#### Министерство науки и высшего образования Российской Федерации

#### Федеральное государственное бюджетное образовательное учреждение науки и высшего образования

#### «Владимирский государственный университет

#### имени Александра Григорьевича и Николая Григорьевича Столетовых»

**(ВлГУ)**

**Кафедра информационных систем и программной инженерии**

Лабораторная работа № 04

по дисциплине

"Администрирование и безопасность программно-информационных систем"

Тема: "Алгоритм Виженера"

Выполнил:

ст. гр. ПРИ-117

В.Г. Хлызова

Принял:

И.В. Спирин

Владимир, 2020 г.

## ЦЕЛЬ РАБОТЫ

Целью работы является реализация криптографического алгоритма шифрования с использованием открытого текста в качестве ключа по таблице Виженера.

ХОД РАБОТЫ

Задание 1: Зашифруйте с помощью алгоритма Виженера следующую последовательность:

Ей рано нравились романы

Они ей заменяли всё

Она влюблялася в обманы

И Ричардсона и Руссо

Ключ «идеал»

1. Сдвигаем алфавит



1. Исходный текст разбиваем на группы по 5 символов

ейран онрав ились роман ыоние йзаме нялив сёона влюбл ялася вобма ныири чардс онаир уссо

1. Заменяем символы каждой группы на соответствующие символы из словаря

ннхащ чсхан спнсз щтсащ дттир тлемр цгрин ъиунл кпгбч зпеск ктёмл цянрф адхдэ чсеиь ьхцо

1. Возвращаем текст к исходному форматированию

Нн хащч сханспнсз щтсащд

Тти рт лемрцгри нъи

Унл кпгбчзпеск к тёмлця

Н рфадхдэчсе и ььхцо

Задание 2: Расшифруйте с помощью алгоритма Виженера следующую последовательность:

Фу эъцё сйу дюсягм ьръгм

С аяцшффжмм схщм зпаэпдпьйс

Ню т щхитрд хе сщтзл сбула

Ключ «проза»

1. Сдвигаем алфавит



1. Разбиваем текст на группы

фуэъц ёсйуд юсягм ьръгм саяцш ффжмм схщмз паэпд пьйсн ютщхи трдхе сщтзл сбула

1. Заменяем символы каждой группы на соответствующие символы из алфавита

еготц цбылд обрым малым впрош едшем векез апозд алыйн овкни гахне видал вреда

1. Возвращаем текст к исходному форматированию

Ег отцц был добрым малым

В прошедшем веке запоздалый

Но в книгах не видал вреда

Задание 3: Напишите алгоритм и программу для шифрования/дешифрования строк алгоритмом Виженера.

alphabet=**"абвгдеёжзийклмнопрстуфхцчшщъыьэюя"**signs=[**" "**,**";"**,**","**,**":"**,**"-"**,**"!"**,**"?"**, **"\""**, **"."**]  
  
*# Сдвигаем алфавит и генерируем словарь***def** creating\_dictionary(key):  
 key=key.lower()  
 dictionary = []  
 **for** i **in** key:  
 temporary\_dictionary=alphabet[alphabet.index(i):alphabet.index(**"я"**)]+**"я"**+alphabet[alphabet.index(**"а"**):alphabet.index(i)]  
 dictionary.append(temporary\_dictionary)  
 print(temporary\_dictionary)  
 **return** dictionary  
  
*# Переводим введенную фразу в нижний регистр, удаляем пробелы и знаки препинания***def** share\_phrase(phrase, numberOfLetters):  
 phrase=phrase.lower()  
 **for** i **in** signs:  
 phrase=phrase.replace(i, **''**)  
 phrase=[phrase[i:i+numberOfLetters] **for** i **in** range(0, len(phrase), numberOfLetters)]  
 **return** phrase  
  
*# Метод шифрования***def** encryption(dictionary,word,numberOfLetters):  
 j=0  
 encrypted\_word=**""  
 while** j<numberOfLetters:  
 **for** i **in** word:  
 index=alphabet.index(i)  
 encrypted\_word+=dictionary[j][index]  
 j+=1  
 **return** encrypted\_word  
  
