Лабораторная работа 1 "Разработка и тестирование программного обеспечения"

Для выполнения лабораторной работы был выбран шифр Вижинера – метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.

# Принцип работы алгоритма

Шифрование:

Для работы с шифром используется таблица алфавитов (или квадрат Вижинера) (рис. 1), которая составляется последовательно из n строк по n символов, где n – количество знаков алфавита, причём каждая следующая строка сдвигается на несколько позиций относительно предыдущей. Первая строка таблицы – это алфавит шифра Цезаря с нулевым сдвигом, каждая новая строка со сдвигом равным 1, 2, 3 и так далее до n. По горизонтали расположены буквы открытого текста, по вертикали – буквы ключа. Ключ должен быть такой же длины символов, что и открытый текст, если ключ оказался короче, то он записывается циклически до тех пор, пока его длина не будет соответствовать длине исходного текста.

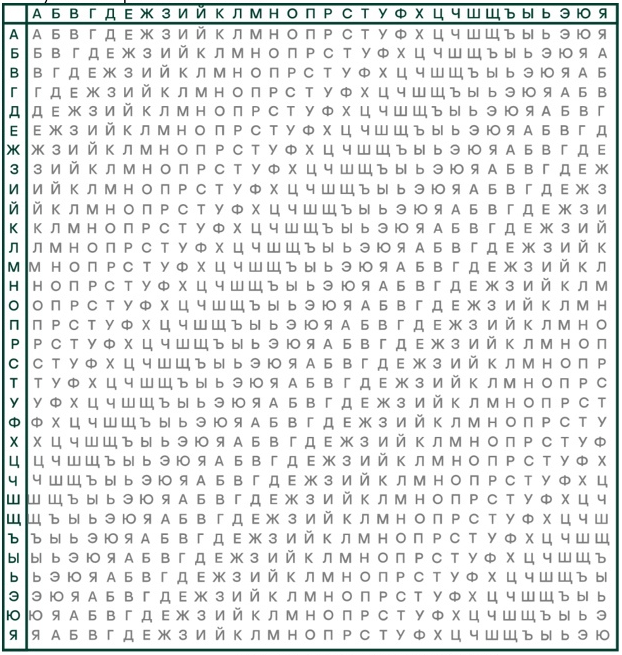


Рисунок 1 – Квадрат Вижинера для русского алфавита (без буквы ё)

Процесс шифрования в математическом виде:

Если – количество букв в алфавите, – номер буквы открытого текста, – номер буквы ключа в алфавите, то шифрование Виженера можно записать следующим образом:

Процесс шифрования в форме простого алгоритма:

Первый символ зашифрованного текста находится на пересечении строки с обозначением первой буквы ключа и столбца с обозначением первой буквы открытого текста в квадрате Виженера. Для второго символа исходного текста используется второй символ ключа; т.е. второй символ зашифрованного текста получается на пересечении строки с обозначением второй буквы ключа и столбца столбца с обозначением первой буквы открытого текста. Остальная часть исходного текста шифруется подобным способом.

Дешифровка:

Процесс дешифрования в математическом виде:

Процесс дешифрования в форме простого алгоритма:

Находим в квадрате Виженера строку с обозначением первой буквы ключа, далее в этой строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются аналогично.

# Реализация алгоритма

Алгоритм шифрования реализован на языке Python

Предусмотрена работа как с английским языком, так и с русским (при использовании русского языка не учитывается буква «ё», она заменяется на букву «е» и далее шифруется/дешифруется аналогично). Все символы кроме символов алфавита удаляются как из открытого текста/шифротекста, так и из ключа. Алгоритмы шифрования и дешифрования не чувствительны к регистру, поэтому было выполнено приведение всех входных данных едино к верхнему регистру, выходные данные соответственно также в верхнем регистре.

