*Completed by student ПК-12-2 Beklenischev Vladislav*

# Program Description

## General

Program "Caesar cipher" is the result of the laboratory work for the course "Methods of protection of information" and created only for educational purposes to demonstrate the encrypting / decrypting various text files.

To run the program you need the following software:

* Windows 7, 8, 8.1,
* Library .NET Framework version 4.5.

This program was written by tools of C# language on the .NET Framework in the environment Microsoft Visual Studio 2012.

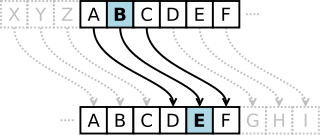
## Functional purpose

Application is designed to decrypt / encrypt files using an encryption algorithm “Caesar cipher”.

## Description of the logical structure

Program is based on the encryption algorithm Caesar (Caesar cipher or **shift** code**),** the results of which can be seen by using this software.

Caesar cipher - a type of substitution cipherin which each symbol in the plaintext is replaced by the character at a constant number of positions to the left or right of it in the alphabet.



In the example shown on the image above, in the cipher with a **shift** to the right by three English letter A was replaced by the English letter C, B - E, C - F, and etc.

The algorithm is based on the following **mathematical model**:

If we compare each character of the alphabet sequence number (numbering from 0), the encryption and decryption can be expressed as modular arithmetic:





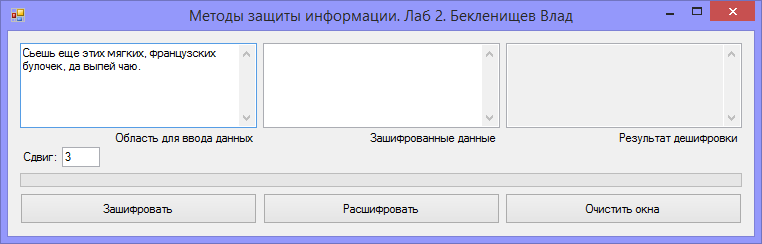
where x - symbol of the decrypted text, y - symbol of the encrypted text, k - key (or shift), n - the power of the alphabet.

For the program n (power of the alphabet) corresponds to the power of the symbol table Unicode - 2 ^ 16 (65536).

## Calling and loading

The program is an application for Windows operating systems 7, 8, 8.1, 10. It can be run from the "Start" menu or by using the shortcut on the desktop.

After starting the main application window will appear:



## Input data

Input data are text messages that can be administered in the field "Field data entry" or in the field "encrypted data".

Also, the user can enter their own **shift** parameter (key). By default in the program this value is equal to 3. It is important to note that when you entering the encrypted data you must also enter a value corresponding to a shift in the field "Сдвиг" to obtain the correct decoding value.

## Output

Result of the program will be:

* encrypted text in the second field (after pressing the "Зашифровать")
* decrypted text in the third field (after you clicking the “Расшифровать”)

The text in the third field will be correspond to the text of the first field.

The user can clear all fields at once by clicking the "Очистить окна". It should take into account that you can not make encryption operations over the empty fields (1 and 2). If a user attempts to do this, the program will give a warning.