МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

## Факультет информационных технологий и робототехники

Кафедра программного обеспечения вычислительной техники

и автоматизированных систем

**Отчет по лабораторной работе № 1**

по дисциплине: ”Теория информации”

на тему: ***”Изучение криптографических систем, основанных на методе подстановки”***

Выполнил**:** студент группы *10701118* Воробей И.А.

Алейников Д.В.

Приняла**:** доц. Нессенчук А.А.

Минск 2019

# Лабораторная работа № 1.Изучение криптографических систем, основанных на методе подстановки

Цель работы: Изучение способов шифрования информации в криптографических системах, основанных на методе подстановки

Краткие теоретические сведения:

Криптографические системы, основанные на методе подстановки, разделяются на четыре основных класса (monoalphabetic, homophonic, polyalphabetic, polygram).

В системах класса monoalphabetic символ исходного текста заменяется другим символом таким образом, что между ними существует однозначное соответствие.

Существует алгоритм Цезаря, где i-ая буква алфавита заменяется (i+k)-й буквой по модулю 26. В криптографических системах класса homophonic имеются несколько вариантов замены исходного символа. Буква А может быть зашифрована как (37,17,24)

Криптографические системы класса polyalphabetic основаны на использовании нескольких различных ключей. Большинство шифраторов подобного типа являются периодическими с периодом Р.

Криптографические системы класса polygram характерезуются подстановкой не одного, а нескольких символов в исходном тексте. В общем случае n символ исходного текста заменяются n символами шифротекста.

## Задание на выполнение работы:

1) Реализовать алгоритмы и программу шифрования исходного текста (на базе произвольно выбранного алфавита) в системе класса monoalphabetic.

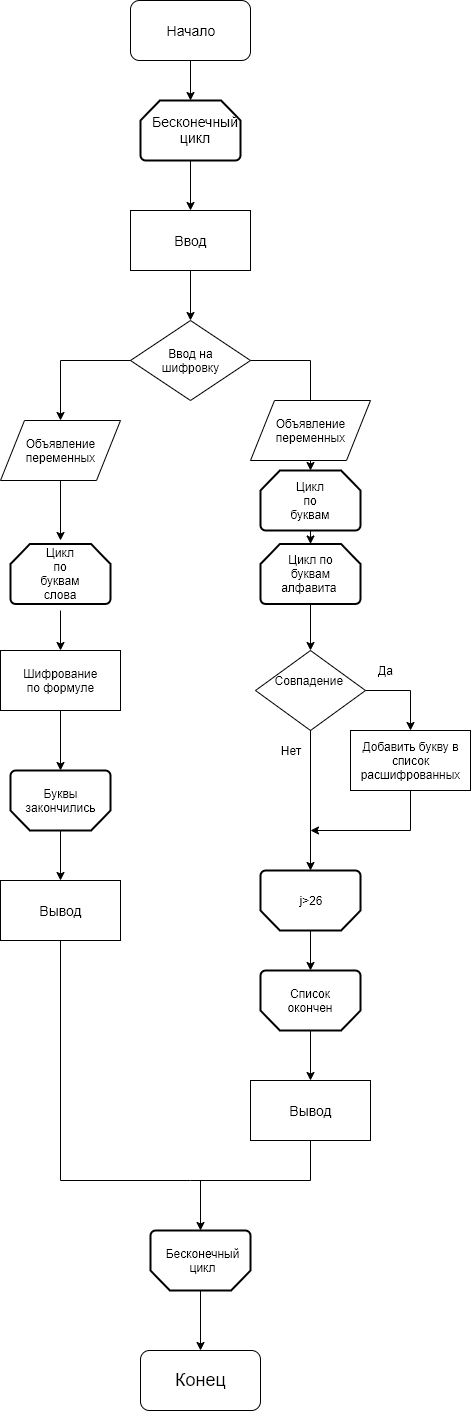
Алгоритм шифрования реализовать с использованием

-формулы (1.3) Ek(i)=(i\*k)mod n;

2) Реализовать алгоритм и программу дешифрования сформированного согласно пункту 1 шифротекста.

