

# ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМОВ ШИФРОВАНИЯ ЗАМЕНОЙ

## Вариант №3

отчет о лабораторной работе №3  
по дисциплине  
*МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ  
ИНФОРМАЦИИ*

Выполнила \_\_\_\_\_

ст. гр. №230711, Павлова В.С.

Проверила \_\_\_\_\_

доцент каф. ИБ, Басалова Г.В.

## ХОД РАБОТЫ

**Задание.** Реализовать программно алгоритм шифрования по таблице Вижинера. Слово-ключ задаётся с клавиатуры.

### Листинг 1 – Программная реализация алгоритма шифрования

```
public static byte[] Encode(byte[] input, byte[] key)
{
    byte[] result = new byte[input.Length];
    int keyCharIndex = 0;
    for (int i = 0; i < input.Length; i++)
    {
        //формула вычисления сдвига
        //сдвиг = (код исходного симв. + код ключа) / мощность алф
        int movementCount = (input[i] + key[keyCharIndex]) % 256;

        result[i] = (byte)movementCount;

        keyCharIndex++;

        if ((keyCharIndex + 1) == key.Length)
            keyCharIndex = 0;
    }
    return result;
}
```

### Листинг 2 – Программная реализация алгоритма дешифрования

```
public static byte[] Decode(byte[] input, byte[] key)
{
    byte[] result = new byte[input.Length];
    int keyCharIndex = 0;
    for(int i = 0; i < input.Length; i++)
```

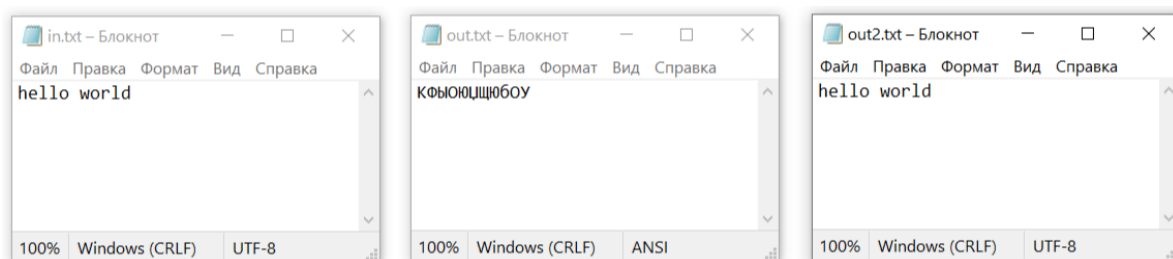
## Листинг 2 – Программная реализация алгоритма дешифрования (продолжение)

```
{    //формула обратного сдвига
    //сдвиг = (код исходного симв. + мощность - код ключа) / мощность
    int movementCount = (input[i] + 256 - key[keyCharIndex]) % 256;

    result[i] = (byte)movementCount;
    keyCharIndex++;
    if ((keyCharIndex + 1) == key.Length)
        keyCharIndex = 0;
}

return result;
}
```

### Демонстрационный пример №1. Файл .txt, ключ $k = \text{book}$

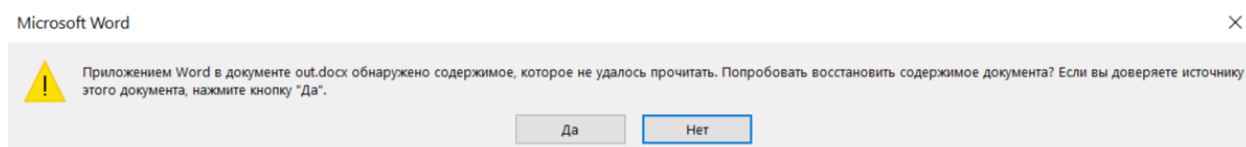


### Демонстрационный пример №2. Файл .jpg, ключ $k = \text{sobaka}$



### Демонстрационный пример №3. Файл .docx, ключ $k = \text{cat\_34}$

Зашифрованный файл не открылся:



После расшифрования все работает:

