**Учебная практика 6: Шифрование данных**

Задание:

* Создать программу WindowsForms – Задание 6
* Используя System.Security.Cryptography выполнить шифрование данных
* Выполнить дешифрование

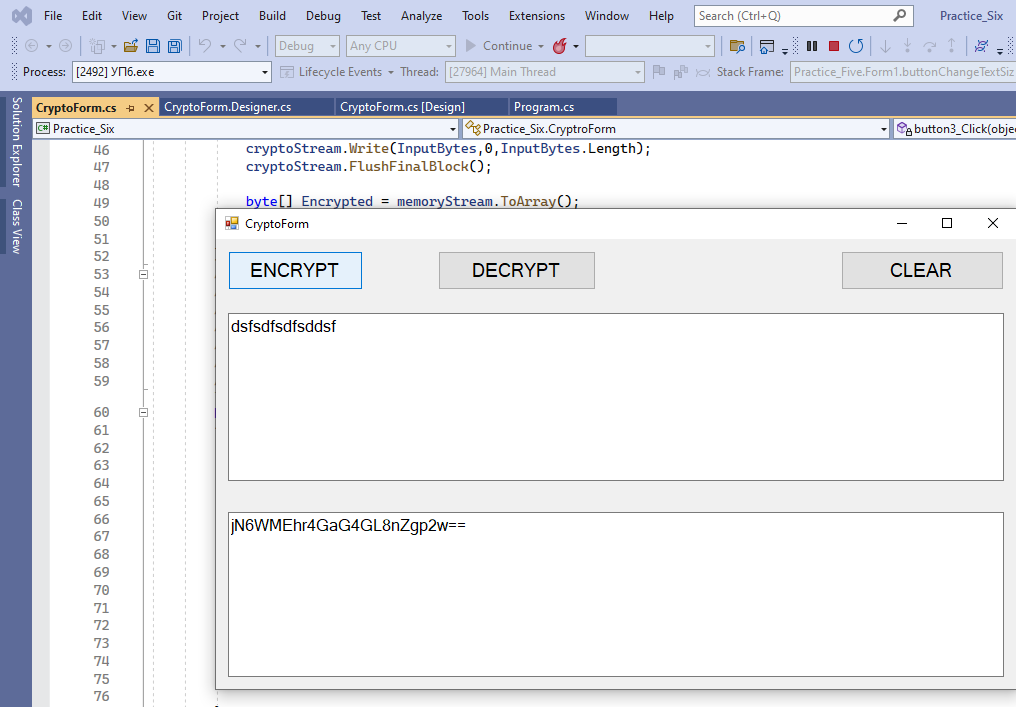
**Ход выполнения:**

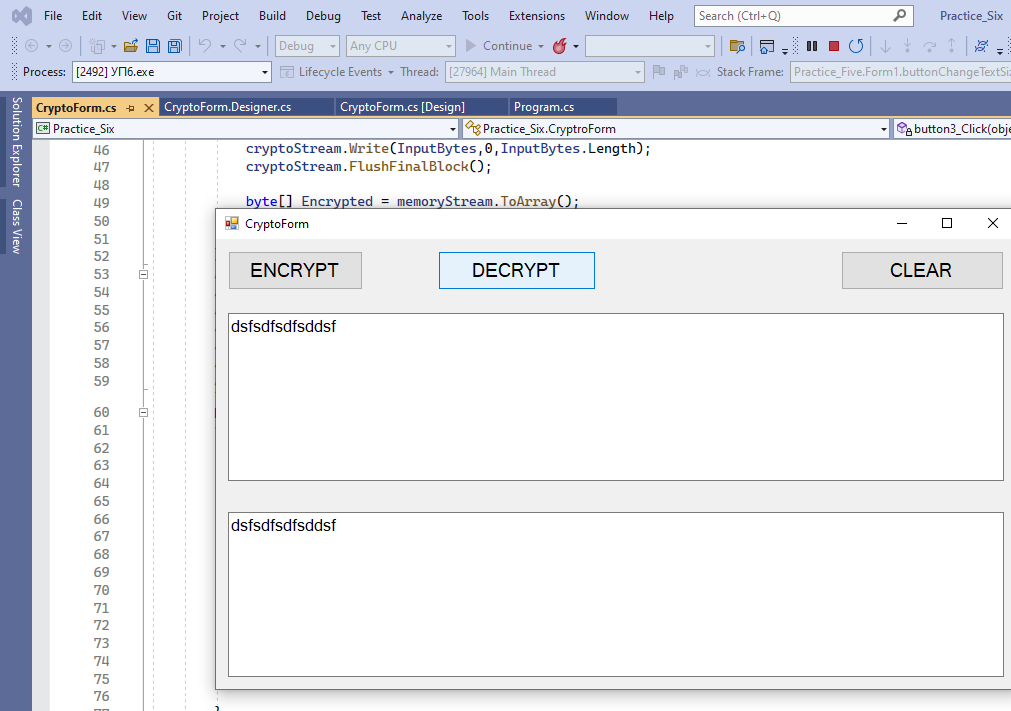
* Взял за основу проект лабораторной работы №6. В программе есть два поля: Верхнее для ввода сообщения, нижнее для вывода зашифрованного сообщения.

