Федеральное государственное автономное

образовательное учреждение

высшего образования

«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

|  |
| --- |
| Институт космических и информационных технологий |
| *институт* |
| Кафедра Прикладной математики и компьютерной безопасности |
| *кафедра* |

**ЛАБОРАТОРНАЯ РАБОТА №3**

|  |
| --- |
| **Шифр Цезаря** |
| *тема* |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Руководитель | | |  |  |  | В.И.Вайнштейн |
|  | |  |  | *подпись, дата* |  | *инициалы, фамилия* |
| Студент | КИ15-01 №031508683 | |  |  |  | М.С.Димаксян |
|  | *номер группы, зачетной книжки* | |  | *подпись, дата* |  | *инициалы, фамилия* |

Красноярск 2019

**Задание:**

Реализовать шифр Цезаря на любом языке программирования.

**Теория:**

**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.

**Исходный код:**

**Алгоритм зашифрования:**

private void f3\_ButtonEncrypt\_Click(object sender, EventArgs e)

{

int rot, tmpout;

if (f3\_fieldRotate.TextLength <1 || !int.TryParse(f3\_fieldRotate.Text, out tmpout) || (rot = Convert.ToInt16(f3\_fieldRotate.Text)) < 0)

{

MessageBox.Show("Поле \"сдвиг\" должно содержать целое неотрицательное число.");

}

else

{

string Source = f3\_fieldOriginal.Text;

char[] Code = Source.ToCharArray();

for (int i = 0; i < Code.Length; i++)

{

int tmp = Convert.ToInt16(Code[i]); //Код текущего символа

if ((tmp >= 65 && tmp <= 90) || (tmp >= 97 && tmp <= 122))

{

int rot\_en = rot % 26;

tmp = tmp + rot\_en;

if (tmp > 122 || (tmp>90 && (tmp-rot\_en< 91))) tmp = tmp - 26;

Code[i] = Convert.ToChar(tmp);

}

else if ((tmp >= 1040 && tmp <= 1071) || tmp == 1025 {

string ALF = "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ";

char tmp2 = Convert.ToChar(tmp);

tmp = (ALF.IndexOf(tmp2) + rot) % 33;

tmp2 = ALF[tmp];

Code[i] = tmp2;

}

else if ((tmp >= 1072 && tmp <= 1103) || tmp == 1105)

{

string alf = "абвгдеёжзийклмнопрстуфхцчшщъыьэюя";

char tmp2 = Convert.ToChar(tmp);

tmp = (alf.IndexOf(tmp2) + rot) % 33;

tmp2 = alf[tmp];

Code[i] = tmp2;

}

}

string txt = new string(Code);

f3\_fieldCiphertext.Text = txt;

}

}

**Алгоритм расшифрования:**

private void f3\_ButtonDecrypt\_Click(object sender, EventArgs e)

{

int rot, tmpout;

if (f3\_fieldRotate.TextLength < 1 || !int.TryParse(f3\_fieldRotate.Text, out tmpout) || (rot = Convert.ToInt16(f3\_fieldRotate.Text)) < 0)

{

MessageBox.Show("Поле \"сдвиг\" должно содержать целое неотрицательное число.");

}

else

{

string Source = f3\_fieldCiphertext.Text;

char[] Code = Source.ToCharArray();

int rotRU = (33 - rot) % 33;

int rotEN = (26 - (rot % 26)) % 26;

for (int i = 0; i < Code.Length; i++)

{

int tmp = Convert.ToInt16(Code[i]); // Код текущего символа

if ((tmp >= 65 && tmp <= 90) || (tmp >= 97 && tmp <= 122))

tmp = tmp + rotEN;

if (tmp > 122 || (tmp > 90 && (tmp - rotEN < 91))) tmp = tmp - 26;

Code[i] = Convert.ToChar(tmp);

}

else if ((tmp >= 1040 && tmp <= 1071) || tmp == 1025)

{

string ALF = "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ";

char tmp2 = Convert.ToChar(tmp);

tmp = (ALF.IndexOf(tmp2) + rotRU) % 33;

tmp2 = ALF[tmp];

Code[i] = tmp2;

}

else if ((tmp >= 1072 && tmp <= 1103) || tmp == 1105)

