Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

КАФЕДРА ИНФОРМАТИКИ

Отчёт по лабораторной работе №1

“Шифр Цезаря.”

Выполнил:

студент гр. 853504

Кузьма В. В.

Проверил:

Протько М.И.

Минск 2021

**Содержание**

[**1.** **Цель работы** 3](#_Toc65156180)

[**2. Краткие теоретические сведения** 4](#_Toc65156181)

[**3. Реализация задачи** 5](#_Toc65156182)

[**Приложение. Текст программ** 6](#_Toc65156183)

# 

# **Цель работы**

Реализовать программные средства шифрования и дешифрования текстовых файлов при помощи **шифра Цезаря**, (шифра сдвига, кода Цезаря) и **шифра Виженера**.

# 

# **2. Краткие теоретические сведения**

**Шифр Цезаря** – это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом 4 А была бы заменена на Г, Б станет Д, и так далее.

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

**Y = (X + K) mod n;**

**X = (Y – K + N) mod n;**

**X** – Символ открытого текста;

**Y** – Символ шифрованного текста;

**N** – Мощность алфавита;

**K** – Ключ;

С точки зрения математики шифр Цезаря является частным случаем аффинного шифра.

Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова. Например, предположим, что исходный текст имеет такой вид:

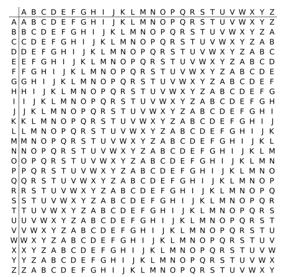


Рис 1. Квадрат Виженера.

## **3. Реализация задачи**

Программу реализовал на языке программирования **Python**. Результат программы:

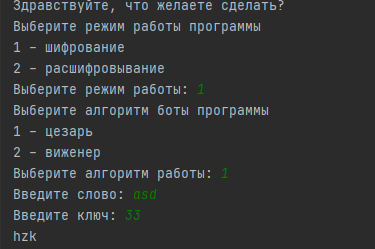
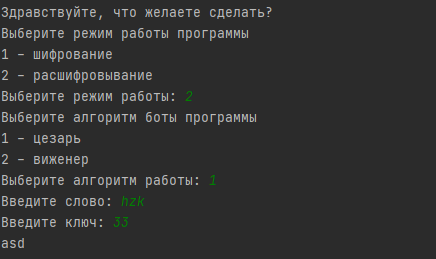


Рис 2. Результат работы шифра Цезаря.

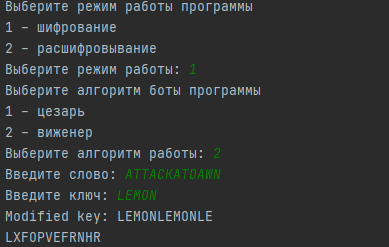
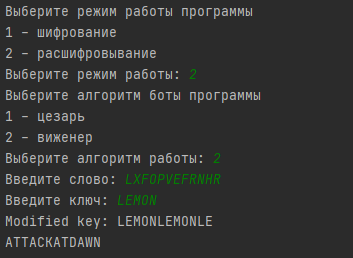
 

Рис 3. Результат работы шифра Виженера.

# 

# **Приложение. Текст программ**

if \_\_name\_\_=="\_\_main\_\_":   
 print("Здравствуйте, что желаете сделать?")  
 print("Выберите режим работы программы")  
 print("1 - шифрование")  
 print("2 - расшифровывание")  
 mode = int(input("Выберите режим работы: "))  
 print("Выберите алгоритм боты программы")  
 print("1 - цезарь")  
 print("2 - виженер")  
 algo = int(input("Выберите алгоритм работы: "))  
 word = input("Введите слово: ")  
 key = input("Введите ключ: ")  
 get\_base = lambda letter: ord('A') if letter >='A' and letter <='Z' else ord('a')  
 cezar\_encryption = lambda letter: chr(get\_base(letter) + ((ord(letter) - get\_base(letter) + int(key)) % 26))  
 cezar\_decryption = lambda letter: chr(get\_base(letter) + ((ord(letter) - get\_base(letter) - int(key) + 26) % 26))  
 vizener\_encryption = lambda letter: chr(get\_base(letter[0]) + ((ord(letter[0]) - get\_base(letter[0]) + ord(letter[1]) - get\_base(letter[1])) % 26))  
 vizener\_decryption = lambda letter: chr(get\_base(letter[0]) + ((ord(letter[0]) - get\_base(letter[0]) - ord(letter[1]) + get\_base(letter[1]) + 26) % 26))  
 if (algo == 1 and mode == 1):  
 f = cezar\_encryption  
 print(''.join(list(map(f, word))))  
 if (algo == 1 and mode == 2):  
 f = cezar\_decryption  
 print(''.join(list(map(f, word))))  
  
 if (algo == 2):  
 if (len(word) < len(key)):  
 raise ValueError("key > word")  
 if not all(c.isupper() for c in word):  
 raise ValueError("word contains negative symbols")  
 if not all(c.isupper() for c in key):  
 raise ValueError("key contains negative symbols")  
 s = key  
 i = 0  
 while(len(key) < len(word)):  
 key += s[i]  
 i+=1  
 if i>=len(s):  
 i = 0  
 print(f"Modified key: {key}")  
 if (mode == 1):  
 f = vizener\_encryption  
 print(''.join(list(map(f, zip(word, key)))))  
 if (mode == 2):  
 f = vizener\_decryption  
 print(''.join(list(map(f, zip(word, key)))))