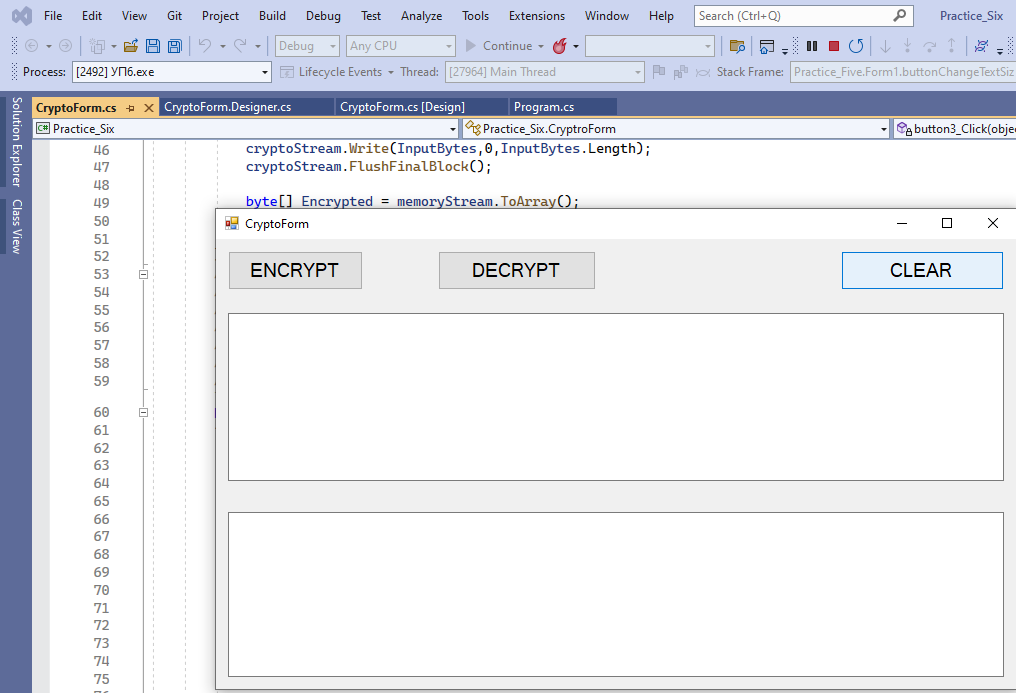
A picture containing text, screenshot, software, display

Description automatically generated

* Для шифрования нужно нажать кнопку ENCRYPT, для расшифрования кнопку DECRYPT. Кнопка CLEAR очищает оба поля.







