Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

КАФЕДРА ИНФОРМАТИКИ

Лабораторная работа № 1

Шифр Цезаря. Шифр Виженера

Выполнила студентка гр. 053503

Зырянова М. М.

Проверил

Протько М. И.

Минск 2023

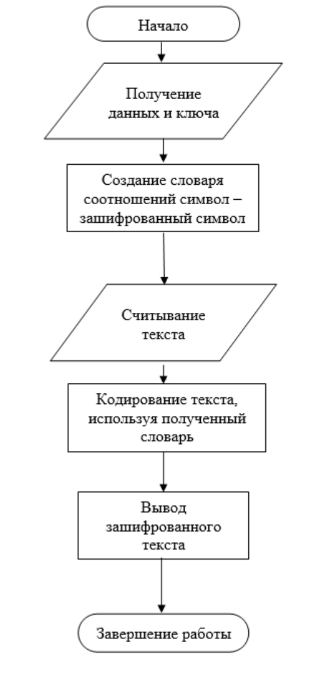
# **1. Введение**

Целью данной лабораторной работы было изучить и реализовать программные средства шифрования и дешифрования текстовых файлов при помощи Шифра Цезаря и шифра Вижинера.

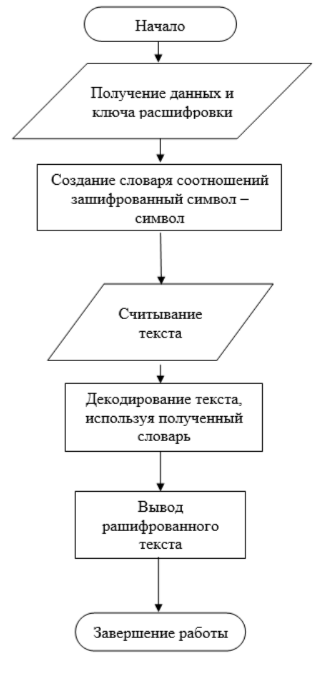
# **2. Блок-схема алгоритма**

**2.1. Шифр Цезаря:**

Общая блок-схема алгоритма кодирования для шифра Цезаря.

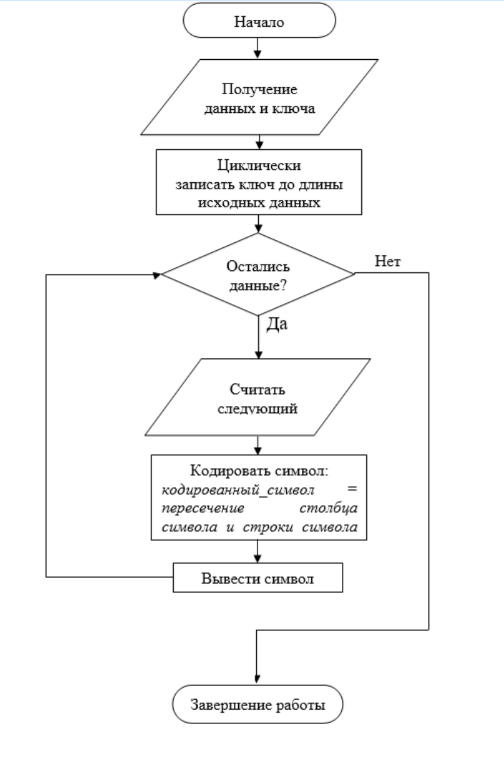


Общая блок-схема алгоритма декодирования для шифра Цезаря.

