ЛАБОРАТОРНА РОБОТА № 4
ЗАХИСТ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

Мета: здобуття практичних навичок захисту інформації за допомогою шифру перестановки та заміни.

Хід роботи:

Завдання 1: провести програмну реалізацію методу заміни

4.	Зупинка	Атака, що має на меті змусити сервер не відповідати на запити

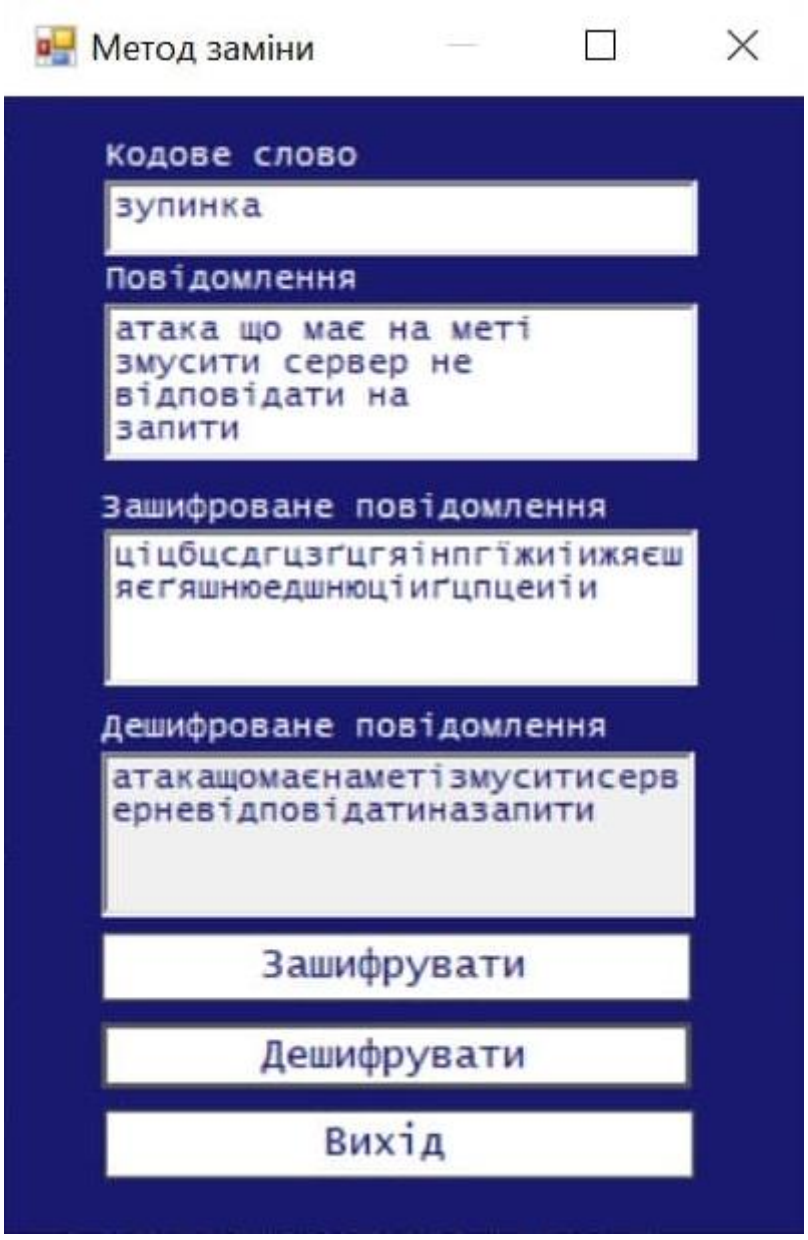
Лістинг програми:

```
using System;
using System.Windows.Forms;

namespace WindowsFormsApp1
{
    public partial class Form1 : Form
    {
        char[] k = new char[33] { 'а', 'б', 'в', 'г', 'ґ', 'д', 'е', 'є', 'ж', 'з', 'и', 'і', 'ї', 'й', 'к',
'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ', 'ь', 'ю', 'я' };
        char[] alphabet = new char[33];
        char[] res = new char[60];
        int n = 0;
        int z = 0;
        int c = 0;
        int x = 0;
        int m = 0;

        public Form1()
        {
            InitializeComponent();
            button2.Enabled = false;
            textBox3.Enabled = false;
            textBox4.Enabled = false;
        }

        private void button3_Click(object sender, EventArgs e)
        {
            Application.Exit();
        }

        private void button1_Click(object sender, EventArgs e)
        {
            button2.Enabled = true;
            textBox3.Enabled = true;
            string str = textBox1.Text;
            string str2 = textBox2.Text;
            char[] ar = new char[str.Length];

            for (int i = 0; i < str.Length; i++)
            {
                ar[i] = str[i];
                n = i;
            }

            for (int i = 0; i < str.Length; i++)
                alphabet[n + i + 1] = ar[i];
```

```
        for (int q = 0; q < 33; q++)
        {
            z = 0;
            for (int i = 0; i < n + 1; i++)
            {
                if (k[q] != ar[i])
                {

                    if (z == n)
                    {
                        if ((n + n + 2 + c) > 32)
                        {
                            alphabet[x] = k[q];
                            x++;
                        }
                        if ((n + n + 2 + c) < 33)
                        {
                            alphabet[n + n + 2 + c] = k[q];
                            c++;
                        }

                    }
                    z++;
                }
                if (k[q] == ar[i])
                    z = 0;
            }
        }

        char[] bet = new char[str2.Length];

        for (int i = 0; i < str2.Length; i++)
        {
            bet[i] = str2[i];
            m = i;
        }

        for (int y = 0; y < m + 1; y++)
        {
            for (int i = 0; i < 33; i++)
            {
                if (bet[y] == k[i])
                    res[y] = alphabet[i];
            }
        }

        for (int i = 0; i < m + 1; i++)
            textBox3.Text += res[i].ToString(); ;
    }

    private void button2_Click(object sender, EventArgs e)
    {
        string str2 = textBox3.Text;
        char[] bet = new char[str2.Length];

        for (int i = 0; i < str2.Length; i++)
        {
            bet[i] = str2[i];
            m = i;
        }

        for (int y = 0; y < m + 1; y++)
        {
            for (int i = 0; i < 33; i++)
            {
                if (bet[y] == alphabet[i])
                    res[y] = k[i];
            }
        }

        for (int i = 0; i < m + 1; i++)
            textBox4.Text += res[i].ToString();
    }

    private void label3_Click(object sender, EventArgs e)
    {
```

```
        }

        private void Form1_Load(object sender, EventArgs e)
        {

        }
    }
}
```

