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 №7**

|  |
| --- |
| **Диск Альберти** |
| *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 диск Альберти на любом языке программирования.

**Теория:**

Итальянец Альберти (XVI в.) впервые выдвинул идею «двойного шифрования» — текст, полученный в результате первого шифрования,подвергался повторному зашифрованию. В трактате Альберти был приведен и его собственный шифр, который он назвал «шифром, достойным королей». Он утверждал, что этот шифр недешифруем. Реализация шифра осуществлялась с помощью шифровального диска, положившего начало целой серии многоалфавитных шифров. Устройство представляло собой пару дисков — внешний, неподвижный (на нем были нанесены буквы в естественном порядке и цифры от 1 до 4) и внутренний - подвижный - на нем буквы были переставлены. Процесс шифрования заключался в нахождении буквы открытого текста на внешнем диске и замену ее на соответствующую (стоящей под ней) букву шифрованного текста. После шифрования нескольких слов внутренний диск сдвигался на один шаг. Ключом данного шифра являлся порядок расположения букв на внутреннем диске и его начальное положение относительно внешнего диска.

**Исходный код:**

**Задание алфавита:**

string ALF = "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯабвгдеёжзийклмнопрстуфхцчшщъыьэюяABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789!@#$%^&\*()\_+-={};'/.,<>?№: ";

string ALF\_mixed = "'LеиNмgШmQVЯаX{Y6Zabc01ПРСТсур$Д#Э7H8kчшяAф4DF!%p^\*)+НvОЧ-=}lЫRгЬЛ;зKёSjTЩUА3CnжEУ5ВMu&ткqOЦP/.s>\_хцФщъwxьyЁЖы№BefМhi(2нопoБrG?d:tЗИ@ЙКz, ЪдЕWйЮIлбJвГ9эюХ<";

**Алгоритм зашифрования:**

private void f7\_ButtonEncrypt\_Click(object sender, EventArgs e)

{

char[] Source = f7\_fieldOriginal.Text.ToCharArray();

int rot = Convert.ToInt32(f7\_fieldRotate.Text);

int blockLength = Convert.ToInt32(f7\_fieldLength.Text);

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

{

Source[i] = ALF\_mixed[(ALF.LastIndexOf(Source[i]) + (rot \* (i / blockLength))) % ALF\_mixed.Length];

}

f7\_fieldCiphertext.Text = new string(Source);

}

**Алгоритм расшифрования:**

private void f7\_ButtonDecrypt\_Click(object sender, EventArgs e)

{

char[] Source = f7\_fieldCiphertext.Text.ToCharArray();

int rot = Convert.ToInt32(f7\_fieldRotate.Text);

int blockLength = Convert.ToInt32(f7\_fieldLength.Text);

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

{

Source[i] = ALF[(((ALF\_mixed.LastIndexOf(Source[i]) - (rot \* (i / blockLength))) % ALF.Length) + ALF.Length) % ALF.Length];

}

f7\_fieldOriginal.Text = new string(Source);

}

**Результат работы программы:**

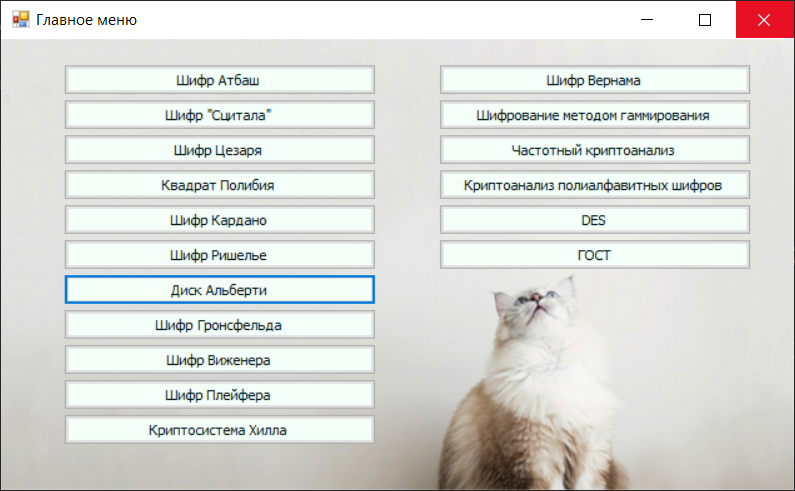


Рисунок 1. Главное меню программы.

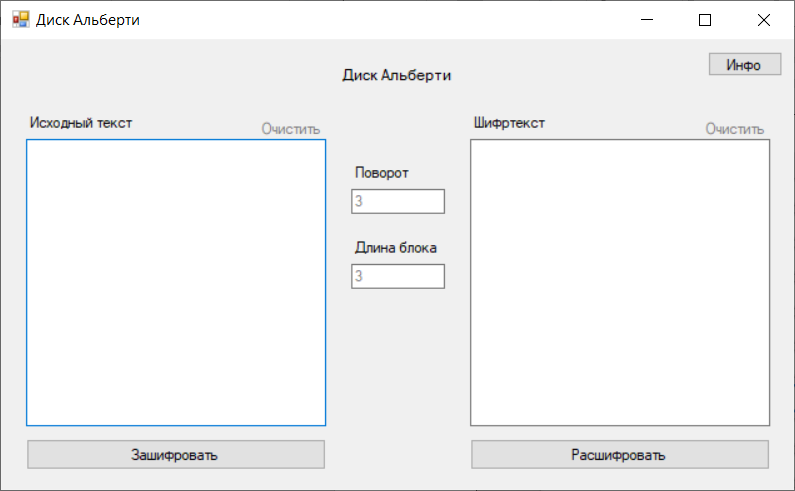


Рисунок 2. Окно диска Альберти.

