римского императора [Гая Юлия Цезаря](https://ru.wikipedia.org/wiki/%D0%AE%D0%BB%D0%B8%D0%B9_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8C), использовавшего его для секретной переписки.

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами [модульной арифметики](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D1%83%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B0%D1%80%D0%B8%D1%84%D0%BC%D0%B5%D1%82%D0%B8%D0%BA%D0%B0):

Y = (X + K) mod N

X= (Y – K + N) mod N

Где «X»{\displaystyle x} — символ открытого текста, «Y»{\displaystyle y} — символ шифрованного текста, «N»{\displaystyle n} — [мощность](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D1%89%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%BC%D0%BD%D0%BE%D0%B6%D0%B5%D1%81%D1%82%D0%B2%D0%B0) алфавита, а «K»{\displaystyle k} — ключ.

(Пример шифрования с использованием ключа «K=4»)

|  |  |
| --- | --- |
| Исходный алфавит: | A B C D E F G H I J K L M N O P Q R S T U V W X Y Z |
| Алфавит замены: | E F G H I J K L M N O P Q R S T U V W X Y Z A B C D |

3.3 Блочная шифровка

Блочный шифр — разновидность [симметричного](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) [шифра](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80), оперирующего группами бит фиксированной длины — блоками, характерный размер которых меняется в пределах 64‒256 бит. Если исходный текст (или его остаток) меньше размера блока, перед [шифрованием](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) его дополняют. Фактически, блочный шифр представляет собой подстановку на алфавите блоков, которая, как следствие, может быть моно- или полиалфавитной. Блочный шифр является важной компонентой многих [криптографических протоколов](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) и широко используется для защиты данных, передаваемых по сети.

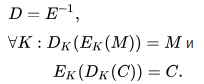
Блочный шифр состоит из двух парных алгоритмов: [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) и [расшифрования](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%81%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5). Оба алгоритма можно представить в виде функций. Функция шифрования E ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Encryption — шифрование) на вход получает блок данных M ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Message — сообщение) размером n бит и ключ K ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Key — ключ) размером k бит и на выходе отдает блок шифротекста C ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Cipher — шифр) размером n бит:



Для любого ключа K, Ek является [перестановкой](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) на множестве n-битных блоков. Функция расшифрования D ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Decryption — расшифрование) на вход получает шифр C, ключ K и на выходе отдает M:



Являясь, при этом, обратной к функции шифрования:

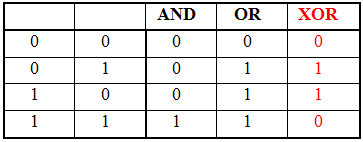


Стоит заметить, что ключ, необходимый для шифрования и дешифрования, один и тот же — следствие симметричности блочного шифра.

3.4 XOR шифровка

XOR – операция, которая принимает значение «истина» только если всего один из аргументов имеет значение «истина».

(Таблица истинности операций AND, OR и XOR)



XOR ­­­– аналогичен оператору AND (\*) и OR (+). Чтобы расшифровать шифр, нам просто нужно XOR шифровать ключ, чтобы восстановить исходный текст. Оператор XOR является чрезвычайно распространенным компонентом в сложных алгоритмах шифрования. Такую тайнопись можно легко разбить, используя постоянный повторяющийся ключ и используя частотный анализ.  Но мы меняем ключ после того, как каждое шифрование нарушает такое шифрование, данный вид криптографии – называется потоковым шифром, в котором каждый следующий бит зашифровывается с использованием другого псевдослучайного ключа.

ОПИСАНИЕ ОПЕРАЦИИ

4.1 Выполняемые функции и задачи

ПО выполняет функции и задачи, приведённые в таблице ниже:

|  |  |  |
| --- | --- | --- |
| Функции | Задачи | Описание |
| Обеспечивает  шифровку и  дешифровку  заданной  информации. | Визуализация  результата. | В ходе выполнения данной задачи  пользователю системы предоставляется  возможность работы с выбранной шифровкой  из состава преднастроенных. |

(Таблица 1 ­– Функции и задачи ПО)

4.2 Описание операций технологического процесса обработки данных, необходимых для выполнения задач

Ниже приведено описание пользовательских операций для выполнения каждой из задач.

Задача «Визуализация результата»

Шаг 1: Ввод алфавита

Условия, при соблюдении которых возможно выполнение операций:

* ПО запустилось в штатном режиме.

Подготовительные действия:

Не требуются.