Функция шифрования:

def encrypt(self, key: str, plaintext: str, lang: str) -> str:  
 first\_letter\_code = 65 if lang == "en" else 1040  
 alphabets\_length = 26 if lang == "en" else 32  
 plaintext = plaintext.upper()  
 key\_length = len(key)  
 key\_as\_int = [ord(i) for i in key]  
 plaintext\_int = [ord(i) for i in plaintext]  
 ciphertext = ''  
 for i in range(len(plaintext\_int)):  
 value = (plaintext\_int[i] + key\_as\_int[i % key\_length]) % alphabets\_length  
 ciphertext += chr(value + first\_letter\_code)  
 return ciphertext

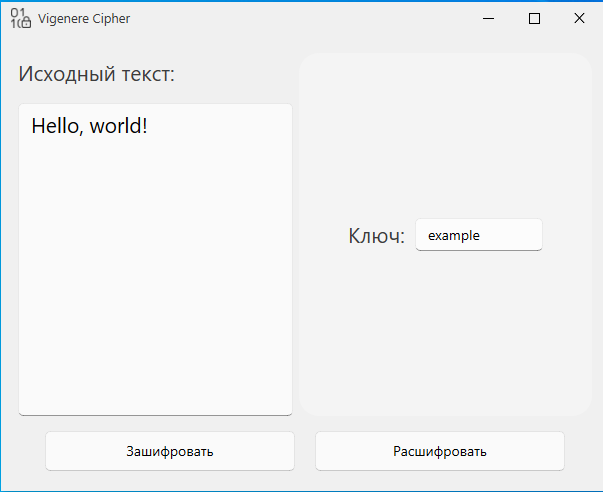
Функция расшифровки:

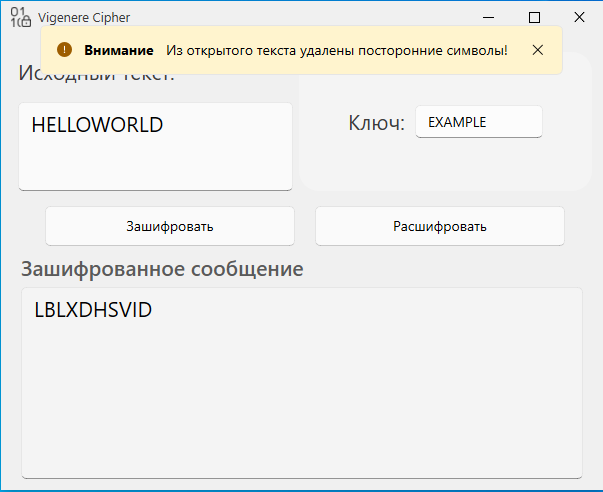
def decrypt(self, key: str, ciphertext: str, lang: str) -> str:  
 first\_letter\_code = 65 if lang == "en" else 1040  
 alphabets\_length = 26 if lang == "en" else 32  
 ciphertext = ciphertext.upper()  
 key\_length = len(key)  
 key\_as\_int = [ord(i) for i in key]  
 ciphertext\_int = [ord(i) for i in ciphertext]  
 plaintext = ''  
 for i in range(len(ciphertext\_int)):  
 value = (ciphertext\_int[i] - key\_as\_int[i % key\_length]) % alphabets\_length  
 plaintext += chr(value + first\_letter\_code)  
 return plaintext