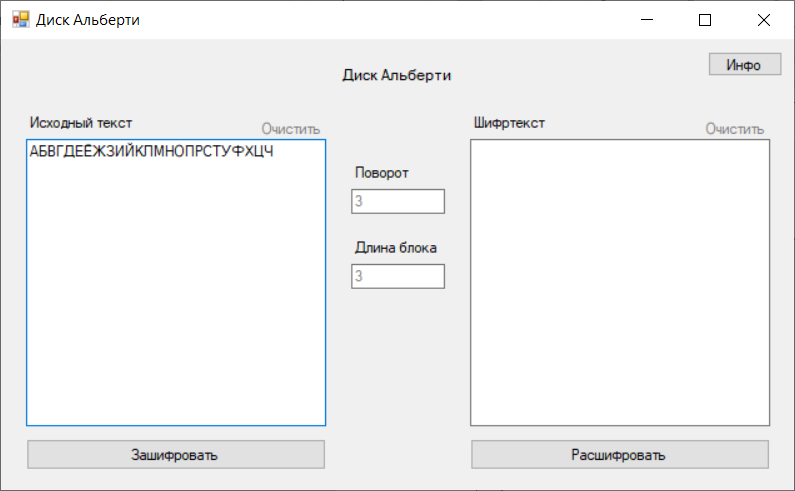


Рисунок 3. Исходный текст.

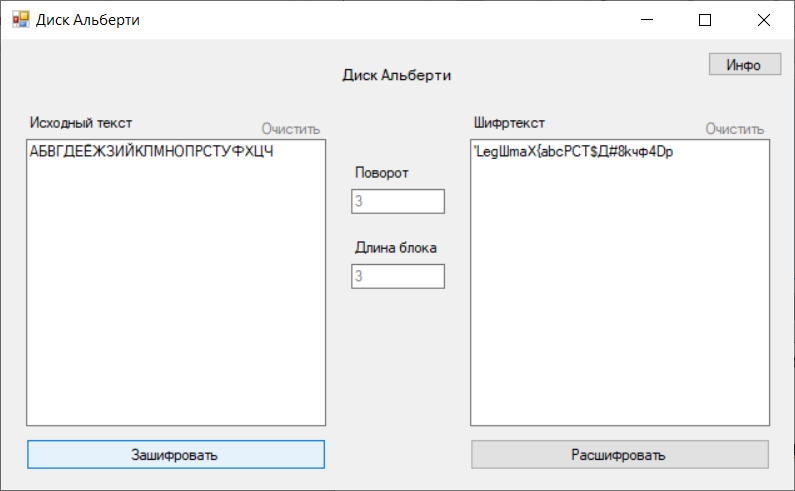


Рисунок 4. Шифртекст (результат зашифрования).

Очистим поле Исходный текст и расшифруем сообщение.

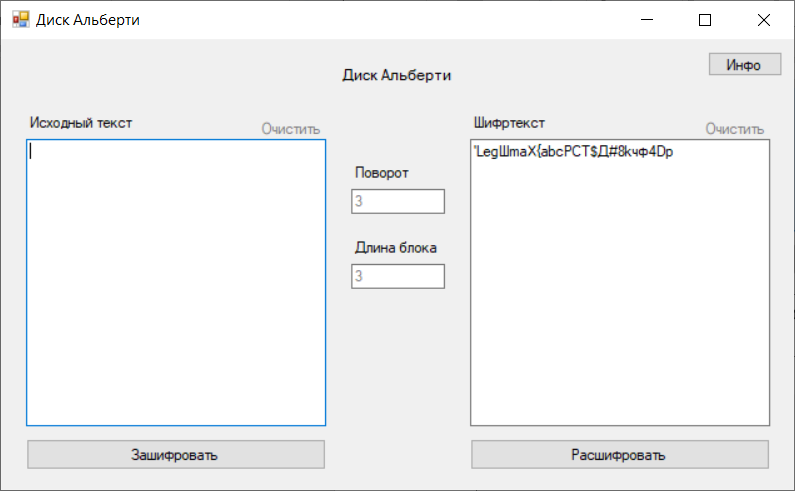


Рисунок 5. Очистка поля Исходный текст.

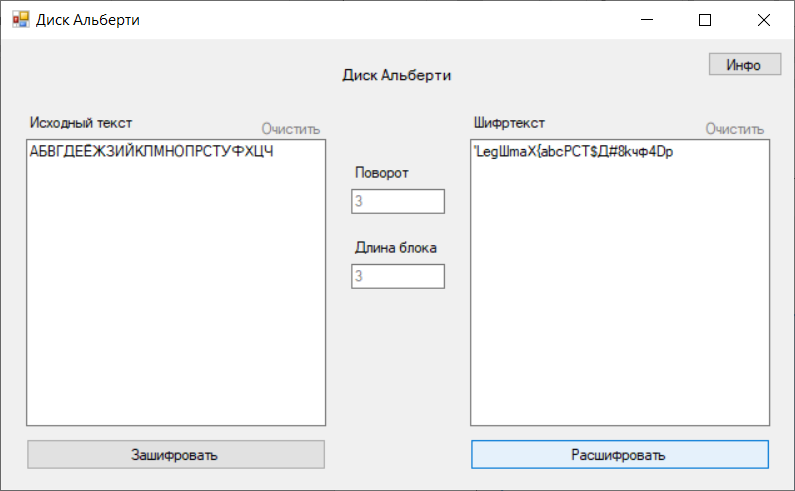


Рисунок 6. Исходный текст (результат расшифрования).

**Вывод:**

В ходе выполнения лабораторной работы я ознакомилась с алгоритмом диска Альберти, 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 диска Альберти.