{

string alf = "абвгдеёжзийклмнопрстуфхцчшщъыьэюя";

char tmp2 = Convert.ToChar(tmp);

tmp = (alf.IndexOf(tmp2) + rotRU) % 33;

tmp2 = alf[tmp];

Code[i] = tmp2;

}

}

string txt = new string(Code);

f3\_fieldOriginal.Text = txt;

}

**Результат работы программы:**

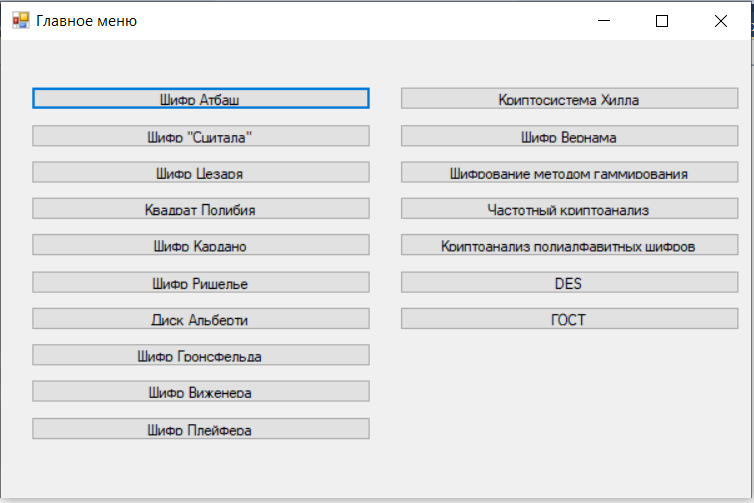


Рисунок 1. Главное меню программы.

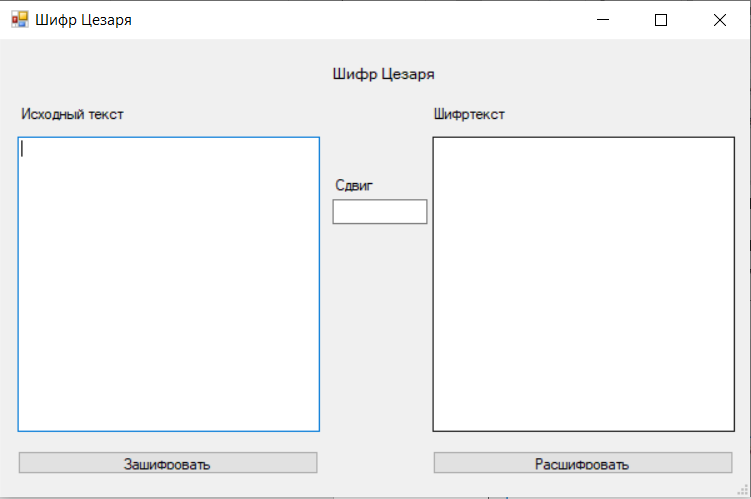


Рисунок 2. Окно шифра Цезаря.

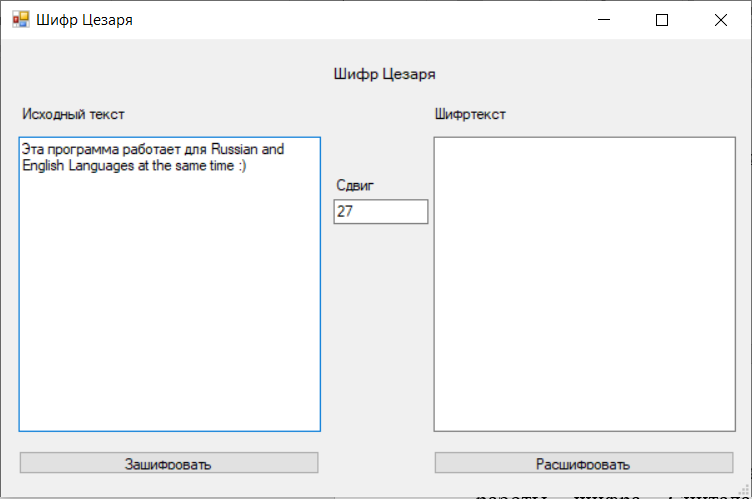


Рисунок 3. Исходный текст.