Результат виконання програми:



Завдання 2: здійснити програмну реалізацію методу перестановки

4.	Фішинг	Регулярно перевіряйте стан своїх електронних рахунків

Лістинг програми:

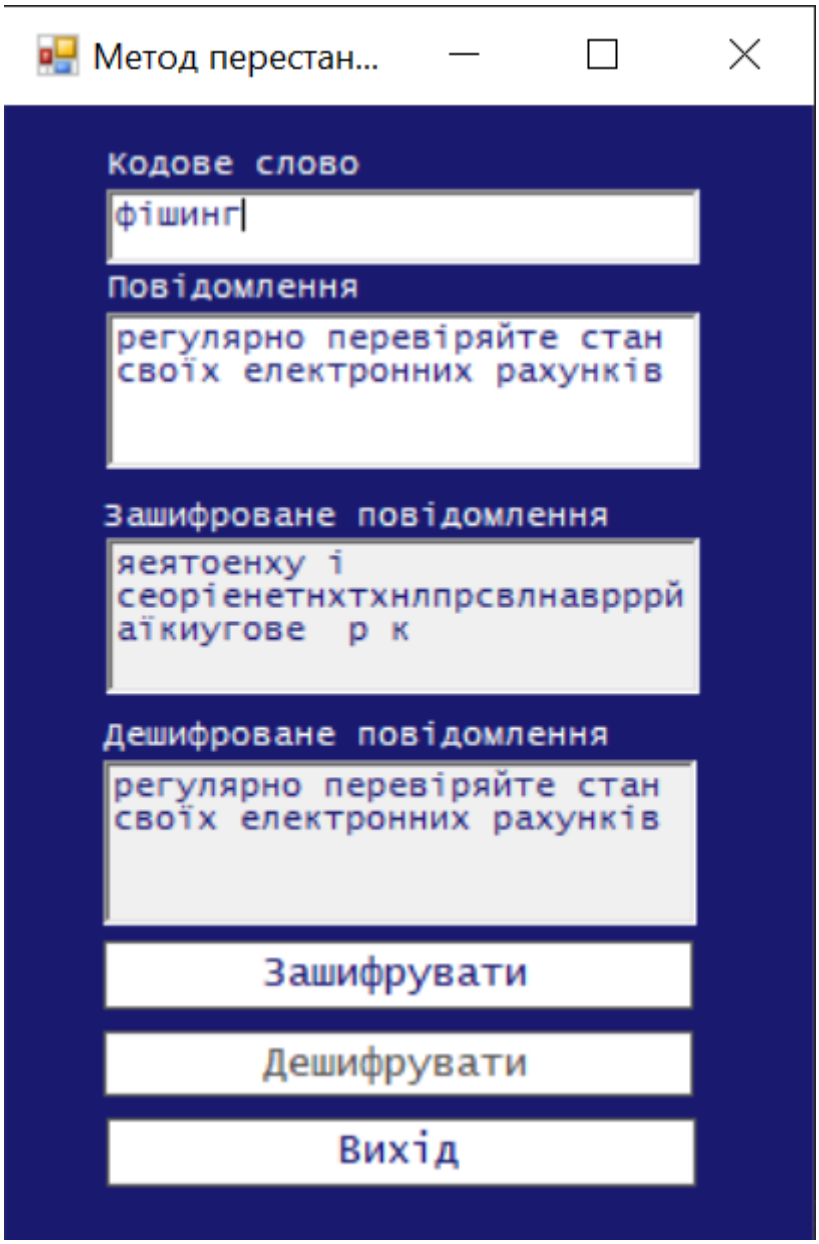
```
using System;
using System.Windows.Forms;

namespace WindowsFormsApp2
{
    public partial class Form1 : Form
    {
```

```
        string[] uaAlphabet = {"а", "б", "в", "г", "ґ", "д", "е", "є", "ж", "з", "и", "і", "ї", "й", "к", "л",
"м", "н", "о", "п", "р", "с", "т", "у", "ф", "х", "ц", "ч", "ш", "щ", "ь", "ю", "я"};

        string key;
        int k;
        int l;
        string[] key_word;
        string start_msg;
        string[] msg;
        string[,] workspace;
        double rows;
        int collumns;
        string code_msg;
        string[] code;

        public Form1()
        {
            InitializeComponent();
            buttonDecrypt.Enabled = false;
            richTextBoxEncrypt.Enabled = false;
            richTextBoxDecrypt.Enabled = false;
        }

        private void buttonEncrypt_Click(object sender, EventArgs e)
        {
            richTextBoxEncrypt.Text = "";
            richTextBoxDecrypt.Text = "";

            if (richTextBoxKey.Text == "" || richTextBoxMessage.Text == "")
            {
                MessageBox.Show("Заповніть усі необхідні поля!");
            }

            else
            {
                buttonDecrypt.Enabled = true;
                //обробка ключового слова
                key = richTextBoxKey.Text;
                key_word = new string[key.Length + 1];
                for (int i = 0; i < key.Length; i++)
                    key_word[i + 1] = key.Substring(i, 1);
                //обробка повідомлення
                start_msg = richTextBoxMessage.Text;
                msg = new string[start_msg.Length + 1];
                for (int i = 0; i < start_msg.Length; i++)
                    msg[i + 1] = start_msg.Substring(i, 1);
                //підготовка робочого масиву
                collumns = key.Length + 1;
                rows = Math.Truncate((double)start_msg.Length / (double)key.Length) + 2;
                workspace = new string[(int)rows, collumns];
                for (int i = 0; i < rows; i++)
                {
                    for (int j = 0; j < collumns; j++)
                        workspace[i, j] = "-1";
                }
                //нумерація букв ключового слова
                k = 1;
                for (int i = 1; i < uaAlphabet.Length; i++)
                {
                    for (int j = 1; j <= key.Length; j++)
                    {
                        if (uaAlphabet[i] == key_word[j])
                        {
                            workspace[0, j] = k.ToString();
                            k++;
                        }
                    }
                }
                //заповнення робочого масиву
                k = 1;
                while (k < msg.Length)
                {
                    for (int i = 1; i < rows; i++)
                    {
                        for (int j = 1; j < collumns; j++)
                        {
                            workspace[i, j] = msg[k];
```

```
                    k++;
                    if (k >= msg.Length)
                        break;
                }
            }
        }
        //кодування
        code = new string[msg.Length + 1];
        k = 1;
        l = 1;
        while (k <= key.Length && l < msg.Length)
        {
            for (int i = 1; i < collumns; i++)
            {
                if (workspace[0, i] == k.ToString())
                {
                    for (int j = 1; j < rows; j++)
                    {
                        if (workspace[j, i] != "-1")
                        {
                            code[l] = workspace[j, i];
                            l++;
                        }
                        if (l >= msg.Length)
                            break;
                    }
                    k++;
                    if (k > key.Length)
                        break;
                }
            }
        }
        //вивід зашифрованої стрічки
        code_msg = "";
        for (int i = 1; i < msg.Length; i++)
        {
            if (i % 5 == 0)
            {
                code_msg += code[i];
                code_msg += "";
            }
            else
                code_msg += code[i];
        }
        richTextBoxEncrypt.Text = code_msg;
    }
}

private void buttonDecrypt_Click(object sender, EventArgs e)
{
    code_msg = "";
    buttonDecrypt.Enabled = false;
    for (int i = 1; i < rows; i++)
    {
        for (int j = 1; j < collumns; j++)
        {
            if (workspace[i, j] != "-1")
            {
                code_msg += workspace[i, j];

            }
        }
    }
    richTextBoxDecrypt.Text = code_msg;
}

private void buttonClose_Click(object sender, EventArgs e)
{
    this.Close();
}

private void Form1_Load(object sender, EventArgs e)
{

}

private void label2_Click(object sender, EventArgs e)
```

```
        {

        }

        private void label4_Click(object sender, EventArgs e)
        {

        }
    }
}
```

Результат виконання програми:



Висновки: в ході виконання лабораторної роботи було здобуто практичні навички захисту інформації за допомогою шифру перестановки та заміни.