

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ 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

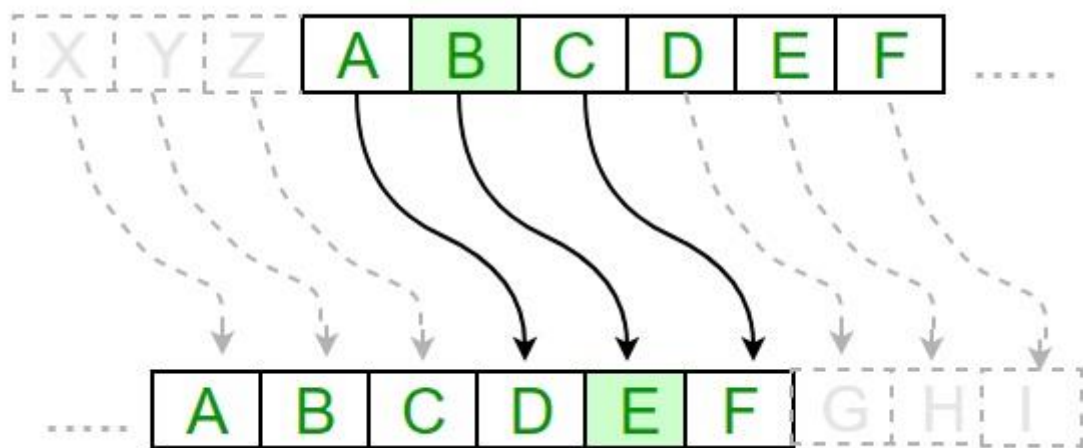
2022

Оглавление

Теоретическое описание метода шифрования.....	3
Подстановка задачи	4
<i>Исходное сообщение.....</i>	<i>4</i>
<i>Ключ</i>	<i>4</i>
<i>Криптографическое преобразование</i>	<i>4</i>
<i>Криптограмма.....</i>	<i>4</i>
<i>Алгоритм разработанной программы</i>	<i>4</i>
Код программы	6
Результаты работы программы	6

Теоретическое описание метода шифрования

Одноалфавитная подстановка (Простейшая подстановка) – это шифр, при котором каждый символ открытого текста заменяется на некоторый, фиксированный при данном ключе символ того же алфавита.



Каждая буква обычного текста заменяется буквой с фиксированным числом позиций вниз по алфавиту.

Подстановка задачи

Исходное сообщение

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

Ключ

Ключ вводится с клавиатуры пользователем.

Криптографическое преобразование

В программе выполняется поиск нужного для шифрования символа в алфавите.

(Наш алфавит: " () : ! _ ? < > . , - а б в г д е ё ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я ")).

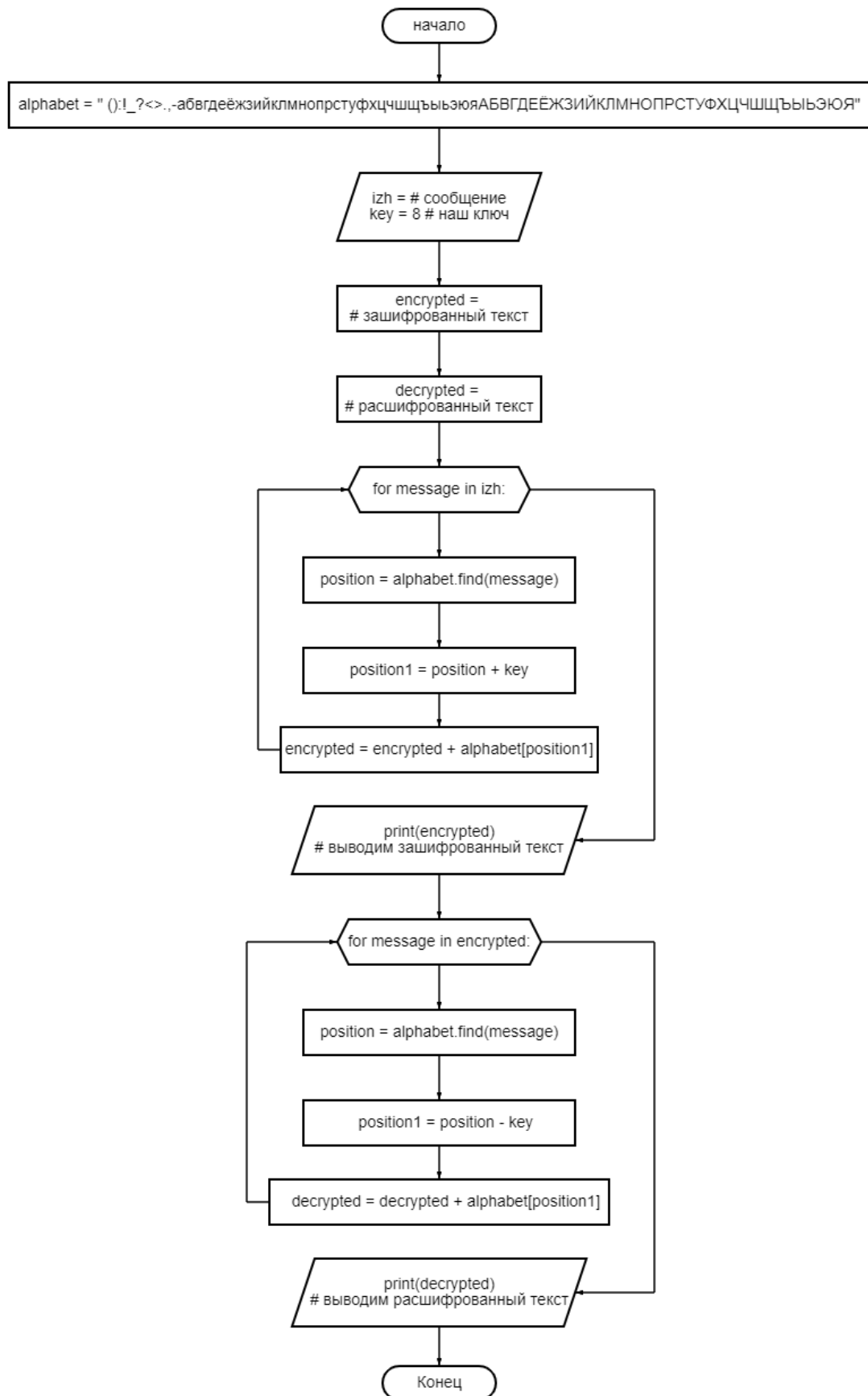
Берется индекс найденного символа и к нему прибавляется ключ в виде целого числа. Получаем новый зашифрованный символ, который записывается в переменную, в которой получится новое предложение.

