Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования «Тульский государственный университет»

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

АЛГОРИТМЫ ГАММИРОВАНИЯ

отчет о лабораторной работе №1

по дисциплине

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Выполнила _____

ст. гр. №230711 Павлова Виктория Сергеевна

Проверила _____

доцент каф. ИБ Басалова Галина Валерьевна

Тула 2023

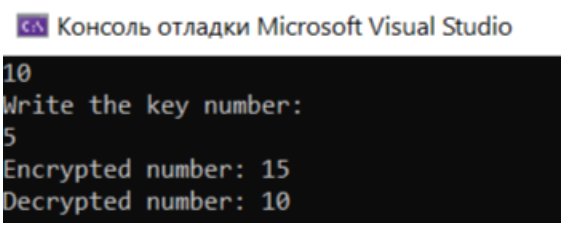
Лабораторная работа №1. Алгоритмы гаммирования

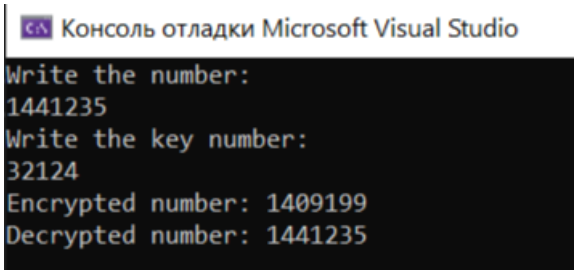
Задание №1. Шифрование двух целых чисел

Листинг 1 – Метод для шифрования двух целых чисел

```
public static string EncryptNum(uint num, uint key)
    => Convert.ToString(num ^ key);
```

Демонстрационный пример:



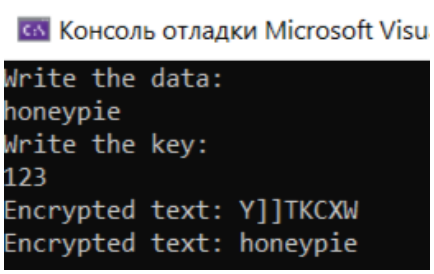


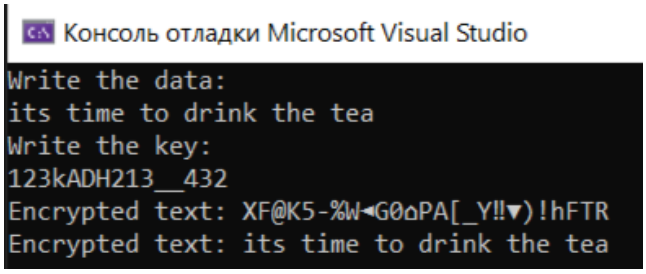
Задание №2. Шифрование строки символов

Листинг 2 – Метод для шифрования строки символов

```
public static string EncryptText(string data, string key)
{

    byte[] result;

    var numArr = Encoding.UTF8.GetBytes(data);
    var keyArr = Encoding.UTF8.GetBytes(key);

    result = new byte[data.Length];

    for (int i = 0; i < data.Length; i += key.Length)
    {
        for (int j = 0; j < key.Length; j++)
        {
            if (i + j < data.Length)
                result[i + j] = (byte)(data[i + j] ^ key[j]);
        }
    }
    return Encoding.UTF8.GetString(result);
}
```

Демонстрационный пример:



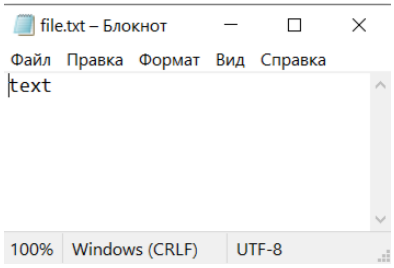


Задание №3. Шифрование файлов

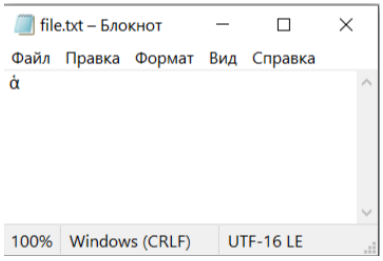
Листинг 3 – Метод для шифрования файлов

```
public static byte[] EncryptFile(string path, string key){
    byte[] data = File.ReadAllBytes(path);
    var result = new byte[data.Length];
    for (int i = 0; i < data.Length; i+= key.Length)
    {
        for (int j = 0; j < key.Length; j++)
        {
            if (i + j < data.Length)
                result[i+j] = (byte)(data[i+j] ^ key[j]);
        }
    }
    return result;
}
```

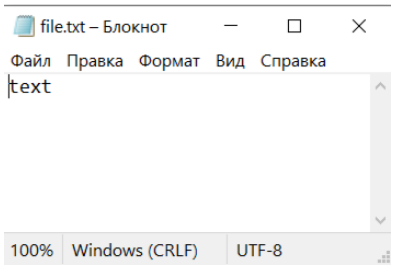
До шифрования:



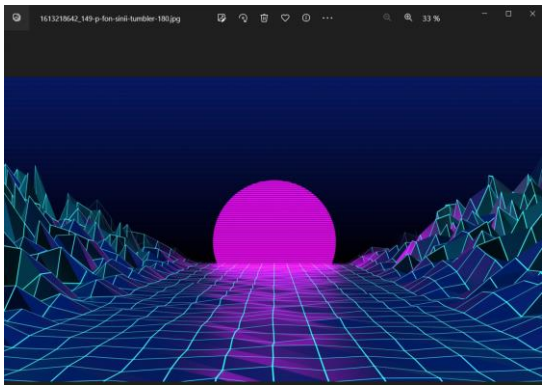
После шифрования:



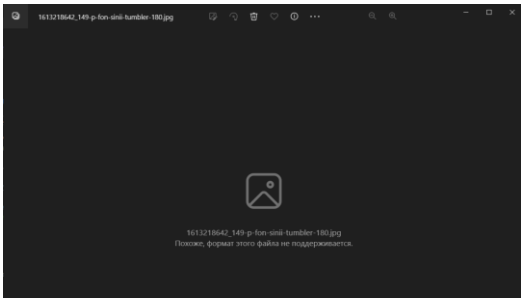
Повторное шифрование:



До шифрования:



После шифрования:



Повторное шифрование: