Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Пермский национальный исследовательский политехнический университет»

Электротехнический факультет

Кафедра «Информационные технологии и автоматизированные системы»

Направление 09.03.04 – «Программная инженерия»

Дисциплина: «Защита информации»

Профиль: «Разработка программно-информационных систем»

Семестр 5

ОТЧЕТ

по лабораторной работе №1

Тема: «Шифры перестановки и замены»

Выполнил: студент группы РИС-22-1б

Поважный В. Е. \_\_\_\_\_\_\_\_\_\_\_

Проверил: доцент кафедры ИТАС

Шереметьев В. Г. \_\_\_\_\_\_\_\_\_\_\_

Дата \_\_\_\_\_\_

Пермь, 2024

**ЦЕЛЬ РАБОТЫ**

Получить практические навыки по применению шифров перестановки и шифров простой замены.

**ЗАДАНИЕ**

Реализовать шифрование текстового сообщения, используя шифр «Полибианский квадрат».

**ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ**

Одним из первых шифров простой замены считается так называемый *полибианский квадрат*. За два века до нашей эры греческий писатель и историк Полибий изобрел для целей шифрования квадратную таблицу размером 5х5, заполненную буквами греческого алфавита в случайном порядке.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *q* | *p* | *w* | *o* | *e* |
| *i* | *r* | *u* | *t* | *y* |
| *z* | *m* | *x* | *n* | *c* |
| *b* | *v* | *a* | *l* | *s* |
| *k* | *d* | *j* | *f* | *h* |

Полибианский квадрат, заполненный случайным образом буквами латинского алфавита и пробелом

При шифровании в этом полибианском квадрате находили очередную букву открытого текста и записывали в шифртекст букву, расположенную ниже ее в том же столбце. Если буква текста оказывалась в нижней строке таблицы, то для шифртекста брали самую верхнюю букву из того же столбца. Например, для слова

*square*

получается шифртекст

*hixjmy*

Концепция полибианского квадрата оказалась плодотворной и нашла применение в криптосистемах последующего времени.

**ХОД РАБОТЫ**

На рисунке 1 представлена форма. В верхнее поле вводится шифруемая фраза. Фраза должна быть записана заглавными буквами русского алфавита без пробелов. При нажатии на кнопку «Старт», алфавит генерируется заново.

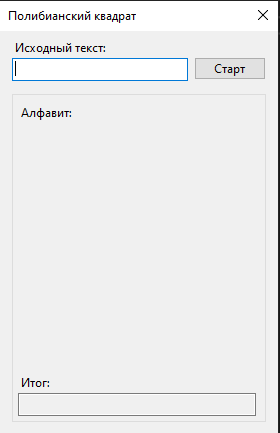


Рисунок 1 – Форма для шифрования.

Пример работы программы представлен на рисунке 2.

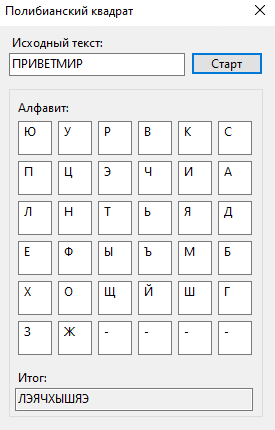


Рисунок 2 – Пример работы программы.

**ПРИЛОЖЕНИЕ А**

**Листинг программы**

public partial class lab1 : Form

{

private char[,] array;

private const int arraySize = 6;

public lab1()

{

InitializeComponent();

}

private void button1\_Click(object sender, EventArgs e)

{

if (textBox1.Text != "")

StartProcess();

else

MessageBox.Show("Строка не должна быть пустой!", "Warning", MessageBoxButtons.OK, MessageBoxIcon.Error);

}

private void StartProcess()

{

foreach (char c in textBox1.Text)

if (c < 1040 || c > 1071)

{

MessageBox.Show("Строка должна иметь только заглавные буквы русского алфавита!", "Warning", MessageBoxButtons.OK, MessageBoxIcon.Error);

return;

}

GenerateGrids();

textBox2.Text = EncryptString(textBox1.Text);

}

private void GenerateGrids()

{

Random rand = new Random();

bool isCorrect = false;

tableLayoutPanel1.Controls.Clear();

List<char> ruChars = new List<char>();

for (int i = 1040; i <= 1071; i++)

ruChars.Add((char)i);

array = new char[arraySize, arraySize];

for (int i = 0; i < arraySize; i++)

for (int j = 0; j < arraySize; j++)

if (ruChars.Count > 0)

{

int random = rand.Next(0, ruChars.Count);

array[i, j] = ruChars[random];

ruChars.RemoveAt(random);

}

else if (ruChars.Count == 0)

array[i, j] = '-';

for (int i = 0; i < arraySize; i++)

for (int j = 0; j < arraySize; j++)

{

TextBox textBox = new TextBox();

textBox.Multiline = true;

textBox.Dock = DockStyle.Fill;

textBox.Text = array[i, j].ToString();

tableLayoutPanel1.Controls.Add(textBox, j, i);

}

}

private string EncryptString(string text)

{

string newText = "";

foreach (char c in text)

for (int i = 0; i < arraySize; i++)

for (int j = 0; j < arraySize; j++)

if (array[i, j] == c)

if (i == arraySize - 1)

newText += array[0, j];

else

newText += array[i + 1, j];

return newText;

}

}