* Да шифрование и дешифрование отвечают методы, Encrypt () и Decrypt ():

private string Encrypt(string plaintext, string Password, byte[] IV)

{

byte[] Key = Encoding.UTF8.GetBytes(Password);

AesManaged aes = new AesManaged();

aes.Key = Key;

aes.IV = IV;

MemoryStream memoryStream = new MemoryStream();

CryptoStream cryptoStream = new CryptoStream(memoryStream,aes.CreateEncryptor(), CryptoStreamMode.Write );

byte[] InputBytes = Encoding.UTF8.GetBytes(plaintext);

cryptoStream.Write(InputBytes,0,InputBytes.Length);

cryptoStream.FlushFinalBlock();

byte[] Encrypted = memoryStream.ToArray();

return Convert.ToBase64String(Encrypted);

}

/// <summary>

/// расшифровка зашифрованного текста

/// </summary>

/// <param name="plaintext"></param>

/// <param name="Password"></param>

/// <param name="IV"></param>

/// <returns></returns>

private string Decrypt(string plaintext, string Password, byte[] IV)

{

byte[] Key = Encoding.UTF8.GetBytes(Password);

AesManaged aes = new AesManaged();

aes.Key = Key;

aes.IV = IV;

MemoryStream memoryStream = new MemoryStream();

CryptoStream cryptoStream = new CryptoStream(memoryStream, aes.CreateDecryptor(), CryptoStreamMode.Write);

byte[] InputBytes = Convert.FromBase64String(plaintext);

cryptoStream.Write(InputBytes, 0, InputBytes.Length);

cryptoStream.FlushFinalBlock();

byte[] Decrypted = memoryStream.ToArray();

return UTF8Encoding.UTF8.GetString(Decrypted, 0, Decrypted.Length);

}

**Весь код программы:**

using System;

using System.IO;

using System.Security.Cryptography;

using System.Text;

using System.Windows.Forms;

namespace Practice\_Six

{

public partial class CryptroForm : Form

{

private static byte[] IV = { 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 };

public CryptroForm()

{

InitializeComponent();

}

private void textBox1\_TextChanged(object sender, EventArgs e)

{

}

/// <summary>

/// шифрование

/// </summary>

/// <param name="plaintext"> текс для шифровки</param>

/// <param name="Password"> Пароль</param>

/// <param name="IV"> параметр шифрования IV</param>

/// <returns></returns>

private string Encrypt(string plaintext, string Password, byte[] IV)

{

byte[] Key = Encoding.UTF8.GetBytes(Password);

AesManaged aes = new AesManaged();

aes.Key = Key;

aes.IV = IV;

MemoryStream memoryStream = new MemoryStream();

CryptoStream cryptoStream = new CryptoStream(memoryStream,aes.CreateEncryptor(), CryptoStreamMode.Write );

byte[] InputBytes = Encoding.UTF8.GetBytes(plaintext);

cryptoStream.Write(InputBytes,0,InputBytes.Length);

cryptoStream.FlushFinalBlock();

byte[] Encrypted = memoryStream.ToArray();

return Convert.ToBase64String(Encrypted);

}

/// <summary>

/// расшифровка зашифрованного текста

/// </summary>

/// <param name="plaintext"></param>

/// <param name="Password"></param>

/// <param name="IV"></param>

/// <returns></returns>

private string Decrypt(string plaintext, string Password, byte[] IV)

{

byte[] Key = Encoding.UTF8.GetBytes(Password);

AesManaged aes = new AesManaged();

aes.Key = Key;

aes.IV = IV;

MemoryStream memoryStream = new MemoryStream();

CryptoStream cryptoStream = new CryptoStream(memoryStream, aes.CreateDecryptor(), CryptoStreamMode.Write);

byte[] InputBytes = Convert.FromBase64String(plaintext);

cryptoStream.Write(InputBytes, 0, InputBytes.Length);

cryptoStream.FlushFinalBlock();

byte[] Decrypted = memoryStream.ToArray();

return UTF8Encoding.UTF8.GetString(Decrypted, 0, Decrypted.Length);

}

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

{

textBox1.Clear();

textBox2.Clear();

}

private void button2\_Click(object sender, EventArgs e)

{

try

{

textBox2.Text = Encrypt(textBox1.Text, "5555555555555555", IV);

}

catch (Exception ex)

{

MessageBox.Show(ex.Message);

}

}

private void button3\_Click(object sender, EventArgs e)

{

try

{

textBox2.Text = Decrypt(textBox2.Text, "5555555555555555", IV);

}

catch (Exception ex)

{

MessageBox.Show(ex.Message);

}

}

}

}