*# Метод дешифрования***def** decode(dictionary,word,numberOfLetters):  
 j=0  
 encrypted\_word=**""  
 while** j<numberOfLetters:  
 **for** i **in** word:  
 index=dictionary[j].index(i)  
 encrypted\_word+=alphabet[index]  
 j+=1  
 **return** encrypted\_word  
  
*# Форматирование строки***def** formatting(phrase, source\_phrase):  
 index=0  
 phrase\_array=list(phrase)  
 **for** i **in** source\_phrase:  
 **for** s **in** signs:  
 **if** i==s:  
 phrase\_array.insert(index,s)  
 index += 1  
 phrase=**""**.join(phrase\_array)  
 **return** phrase  
  
phrase = input(**"Введите фразу: "**)  
source\_phrase=phrase  
key = input(**"Введите ключ шифрования: "**)  
  
print(**"\nСдвигаем словарь"**)  
dictionary=creating\_dictionary(key)  
  
print(**"\nРазбиваем текст на группы"**)  
phrase =share\_phrase(phrase, len(key))  
print(phrase)  
  
choice = input(**"\nВыбирите действие:\n"  
 " 1: Зашифровать\n"  
 " 2: Дешифровать\n"**)  
  
encrypted\_keyword = []  
  
**if** choice==**"1"**:  
 print(**"\nЗаменяем символы каждой группы на соответствующие символы из словаря"**)  
 **for** i **in** phrase:  
 encrypted\_keyword.append(encryption(dictionary, i, len(key)))  
 print(encrypted\_keyword)  
**elif** choice==**"2"**:  
 print(**"\nЗаменяем символы каждой группы на соответствующие символы из алфавита"**)  
 **for** i **in** phrase:  
 encrypted\_keyword.append(decode(dictionary, i, len(key)))  
 print(encrypted\_keyword)  
**else**:  
 print(**"Вы ввели неверный символ ((("**)  
  
print(**"\nВозвращаем текст к исходному форматированию"**)  
phrase=**""**.join(encrypted\_keyword)  
phrase=formatting(phrase, source\_phrase)  
print(phrase)

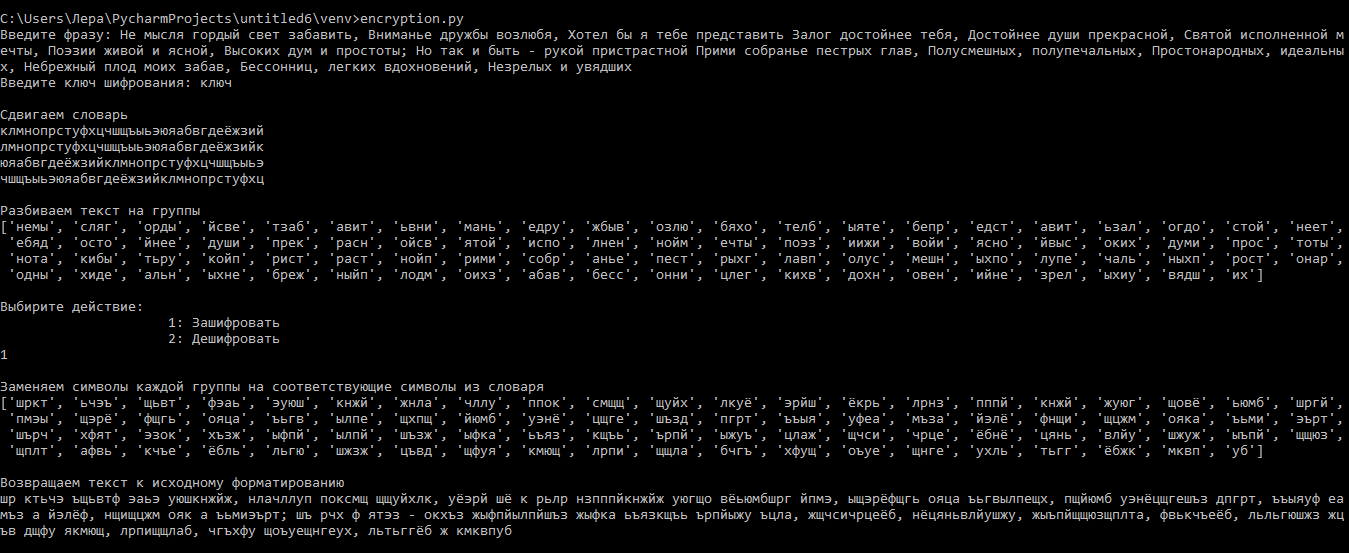


Рисунок 1. Результат выполнения шифрования.

