

Задание

Написать программу для шифрования/дешифрования файлов на языке C#

Текст программы

```
using System;
using System.IO;
using System.Security.Cryptography;

class FileEncryptor
{
    static void Main()
    {
        string inputFile = "input.txt";
        string encryptedFile = "encrypted.bin";
        string decryptedFile = "decrypted.txt";

        // Генерация случайного ключа и вектора инициализации
        byte[] key = GenerateRandomBytes(32); // 256 бит (32 байта)
        byte[] iv = GenerateRandomBytes(16); // 128 бит (16 байт)

        // Шифрование файла
        EncryptFile(inputFile, encryptedFile, key, iv);

        Console.WriteLine("File encrypted successfully.");

        // Дешифрование файла
        DecryptFile(encryptedFile, decryptedFile, key, iv);

        Console.WriteLine("File decrypted successfully.");
    }

    // Шифрование файла
    static void EncryptFile(string inputFile, string outputFile, byte[] key, byte[] iv)
    {
        using (Aes aesAlg = Aes.Create())
        {
            // Устанавливаем ключ и вектор инициализации для алгоритма AES
            aesAlg.Key = key;
            aesAlg.IV = iv;

            // Открываем поток для чтения из исходного файла
            using (FileStream inputStream = new FileStream(inputFile, FileMode.Open))
            {
                // Открываем поток для записи в зашифрованный файл
                using (FileStream outputStream = new FileStream(outputFile, FileMode.Create))
                {
                    // Создаем объект, осуществляющий шифрование
                    using (ICryptoTransform encryptor = aesAlg.CreateEncryptor())
                    {
                        // Создаем поток для шифрования
                        using (CryptoStream cryptoStream = new CryptoStream(outputStream, encryptor,
                            CryptoStreamMode.Write))
                        {
                            // Копируем данные из исходного файла в поток шифрования
                            inputStream.CopyTo(cryptoStream);
                        }
                    }
                }
            }
        }
    }

    // Дешифрование файла
}
```

```

static void DecryptFile(string inputFile, string outputFile, byte[] key, byte[] iv)
{
    using (Aes aesAlg = Aes.Create())
    {
        // Устанавливаем ключ и вектор инициализации для алгоритма AES
        aesAlg.Key = key;
        aesAlg.IV = iv;

        // Открываем поток для чтения из зашифрованного файла
        using (FileStream inputFileStream = new FileStream(inputFile, FileMode.Open))
        {
            // Открываем поток для записи в дешифрованный файл
            using (FileStream outputFileStream = new FileStream(outputFile, FileMode.Create))
            {
                // Создаем объект, осуществляющий дешифрование
                using (ICryptoTransform decryptor = aesAlg.CreateDecryptor())
                {
                    // Создаем поток для дешифрования
                    using (CryptoStream cryptoStream = new CryptoStream(outputFileStream, decryptor,
CryptoStreamMode.Write))
                    {
                        // Копируем данные из зашифрованного файла в поток дешифрования
                        inputFileStream.CopyTo(cryptoStream);
                    }
                }
            }
        }
    }
}

// Генерация случайных байтов для ключей и векторов инициализации
static byte[] GenerateRandomBytes(int length)
{
    using (RNGCryptoServiceProvider rngCrypto = new RNGCryptoServiceProvider())
    {
        byte[] randomBytes = new byte[length];
        rngCrypto.GetBytes(randomBytes);
        return randomBytes;
    }
}

```

Результат работы

ConsoleApp1.runtimeconfig.json20.12.2023 6:01JUN Hie1 Kb

decrypted.txt20.12.2023 6:07Текстовый докум...755 KB

encrypted.bin20.12.2023 6:07Файл "BIN"755 KB

input.txt18.12.2022 14:04Текстовый докум...755 KB

input.txt - Блокнот

BOOK ONE: 1805

CHAPTER I

"Well, Prince, so Genoa and Lucca are now just family estates of the Buonapartes.

But I warn you, if you don't tell me that this means war, if you still try to defend the infi

But how do you do?

I see I have frightened you – sit down and tell me all the news."

It was in July, 1805, and the speaker was the well-known Anna Pavlovna Scherer, maid of hono

Anna Pavlovna had had a cough for some day She was, as she said, suffering from la grippe; g

All her invitations without exception written in French and delivered by a scarlet-liverie

decrypted.txt - Блокнот

BOOK ONE: 1805

CHAPTER I

"Well, Prince, so Genoa and Lucca are now just family estates of the Buonapartes.

But I warn you, if you don't tell me that this means war, if you still try to defend the infi

But how do you do?

I see I have frightened you – sit down and tell me all the news."

It was in July, 1805, and the speaker was the well-known Anna Pavlovna Scherer, maid of hono

Anna Pavlovna had had a cough for some day She was, as she said, suffering from la grippe; g

All her invitations without exception written in French and delivered by a scarlet-liverie

Консоль отладки Microsoft Visual Studio

File encrypted successfully.

File decrypted successfully.

F:\BIG DZ ARCHIEVE\archieve dz 3Sem\PCPL\dz\ConsoleApp1\bin\Debug\net6.0\dz.exe (процесс 11072) завершил работу с кодом 0.

Чтобы автоматически закрывать консоль при остановке отладки, включите параметр "Сервис" ->"Параметры" ->"Отладка" -> "Автоматически закрыть консоль при остановке отладки".

Нажмите любую клавишу, чтобы закрыть это окно: █