Для расшифровки выполняется точно такая же операция, только теперь ключ не прибавляется, а вычитается.

Криптограмма

ЩыБмщъйымъ>лйз>тузщщз>тшрчъщрщъмф-
>щрффъмьшряхГм>.цлхцтуЁямйГм,>р>зщрффъмьшряхГм>.лйыэтуЁямйГм,е

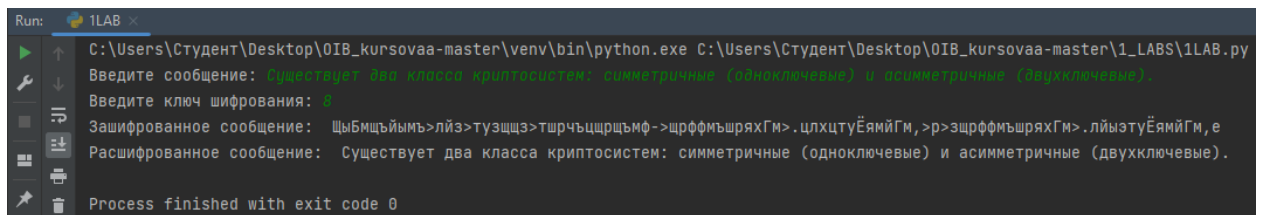
Алгоритм разработанной программы:



Код программы

```
alphabet = " () : ! _ ? < > . , -  
абвгдеёжзийклмнопрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"  
izh = input("Введите сообщение: ")  
key = int(input("Введите ключ шифрования: "))  
encrypted = ""  
decrypted = ""  
  
for message in izh:  
    position = alphabet.find(message)  
    position1 = position + key  
    encrypted = encrypted + alphabet[position1]  
print("Зашифрованное сообщение: ", encrypted)  
  
for message in encrypted:  
    position = alphabet.find(message)  
    position1 = position - key  
    decrypted = decrypted + alphabet[position1]  
print("Расшифрованное сообщение: ", decrypted)
```

Результаты работы программы



```
Run: 1LAB x  
C:\Users\Студент\Desktop\0IB_kursova-master\venv\bin\python.exe C:\Users\Студент\Desktop\0IB_kursova-master\1_LABS\1LAB.py  
Введите сообщение: Существует два класса криптосистем: симметричные (одноключевые) и асимметричные (двухключевые).  
Введите ключ шифрования: 0  
Зашифрованное сообщение: ЩыБмцъймъ>лйз>тузщз>тшрчъцщрцъмф->щрфмъшряхГм>.цлхцтуЁямйГм,>р>эщрфмъшряхГм>.лйызтуЁямйГм,е  
Расшифрованное сообщение: Существует два класса криптосистем: симметричные (одноключевые) и асимметричные (двухключевые).  
Process finished with exit code 0
```