**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»**

**РУТ (МИИТ)**

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

**Отчёт**

**По лабораторной работе №5**

**по дисциплине**

**«Основы информационной безопасности»**

**Тема: «Простая перестановка»**

**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](#__RefHeading___1)

[Подстановка задачи 4](#__RefHeading___2)

[Исходное сообщение + 4](#__RefHeading___3)

[Ключ 4](#__RefHeading___4)

[Криптографическое преобразование 4](#__RefHeading___5)

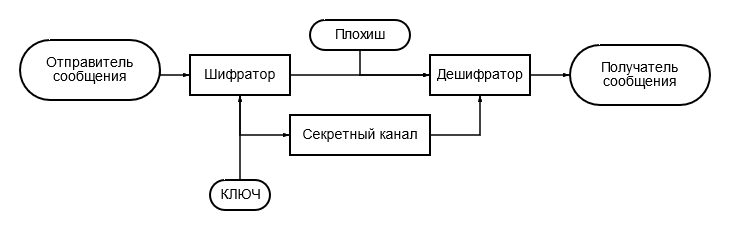
[Криптограмма 4](#__RefHeading___6)

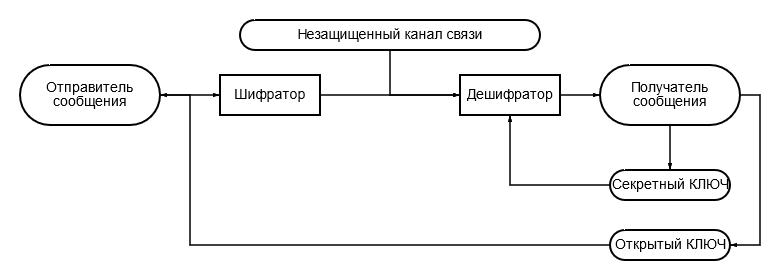
[Алгоритм разработанной программы 4](#__RefHeading___7)

[Код программы 5](#__RefHeading___8)

[Результаты работы программы 6](#__RefHeading___9)

## 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 +

Механизмы подстановки трафика используются для реализации слу

### Ключ

Ключом моего шифра служит число 28.

### Криптографическое преобразование

### Криптограмма

### Алгоритм разработанной программы

## Код программы

## Результаты работы программы