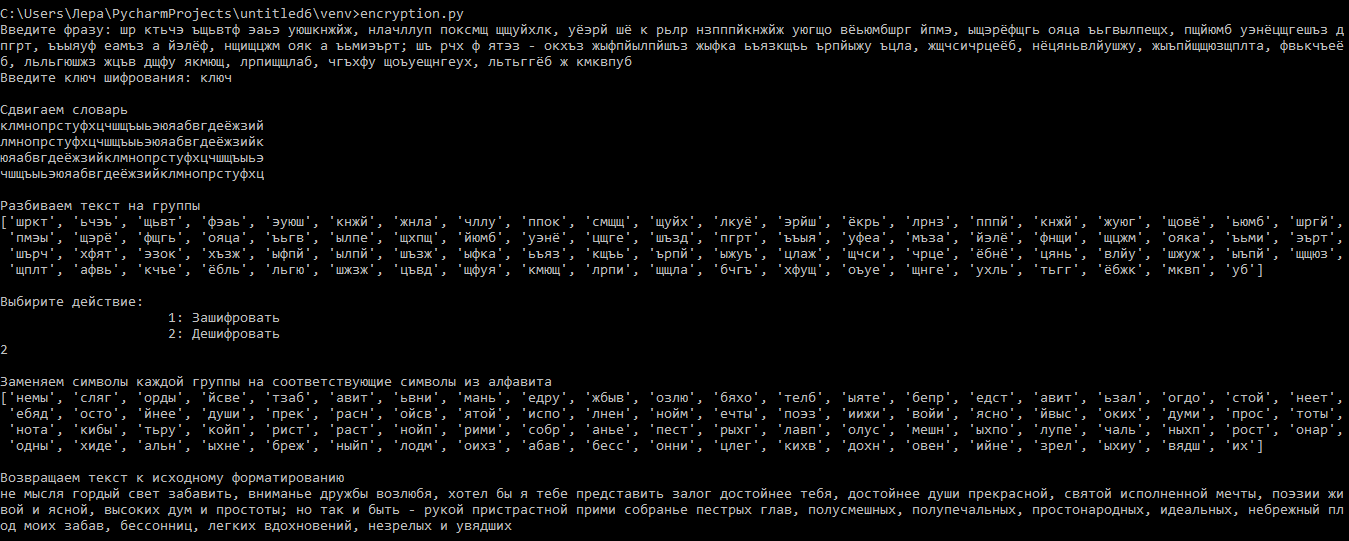


Рисунок 2. Результат выполнения дешифрования.

