**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОН АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕУЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»**

**РУТ (МИИТ)**

**Кафедра «Цифровые технологии управления транспортными процессами»**

**Отчёт**

**По лабораторной работе №1**

**по дисциплине**

**«Основы информационной безопасности»**

**Тема: «Одноалфавитная подстановка»**

**Вариант №28**

Выполнил: ст. гр. УИС-211

Чаругин А. М.

Проверил: Цыганова Н. А.

Панькина К. Е.

**МОСКВА**

**2022**

**Оглавление**

[Теоретическое описание метода шифрования 3](#_Toc119183129)

[Подстановка задачи 3](#_Toc119183130)

[**Исходное сообщение 3**](#_Toc119183131)

[**Ключ 3**](#_Toc119183132)

[**Криптографическое преобразование 3**](#_Toc119183133)

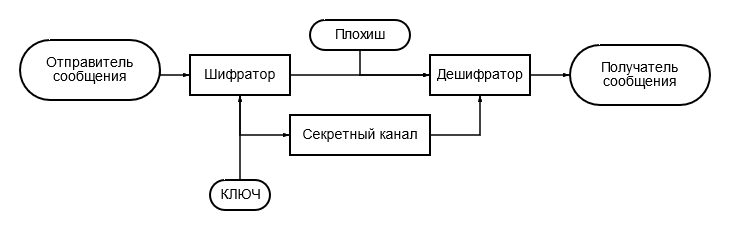
[**Криптограмма 3**](#_Toc119183134)

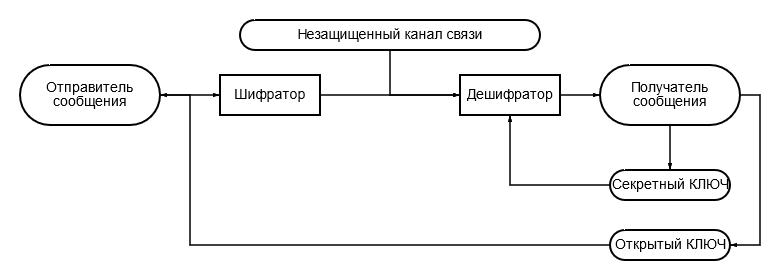
[**Алгоритм разработанной программы 3**](#_Toc119183135)

[Код программы 3](#_Toc119183136)

[Результаты работы программы 3](#_Toc119183137)

## Теоретическое описание метода шифрования

 **Симметричное шифрование** – это способ шифрования данных, при котором один и тот же ключ используется и для кодирования, и для восстановления информации.

**Aсимметричное шифрование** – решает главную проблему симме- тричного шифрования, при котором для кодирования и восстановления данных используется один и тот же ключ. Если передавать этот ключ по незащищенным каналам, его могут перехватить и получить доступ к зашифрованным данным. Асимметричные алгоритмы медленнее симметричных, поэтому во многих криптосистемах применяются и те и другие. Наиболее популярные алгоритмы асимметричные шифрования RSA, DSA, Схема Эль-Гамаля, ECDSA.

## Подстановка задачи

### Исходное сообщение

Существует два класса криптосистем: симметричные (одноключевые) и асимметричные (двухключевые).

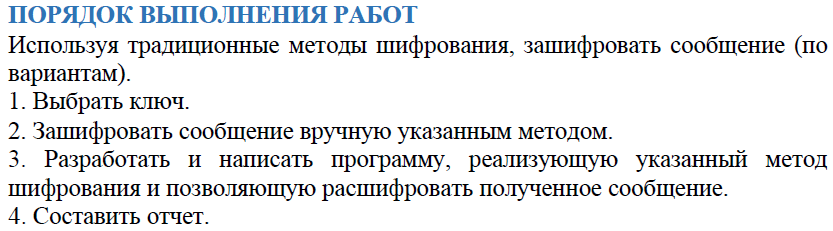
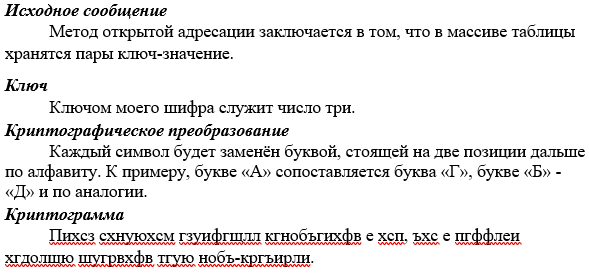
### Ключ

Ключом моего шифра служит число 28.

### Криптографическое преобразование

### Криптограмма

### Алгоритм разработанной программы



## Код программы

**print**('выберите тип шифрования (s) - симметричное или (as) - асимметричное')

a = str(input('Напишите s или as'))

**if** a == 's':

**print**('Выбранный тип шифрования - симметричное'***)***

    IZHODNIK = 'Существует два класса криптосистем: симметричные (одноключевые) и асимметричные (двухключевые).'

    key = [28]

    print('�сходное сообщение: ', IZHODNIK)

    print('Ключ - ', key)

    text = []

    for \_\_ in list(IZHODNIK):

     text.append(ord(\_\_)) # ord() - представление слова, как числ�***�***

    print('после перевода текста в цифры: ', text)

    etext = []

    \_\_key = 0

    for \_\_ in range(0,len(text)):

     etext.append(text[\_\_]+key[\_\_key])

     if \_\_key == len(key)-1:

     \_\_key = 0

     Else:

     \_\_key+=1

    print('Результат работы шифратора: ', etext)

    unetext = []

    \_\_key = 0

    for \_\_ in range(0,len(etext)):

     unetext.append(chr(etext[\_\_]-key[\_\_key]))

     if \_\_key == len(key)-1:

     \_\_key = 0

     Else:

     \_\_key+=1

    print('Результат работы дешифратора: ', unetext)

print('выберите тип шифрования (s) - симметричное или (as) - асимметричное')

a = str(input('Напишите s или as'))

if a == 's':

print('Выбранный тип шифрования - симметричное')

IZHODNIK = 'Существует два класса криптосистем: симметричные (одноключевые) и асимметричные (двухключевые).'

key = [28]

print('Исходное сообщение: ', IZHODNIK)

print('Ключ - ', key)

text = []

for \_\_ in list(IZHODNIK):

text.append(ord(\_\_)) # ord() - представление слова, как число

print('после перевода текста в цифры: ', text)

etext = []

\_\_key = 0

for \_\_ in range(0,len(text)):

etext.append(text[\_\_]+key[\_\_key])

if \_\_key == len(key)-1:

\_\_key = 0

else:

\_\_key+=1

print('Результат работы шифратора: ', etext)

unetext = []

\_\_key = 0

for \_\_ in range(0,len(etext)):

unetext.append(chr(etext[\_\_]-key[\_\_key]))

if \_\_key == len(key)-1:

\_\_key = 0

else:

\_\_key+=1

print('Результат работы дешифратора: ', unetext)

## Результаты работы программы