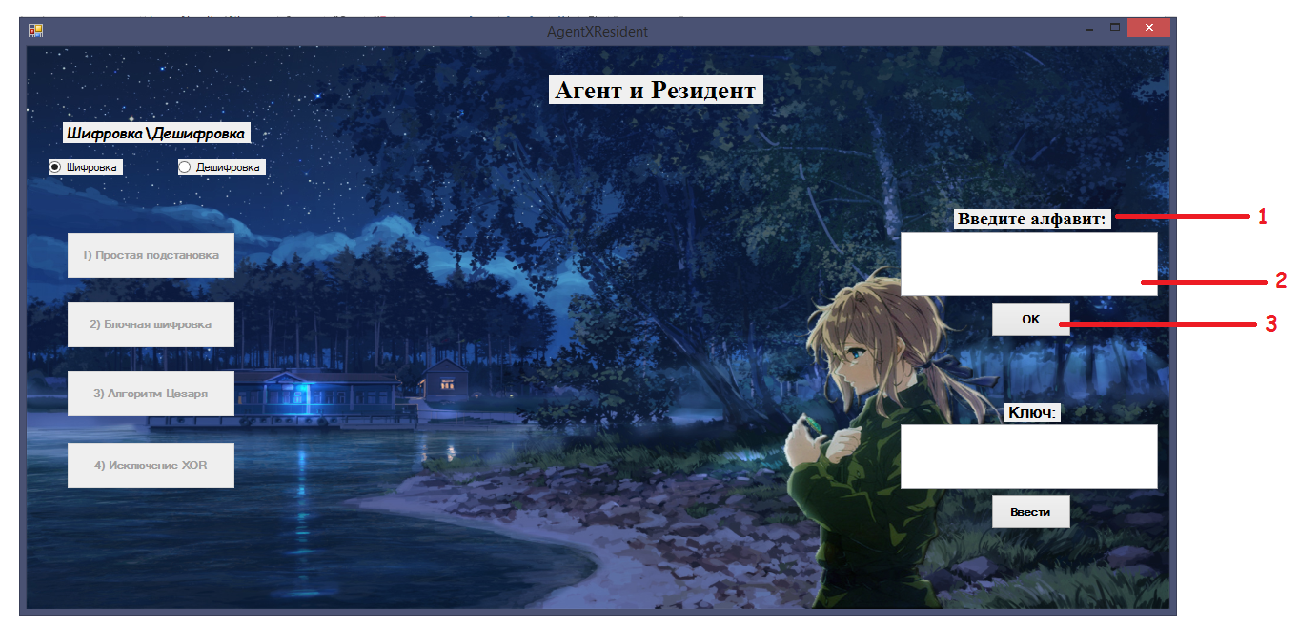
Основные действия в требуемой последовательности:

* В открывшемся окне ПО под надписью «Введите алфавит» ввести пользовательский алфавит. ВВОДИТЬ АЛФАВИТ БЕЗ ПРОБЕЛОВ, И С УЧЁТОМ БОЛЬШИХ И МАЛЫХ БУКВ!

Заключительные действия:

* Нажать на кнопку «ОК».

(Скриншот – Главная страница ПО. Ввод алфавита.)



1. Надпись «Введите алфавит».
2. Поле, куда надо ввести пользовательский алфавит.
3. Кнопка «Ок».

Шаг 2: Ввод ключа

Условия, при соблюдении которых возможно выполнение операций:

* ПО запустилось в штатном режиме.

Подготовительные действия:

Не требуются.

Основные действия в требуемой последовательности:

* В открывшемся окне ПО под надписью «Ключ» ввести пользовательский ключ.

Заключительные действия:

* Нажать на кнопку «Ввести».

(Скриншот – Главная страница ПО. Ввод ключа.)



1. Надпись «Ключ».
2. Поле, куда надо ввести пользовательский ключ.
3. Кнопка «Ввести».

Шаг 3: Ввод информации и её обработка

Условия, при соблюдении которых возможно выполнение операций:

* Введён алфавит.
* Введён ключ.
* Существует поступающая информация.

Подготовительные действия:

* Под надписью «Шифровка\Дешифровка» выберите кнопку «Шифровка».