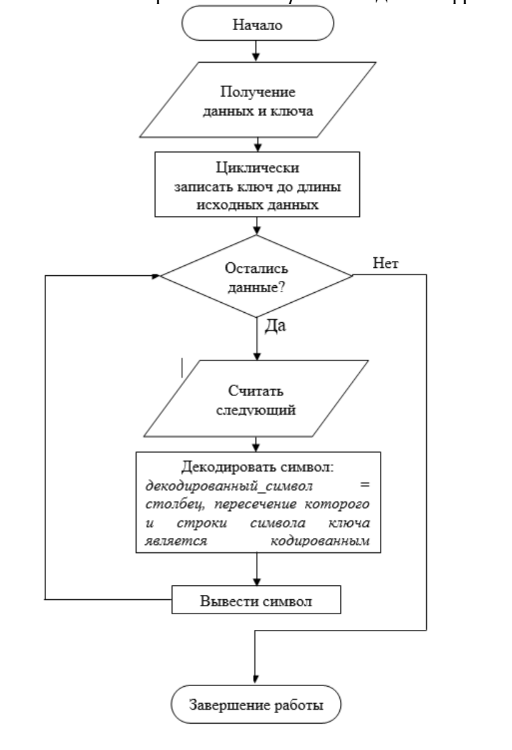
****

**2. Шифр Виженера**

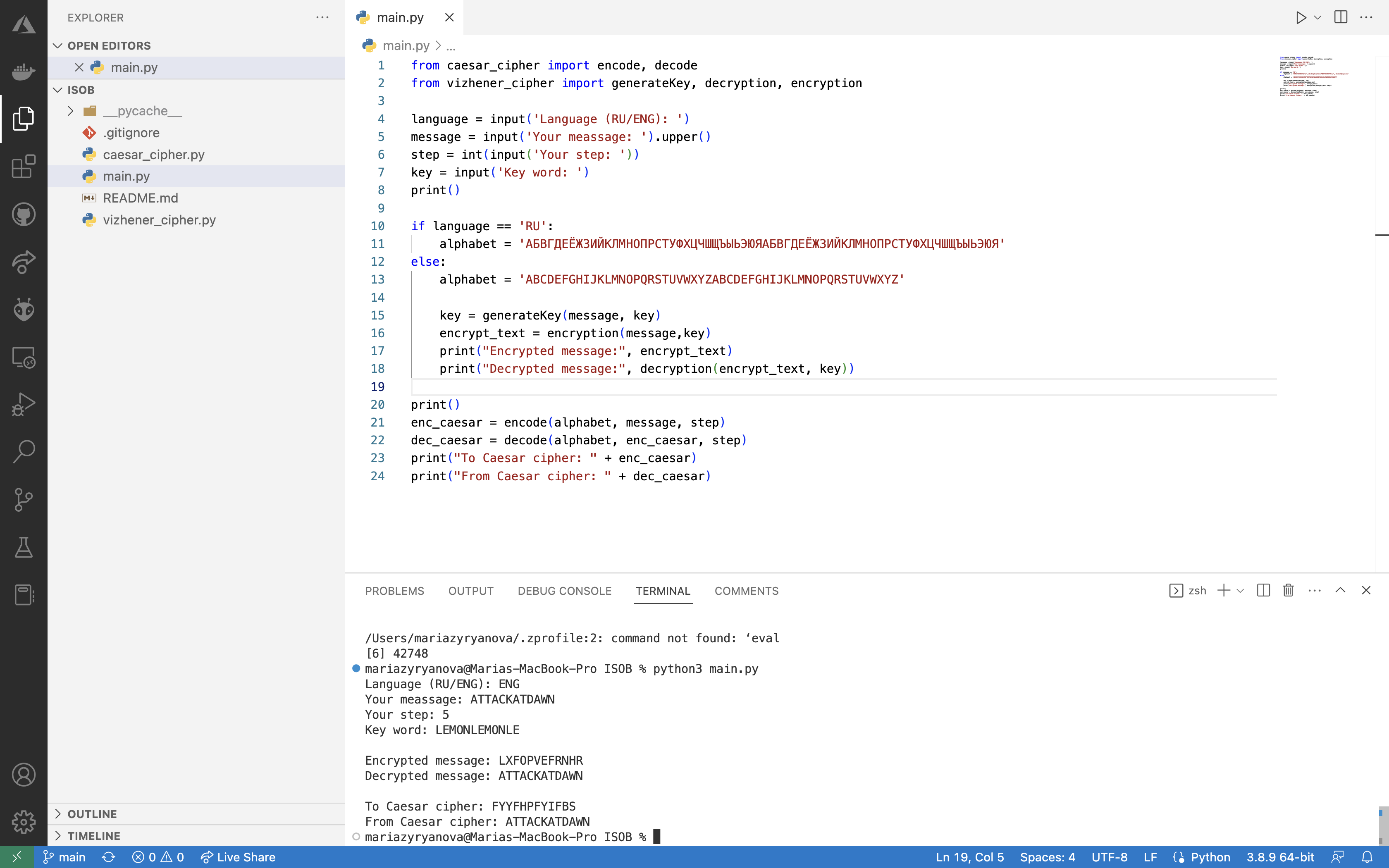
Общая блок-схема алгоритма кодирования для шифра Виженера.

****

Общая блок-схема алгоритма декодирования для шифра Виженера.



**3. Результаты работы программы**



**4. Код программы**

caesar\_cipher.py

def encode(alphabet: str, input: str, step: int) -> str:

output = ''

for i in input:

position = alphabet.find(i)

new\_position = step + position

if i in alphabet:

output += alphabet[new\_position]

else:

output += i

return output

def decode(alphabet: str, input: str, step: int) -> str:

output = ''

for i in input:

position = alphabet.find(i)

new\_position = position - step

if i in alphabet:

output += alphabet[new\_position]

else:

output += i

return output

vizhener\_cipher.py

def generateKey(string, key):

key = list(key)

if len(string) == len(key):

return(key)

else:

for i in range(len(string) -len(key)):

key.append(key[i % len(key)])

return("" . join(key))

def encryption(string, key):

encrypt\_text = []

for i in range(len(string)):

x = (ord(string[i]) +ord(key[i])) % 26

x += ord('A')

encrypt\_text.append(chr(x))

return("" . join(encrypt\_text))

def decryption(encrypt\_text, key):

orig\_text = []

for i in range(len(encrypt\_text)):

x = (ord(encrypt\_text[i]) -ord(key[i]) + 26) % 26

x += ord('A')

orig\_text.append(chr(x))

return("" . join(orig\_text))

main.py

from caesar\_cipher import encode, decode

from vizhener\_cipher import generateKey, decryption, encryption

language = input('Language (RU/ENG): ')

message = input('Your meassage: ').upper()

step = int(input('Your step: '))

key = input('Key word: ')

print()

if language == 'RU':

alphabet = 'АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ'

else:

alphabet = 'ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ'

key = generateKey(message, key)

encrypt\_text = encryption(message,key)

print("Encrypted message:", encrypt\_text)

print("Decrypted message:", decryption(encrypt\_text, key))

print()

enc\_caesar = encode(alphabet, message, step)

dec\_caesar = decode(alphabet, enc\_caesar, step)

print("To Caesar cipher: " + enc\_caesar)

print("From Caesar cipher: " + dec\_caesar)