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 №2**

|  |
| --- |
| **Шифр Сцитала** |
| *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 Скитала на любом языке программирования.

**Теория:**

Идея шифрования текста заключается в том, что сообщение писалось на узкой полоске пергамента. А та в свою очередь наматывалась на палочку (жезл) определённой длины и диаметра. Для прочтения полоска античной бумаги наматывалась на жезл плотно, виток к витку. Далее читалась строка вдоль длины получившегося цилиндра. Затем палочка поворачивалась на определённый угол и читалась следующая строка. Чтобы передаваемое сообщение без искажений уяснялось принимающей стороной, адресант и адресат должны были иметь жезл одинаковой длины и диаметра.

Процесс шифрования заключался в перемене мест исходного текста в соответствии с буквенной ёмкостью диаметра дешифровального приспособления.

**Исходный код:**

**Алгоритм зашифрования:**

private void f2\_ButtonEncrypt\_Click(object sender, EventArgs e)

{

int dia, len, tmpout;

if (f2\_fieldDiametr.TextLength < 1 || !int.TryParse(f2\_fieldDiametr.Text, out tmpout) || ((dia = Convert.ToInt32(f2\_fieldDiametr.Text)) < 2))

{

MessageBox.Show("Неверный диаметр");

}

else

{

string Source = f2\_fieldOriginal.Text;

char[] Code = Source.ToCharArray();

//Вычисление длины Скиталы по диаметру и длине исходного текста

if (f2\_fieldOriginal.TextLength % dia == 0)

len = f2\_fieldOriginal.TextLength / dia;

else

len = f2\_fieldOriginal.TextLength / dia + 1;

//Отображение найденной длины

f2\_fieldLength.Text = Convert.ToString(len);

if (len < 2)

{

MessageBox.Show("Слишком короткий исходный текст!","Ошибка");

}

else

{

//Создаем Скиталу требуемого размера

char[][] mas = new char[dia][];

for (int m = 0; m < dia; m++)

mas[m] = new char [len];

//Заполняем всю Скиталу мусорным символом

for (int m = 0; m < dia; m++)

for (int n = 0; n < len; n++)

mas[m][n] = '⁣';

//Заполняем Скиталу символами исходного текста

int i = 0, j = 0;

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

{

mas[i][j] = Code[m];

j++;

if (j == len)

{

i++;

j = 0;

}

}

//Считываем шифртекст со Скиталы

char[] result = new char [len \* dia];

int cur = 0;

for (int m = 0; m<len; m++)

for (int n = 0; n<dia; n++)

{

result[cur] = mas[n][m];

cur++;

}

string txt = new string(result);

f2\_fieldCiphertext.Text = txt;

}

}

}

**Алгоритм расшифрования:**

private void f2\_ButtonDecrypt\_Click(object sender, EventArgs e)

{

int dia, len, tmpout;

if (f2\_fieldDiametr.TextLength < 1 || !int.TryParse(f2\_fieldDiametr.Text, out tmpout) || ((dia = Convert.ToInt32(f2\_fieldDiametr.Text)) < 2))

{

MessageBox.Show("Неверный диаметр");

}

else

{

string Source = f2\_fieldCiphertext.Text;

char[] Code = Source.ToCharArray();

//Вычисление длины Скиталы по диаметру и длине исходного текста

if (f2\_fieldCiphertext.TextLength % dia == 0)

len = f2\_fieldCiphertext.TextLength / dia;

else

len = f2\_fieldCiphertext.TextLength / dia + 1;

//Отображение найденной длины

f2\_fieldLength.Text = Convert.ToString(len);

if (len < 2)

{

MessageBox.Show("Слишком короткий шифртекст", "Ошибка");

}

else

{

//Создаем Скиталу требуемого размера

char[][] mas = new char[len][];

for (int m = 0; m < len; m++)

mas[m] = new char[dia];

//Заполняем всю Скиталу мусорным символом

for (int m = 0; m < len; m++)

for (int n = 0; n < dia; n++)

mas[m][n] = '⁣';

//Заполняем Скиталу символами шифртекста

int i = 0, j = 0;

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

{

mas[i][j] = Code[m];

j++;

if (j == dia)