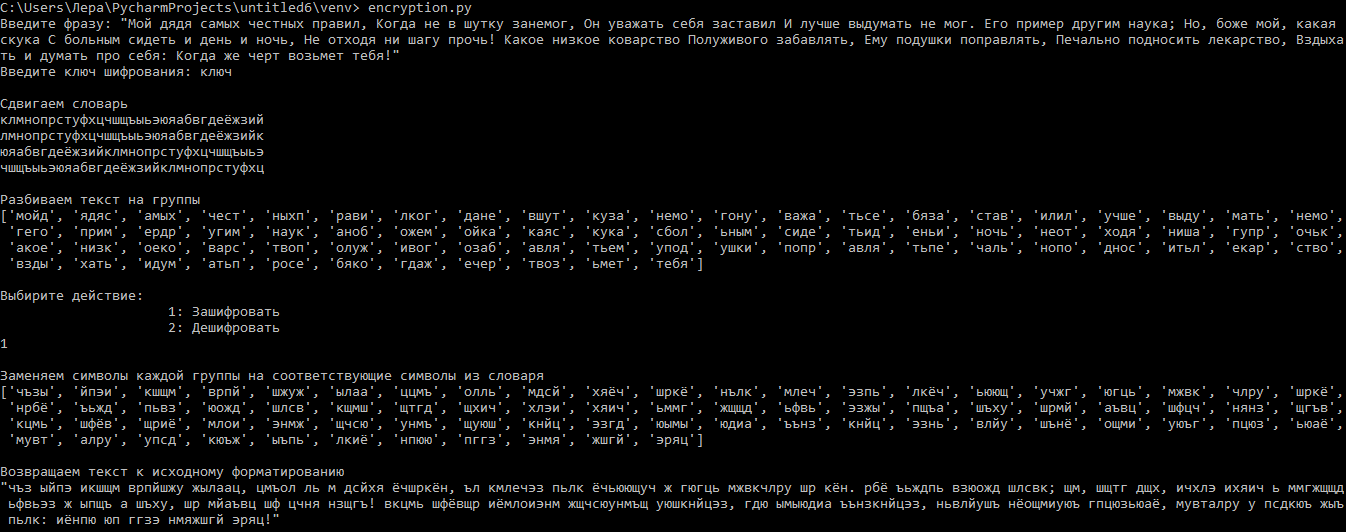


Рисунок 3. Результат выполнения шифрования.

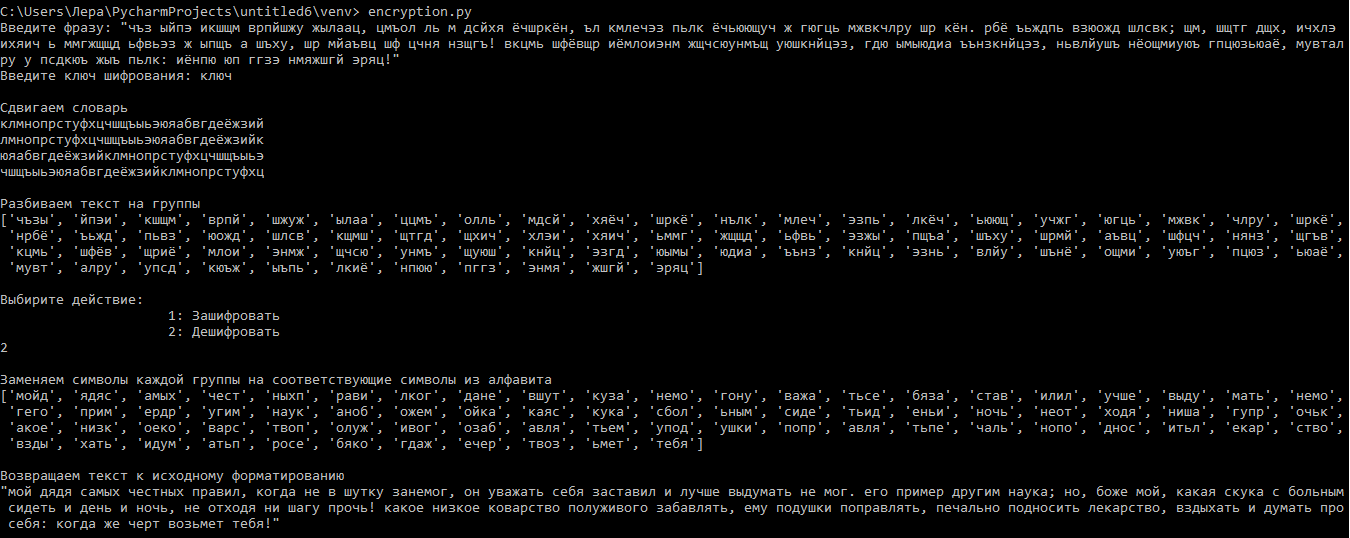


Рисунок 4. Результат выполнения дешифрования.

ВЫВОД

В ходе лабораторной работы была изучена реализация криптографического алгоритма шифрования с использованием открытого текста в качестве ключа по таблице Виженера.