*Выполнил студент ПК-12-2, Бекленищев Владислав*

# Описание программы

## Общие сведения

Программа “Caesar cipher” является результатом выполнения лабораторной работы для курса “Методы защиты информации” и создана только в учебных целях, для демонстрации зашифровывания / расшифровывания различных текстовых сообщений.

Для запуска программы необходимо следующее программное обеспечение:

* Операционная система Windows 7, 8, 8.1;
* Библиотека .NET Framework версии 4.5.

Данная программа была написана с помощью средств языка C# на платформе .NET Framework в среде Microsoft Visual Studio 2012.

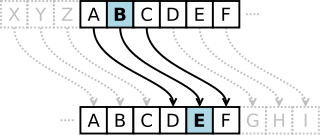
## Функциональное назначение

Приложение предназначено для расшифровывания / зашифровывания текстовых сообщений разной длины с помощью алгоритма шифрования Цезаря.

## Описание логической структуры

В основе программы лежит алгоритм шифрования Цезаря (шифр Цезаря или шифр **сдвига**), результаты работы которого можно увидеть при использовании данного программного продукта.

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите.



В примере, показанном на изображении выше, в шифре со **сдвигом** вправо на 3 английская буква A была бы заменена на английскую букву C, B - E**,** C - F, и так далее. Такие же действия происходят и в программе.

В основе алгоритма лежит следующая **математическая модель**:

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:





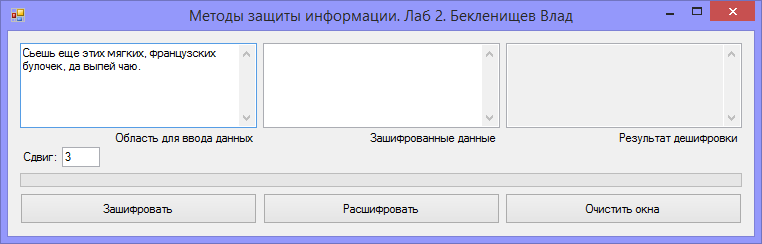
где x - символ шифрованного текста, y - символ зашифрованного текста, k - ключ (или сдвиг), n - мощность алфавита.

Для программы n (мощность алфавита) соответствует мощности таблицы символов Unicode - 2^16 (65536).

## Вызов и загрузка

Так как программа является приложением под операционные системы Windows 7, 8, 8.1, 10 её можно запустить либо из меню “Пуск” либо же с помощью ярлыка на рабочем столе.

После запуска появится главное окно приложения:



## Входные данные

Входными данными являются текстовые сообщения, которые можно вводить либо в поле “Область для ввода данных” либо в поле “Зашифрованные данные”.

Также пользователю предоставляется возможности самостоятельно ввести параметр **сдвига** (ключ). По умолчанию, в программе это значение равняется 3. Важно учитывать, что при вводе зашифрованных данных стоит также ввести соответствующее значение сдвига в поле “Сдвиг” чтобы при дешифровки получить корректные значения.

## Выходные данные

Результатом работы программы будет:

* зашифрованный текст во втором поле (после нажатия на кнопку “Зашифровать”)
* расшифрованный текст в третьем поле (после нажатия на кнопку “Расшифровать”)

Текст в третьем поле будет однозначно соответствовать тексту из первого поля.

Также пользователь может очистить все поля сразу нажав кнопку “Очистить окна”. При этом нужно учесть, что нельзя сделать операции шифрования над пустыми полями (1 и 2). Если пользователь попытается это сделать, программа выдаст предупреждение.