{

i++;

j = 0;

}

}

//Считываем шифртекст со Скиталы

char[] tmp = new char[dia \* len];

int cur = 0;

for (int m = 0; m < dia; m++)

for (int n = 0; n < len; n++)

{

tmp[cur] = mas[n][m];

cur++;

}

string txt = new string(tmp);

f2\_fieldOriginal.Text = txt;

}

}

}

**Результат работы программы:**

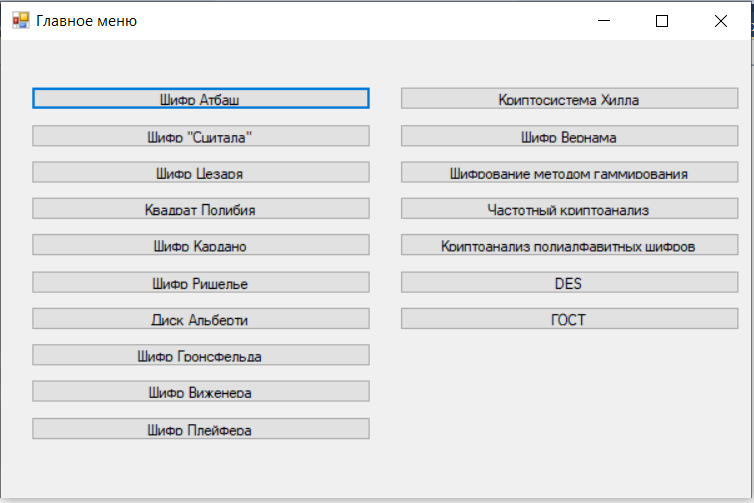


Рисунок 1. Главное меню программы.

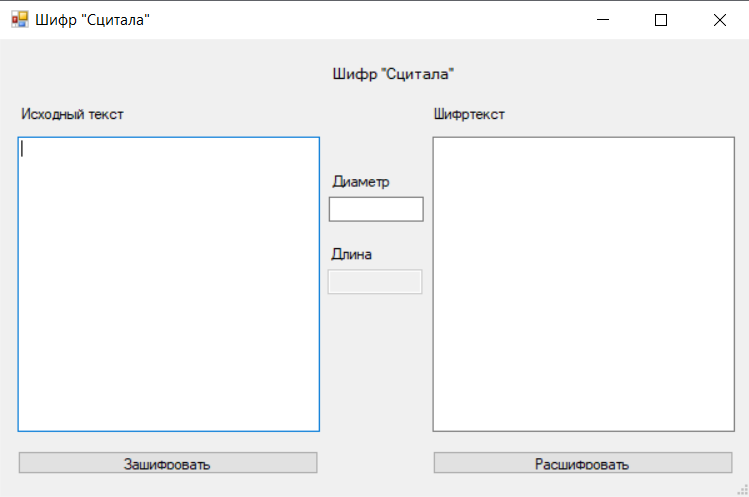


Рисунок 2. Окно шифра «Сцитала».

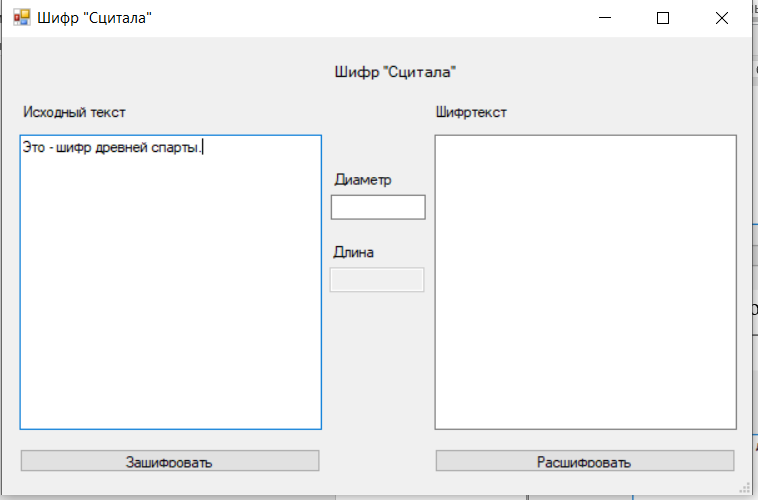


Рисунок 3. Исходный текст.