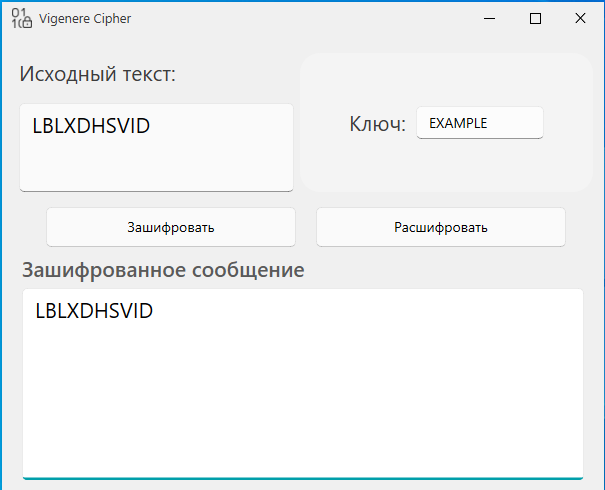
# Результаты тестирования

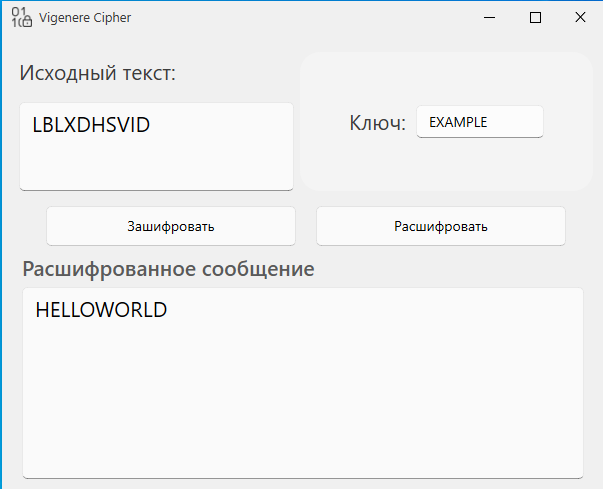
Пример 1:

Шифрование и расшифровка предложения на английском языке.

  
Рисунок 1 – Исходные данные для шифрования

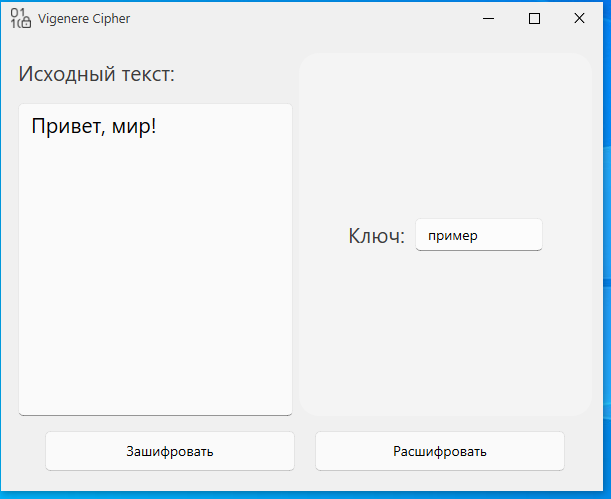
  
Рисунок 2 – Сообщение зашифровано, исходные и выходные данные отображены в едином стиле, пользователю выведено сообщение об изменении формата входных данных (удаление любых символов, кроме символов алфавита)

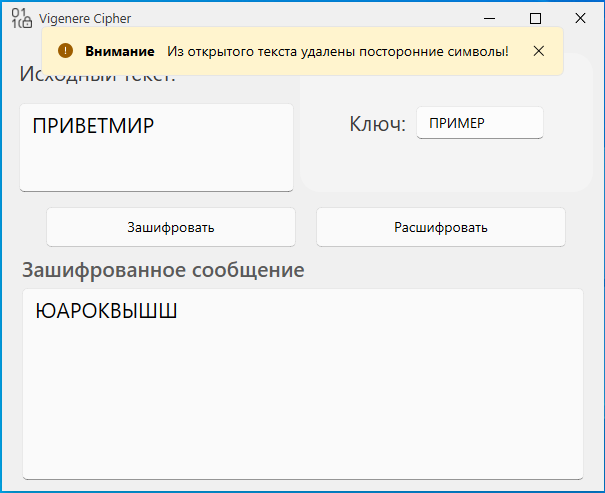
  
Рисунок 3 – Исходные данные для дешифрования. До момента нажатия кнопки «Расшифровать» в поле выходных данных отображается информация предыдущего действия