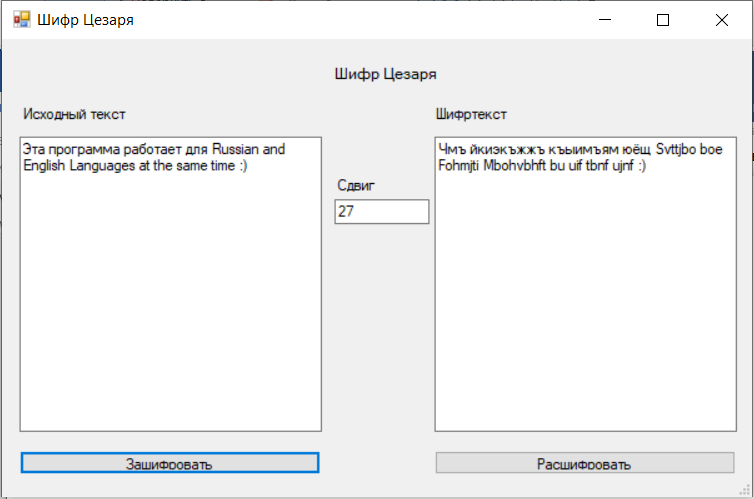


Рисунок 4. Шифртекст (результат зашифрования).

Очистим поле Исходный текст и расшифруем сообщение. Сдвиг необходимо оставить неизменным.

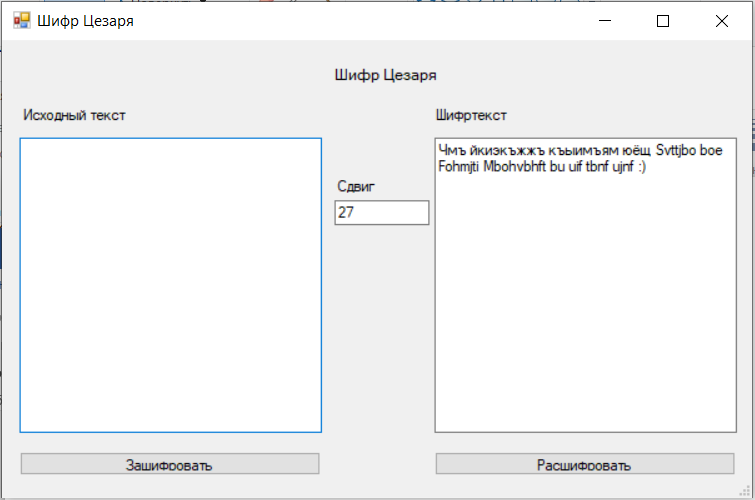


Рисунок 5. Очистка поля Исходный текст.

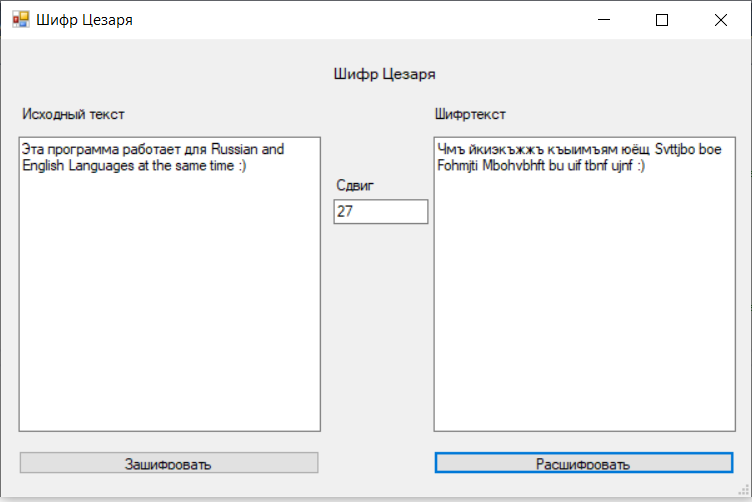


Рисунок 6. Исходный текст (результат расшифрования).

**Вывод:**

В ходе выполнения лабораторной работы я ознакомилась с алгоритмом работы шифра Цезаря, реализовала на практике программу по зашифрованию и расшифрованию данным шифром на языке C#. Данные навыки я могу применить при реализации других шифров и при дальнейшем использовании шифра Цезаря.