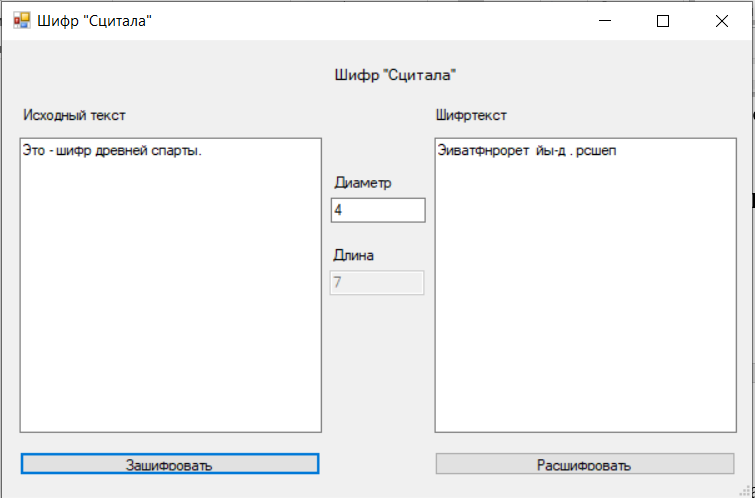


Рисунок 4. Шифртекст (результат зашифрования).

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

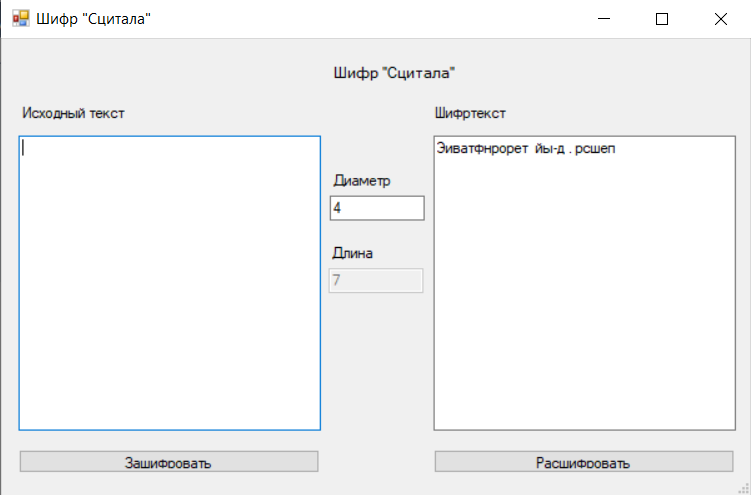


Рисунок 5. Очистка поля Исходный текст.

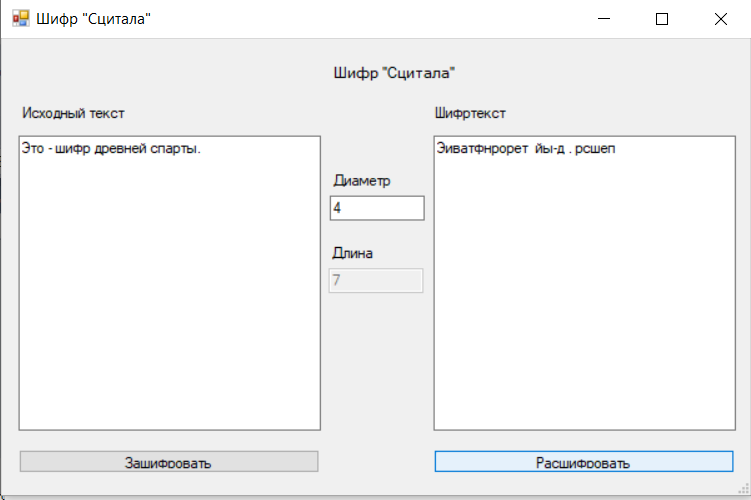


Рисунок 6. Исходный текст (результат расшифрования).

**Вывод:**

В ходе выполнения лабораторной работы я ознакомилась с алгоритмом работы шифра Сцитала, 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 Сцитала.