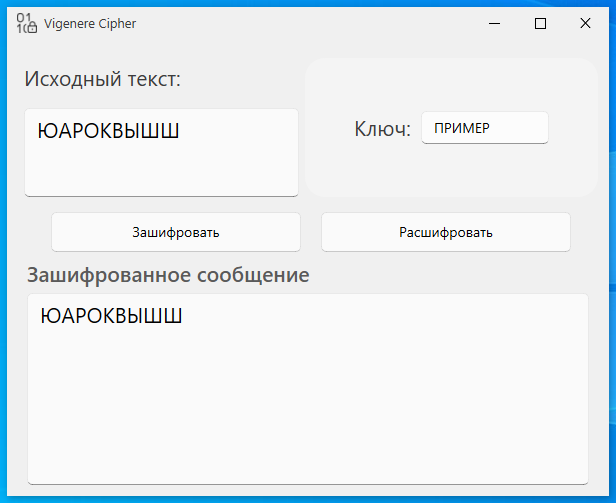
  
Рисунок 4 – Сообщение расшифровано

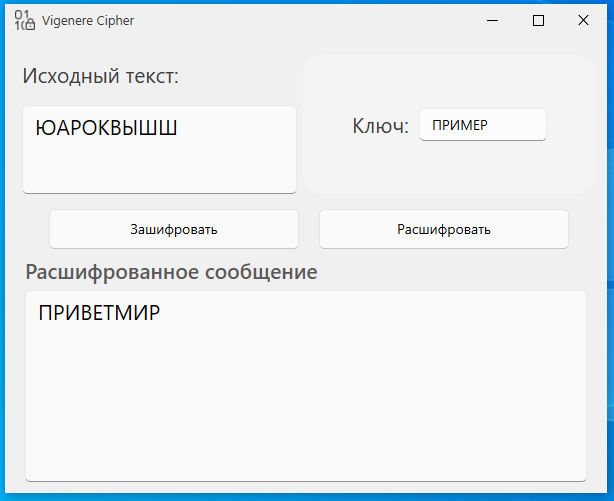
Пример 2:

Шифрование и расшифровка предложения на русском языке.

  
Рисунок 5 – Исходные данные для шифрования

  
Рисунок 6 – Сообщение зашифровано, исходные и выходные данные отображены в едином стиле, пользователю выведено сообщение об изменении формата входных данных (удаление любых символов, кроме символов алфавита)

  
Рисунок 7 – Исходные данные для дешифрования. До момента нажатия кнопки «Расшифровать» в поле выходных данных отображается информация предыдущего действия

  
Рисунок 8 – Сообщение расшифровано

Пример 3:

Шифрование и расшифровка текста на английском языке.

В качестве открытого текста был выбран следующий отрывок:

Once upon a time, a Princess named Snow White lived in a castle with her father the King and her Stepmother the Queen. Her father always reminded his daughter that above all else, a royal family must be fair. Said he: “People over all the land come here to the castle with disputes. They need their ruler to hear each side and make a decision that's fair.”

В качестве ключа был выбран следующий отрывок:

The Queen, Snow White’s stepmother, knew how important being fair was to her husband. She asked her magic mirror:  “Mirror, mirror, on the wall, who is the fairest of them all?”