Алгоритм дешифрования должен быть разработан самостоятельно. Алгоритм может быть реализован, как на основе формулы, так и с использованием логико-смыслового анализа исходных данных задачи.

**Алгоритм решения поставленной задачи:**

****

**Текст программы:**

list1=['a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z']

def Search1(y):

for i in range(26):

if y == list1[i]:

return i

def encription(text):

j = 0

key = 3

n = 26

p=[]

Newlist=[]

for i in text:

x = Search1(i)\*key % n

p=list1[x]

Newlist.append(p)

''.join(Newlist)

return Newlist

def deincription(Newlist):

Endlist=[]

key = 3

n = 26

for i in Newlist:

for j in range(26):

if i==''.join(encription(list1[j])):

Endlist.append(list1[j])

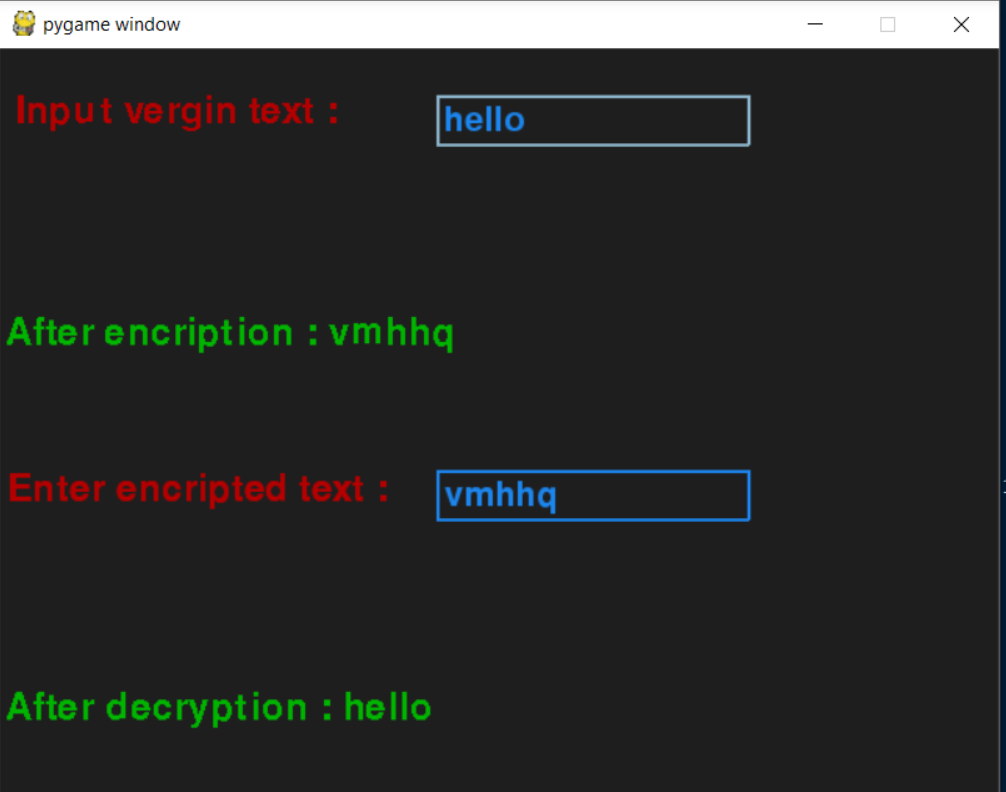
return Endlist

**Описание входных /выходных данных:**

Вводим слово на английском языке в малом регистре. Верхнее окно выводим после введения нажимаем Enter и в следующей строке появляется закодированное слово.

В 2 окно вводим закодированное слово, после нажатия Enter в следующей строке выводиться шифрование.

**Контрольный пример:**



**Вывод:** Изучили способы шифрования информации в криптографических системах, основанных на методе подстановки.

**Список литературы:**

1)Шеннон К.Работы по теории информации и кибернетике.

# 2)Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях.

3) Чмора А.Л. Современная прикладная криптография