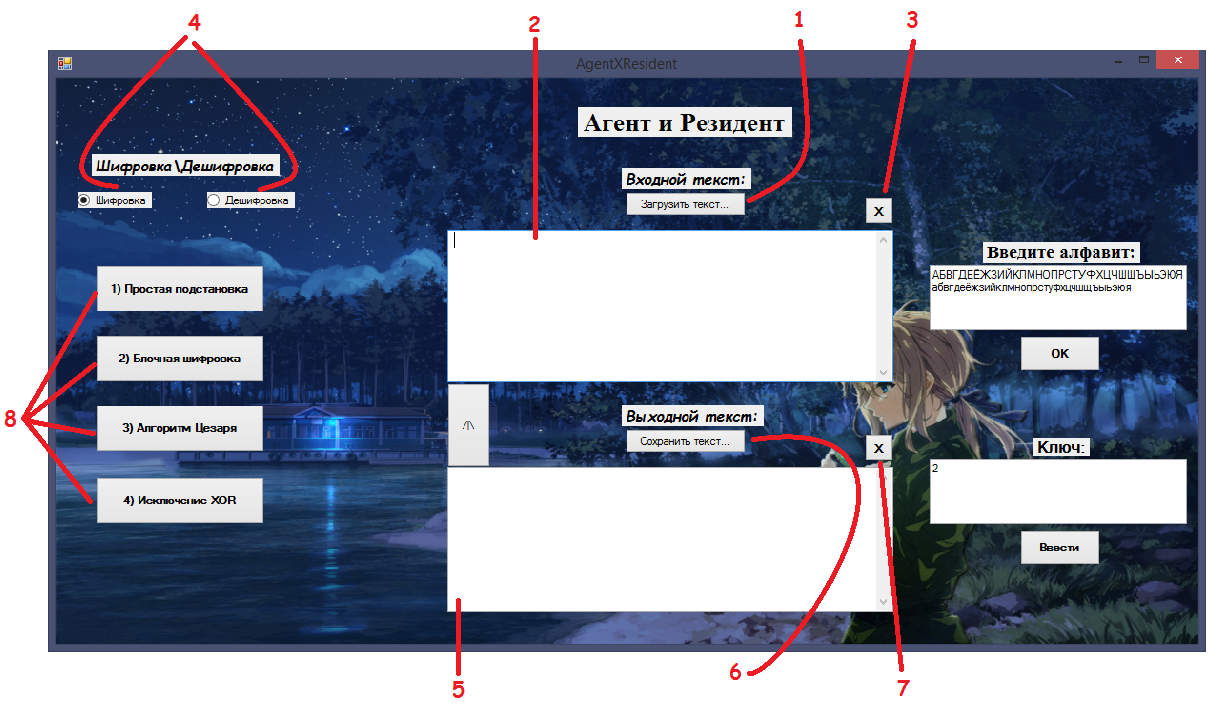
Основные действия в требуемой последовательности:

* В поле под кнопкой «Загрузить текст» ввести шифруемый текст.
* Если существует текстовый файл с шифруемым текстом, следует нажать на кнопку «Загрузить текст». В появившемся окне указать путь к нужному файлу. Распознаются файлы формата «\*.txt».
* После ввода входной информации, нужно выбрать один из четырёх способов шифрования, кликнув на кнопку с подходящим названием.
* В окне «Выходной текст» появится зашифрованный текст. В зависимости от вида шифровки, возможен вывод ключей, для ориентирования в дешифровке.

Заключительные действия:

* Сохранить зашифрованный текст, нажав на кнопку «Сохранить текст», находящуюся под надписью «Выходной текст».

(Скриншот ­– Главная страница ПО. Ввод/Вывод информации.)



1. Кнопка «Загрузить текст».
2. Поле, где должен быть входной текст.
3. Очистить поле входного текста.
4. Кнопки Шифровка\Дешифровка.
5. Поле выходного текста.
6. Кнопка «Сохранить текст».
7. Очистить поле выходного текста.
8. Кнопки видов шифровок.

Шаг 4: Дешифровка заданной информации

Условия, при соблюдении которых возможно выполнение операций:

* Введён алфавит.
* Введён ключ.
* Существует поступающая информация.

Подготовительные действия:

* Под надписью «Шифровка\Дешифровка» выберите кнопку «Дешифровка».

Основные действия в требуемой последовательности:

* В поле под надписью «Входной текст» ввести шифрованный текст. Существует два способа. Первый – если пользователь только что зашифровал информацию, он может сразу перенести её в поле, расположенное выше, нажав на кнопку «*стрелка вверх*». Второй – загрузить текст из текстового файла, нажав на кнопку «Загрузить текст».
* После ввода требуемой информации, нужно выбрать один из четырёх способов дешифровки, кликнув на кнопку с подходящим названием.
* В окне «Выходной текст» появится зашифрованный текст.

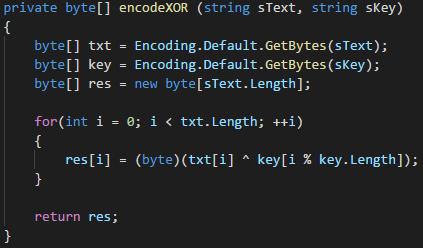
Заключительные действия:

Не требуются.

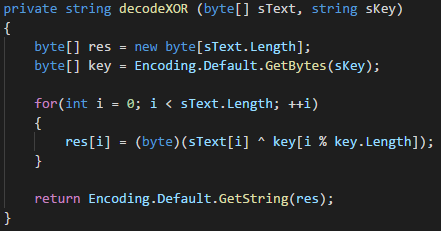
ОПТИМИЗАЦИЯ КОДА

5.1 Шифровка XOR

(Метод шифровки строки по заданному ключу)



(Метод дешифровки строки по заданному ключу)



(Вызов методов шифровки\дешифровки в основной программе)

