|  |  |
| --- | --- |
| **Gerb-BMSTU_01** | **Министерство науки и высшего образования Российской Федерации**  Калужский филиал  федерального государственного бюджетного  образовательного учреждения высшего образования  ***«Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»***  ***(КФ МГТУ им. Н.Э. Баумана)*** |

**ФАКУЛЬТЕТ** \_***ИУК «Информатика и управление»*\_\_**\_\_\_\_\_\_\_\_\_\_\_\_

**КАФЕДРА** \_\_***ИУК4 «Программное обеспечение ЭВМ, информационные технологии»***

**ЛАБОРАТОРНАЯ РАБОТА №8**

**«Python. Простые методы шифрования: метод Цезаря, Полибианский квадрат, метод Виженера»**

**ДИСЦИПЛИНА: «Высокоуровневое программирование»**

|  |  |  |
| --- | --- | --- |
| Выполнил: студент гр. ИУК4-32Б | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ( Карельский М.К. )  (Подпись) (Ф.И.О.) |
| Проверил: | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ( Ерохин И.И. )  (Подпись) (Ф.И.О.) |
| Дата сдачи (защиты):  Результаты сдачи (защиты): | | |
|  | - Балльная оценка:  - Оценка: | |
| Калуга , 2021 | | |

**Цель:** приобретение навыков работы по трем методам простого шифрования.

**Задание:**

Реализовать программы кодирования и декодирования:

1. Методом Цезаря (ключ = порядковый номер студента по списку группы, фраза для шифрования = любое словосочетание);
2. Полибианским квадратом (в начале пишется фамилия и имя студента, фраза для шифрования = любое словосочетание);
3. Методом Вижинера (ключ = фамилия и имя студента, фраза для шифрования = любое словосочетание).

**Листинг:**

*Задача 1*

key = 10

phrase = input('Введите сообщение: ').lower()

cypher = ''

for i in range(len(phrase)):

if phrase[i].isalpha():

if ord(phrase[i]) + key > 122:

cypher += chr(ord(phrase[i]) + key - 26)

else:

cypher += chr(ord(phrase[i]) + key)

else:

cypher += phrase[i]

print('Зашифрованное сообщение:', cypher)

message = ''

for i in range(len(cypher)):

if phrase[i].isalpha():

if ord(cypher[i]) - key < 97:

message += chr(ord(cypher[i]) - key + 26)

else:

message += chr(ord(cypher[i]) - key)

else:

message += cypher[i]

print('Дешифрованное сообщение:', message)

*Задача 2*

matrix = [['а', 'е', 'и', 'й', 'к', 'л'],

['м', 'р', 'с', 'х', 'ь', 'б'],

['в', 'г', 'д', 'ё', 'ж', 'з'],

['н', 'о', 'п', 'т', 'у', 'ф'],

['ц', 'ч', 'ш', 'щ', 'ъ', 'ы'],

['э', 'ю', 'я', ' ', '', '']]

phrase = input('Введите сообщение: ').lower()

cypher = []

for p in range(len(phrase)):

isFound = False

for i in range(6):

for j in range(6):

if phrase[p] == matrix[i][j]:

cypher.append([i, j])

isFound = True

break

if isFound:

break

print('Зашифрованное сообщение:', ' '.join(f'{c[0]}-{c[1]}' for c in cypher))

message = ''

for c in cypher:

message += matrix[c[0]][c[1]]

print('Дешифрованное сообщение:', message)

*Задача 3*

key = 'аеийклмрсхь'

phrase = input('Введите сообщение: ').lower()

cypher = ''

while len(key) < len(phrase):

key += key

for i in range(len(phrase)):

if phrase[i].isalpha():

cypher += chr((ord(phrase[i]) + ord(key[i]) - 2144) % 33 + 1072)

else:

cypher += phrase[i]

print('Зашифрованное сообщение:', cypher)

message = ''

for i in range(len(cypher)):

if cypher[i].isalpha():

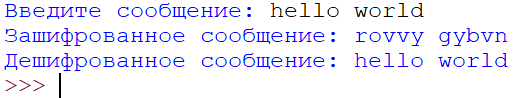
message += chr((ord(cypher[i]) - ord(key[i])) % 33 + 1072)

else:

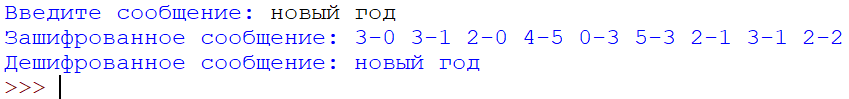
message += cypher[i]

print('Дешифрованное сообщение:', message)

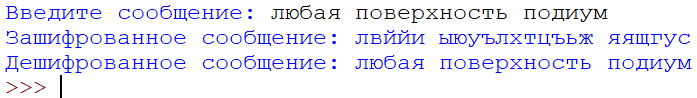
**Результаты:**



**Рисунок 1.** Шифр Цезаря



**Рисунок 2.** Полибианский квадрат



**Рисунок 3.** Шифр Виженера

**Вывод:** в ходе выполнения лабораторной работы были получены навыки шифрования и дешифрования сообщений методами Цезаря, полибианского квадрата и Виженера.