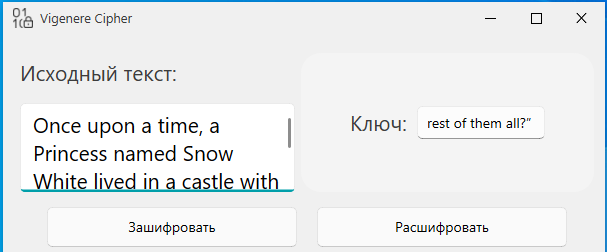
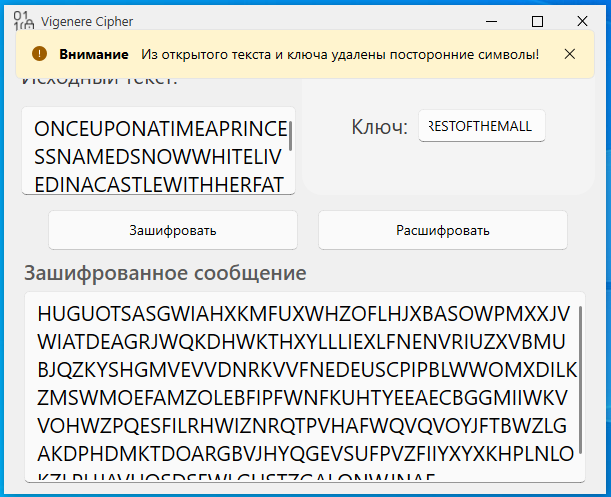
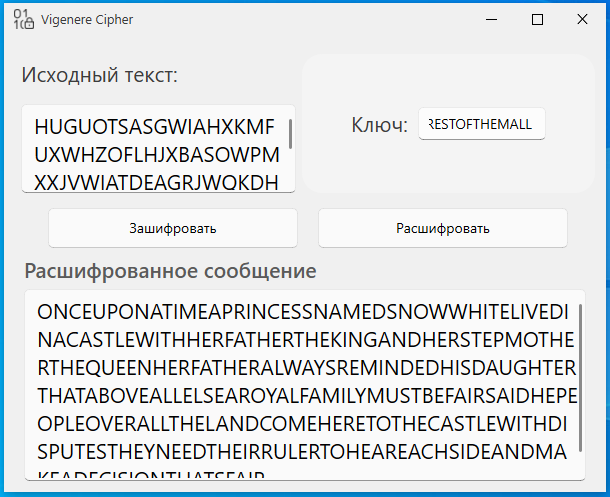


Рисунок 9 – Исходные данные для шифрования

  
Рисунок 10 – Сообщение зашифровано

  
Рисунок 11 – Сообщение расшифровано

Пример 4:

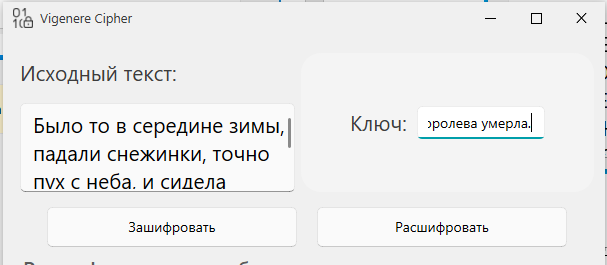
Шифрование и расшифровка текста на русском языке.

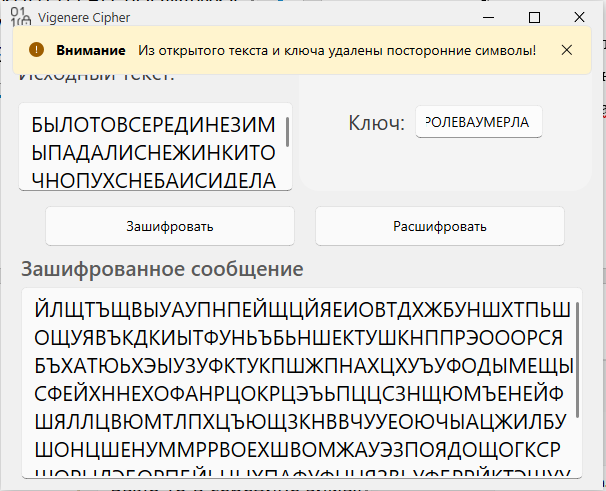
В качестве открытого текста был выбран следующий отрывок:

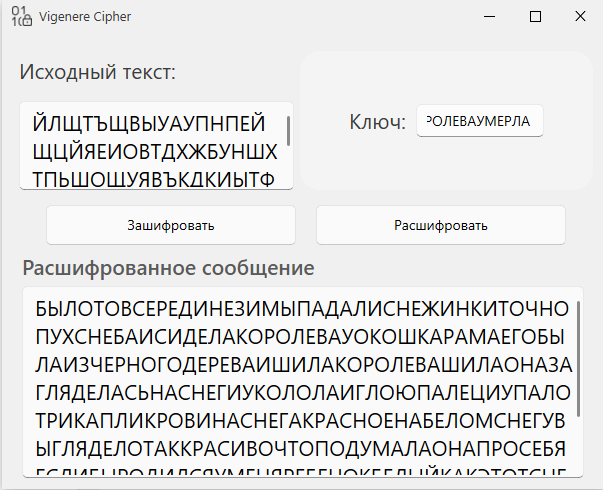
Было то в середине зимы, падали снежинки, точно пух с неба, и сидела королева у окошка, - рама его была из черного дерева, - и шила королева. Шила она, загляделась на снег и уколола иглою палец, и упало три капли крови на снег. А красное на белом снегу выглядело так красиво, что подумала она про себя: «Если бы родился у меня ребенок, белый, как этот снег, и румяный, как кровь, и черноволосый, как дерево на оконной раме!»

В качестве ключа был выбран следующий отрывок:

И родила королева вскоре дочку, и была она бела, как снег, как кровь, румяна, и такая черноволосая, как черное дерево, - и прозвали ее потому Белоснежкой. А когда ребенок родился, королева умерла.

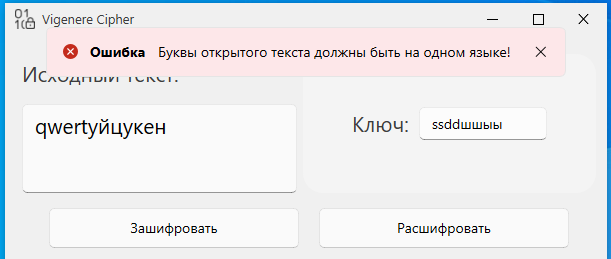
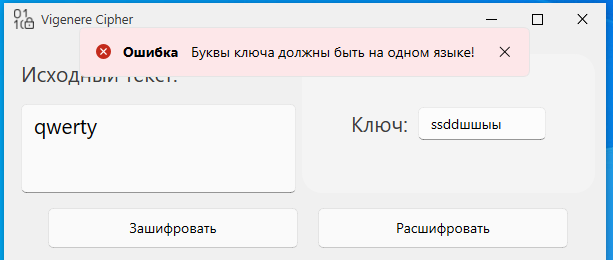
  
Рисунок 12 – Исходные данные для шифрования

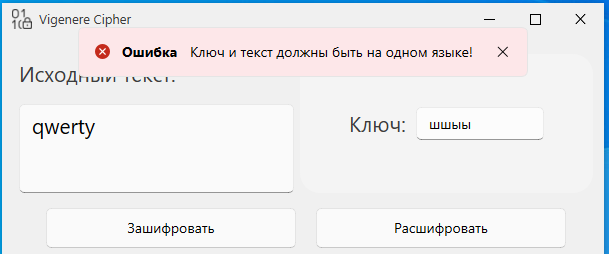
  
Рисунок 13 – Сообщение зашифровано

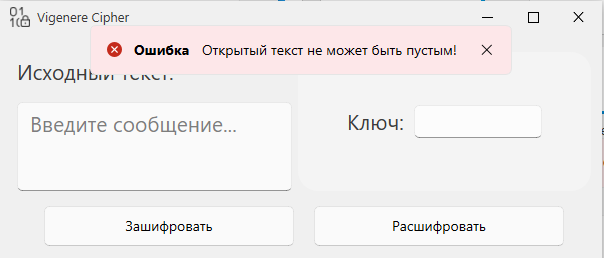
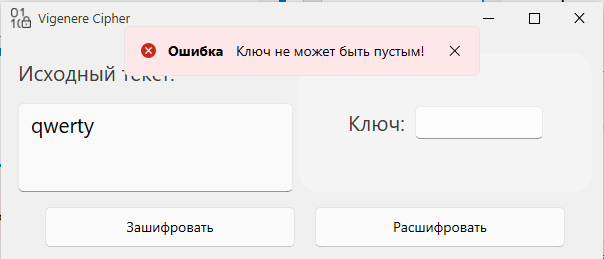
  
Рисунок 14 – Сообщение расшифровано

Пример 5:

В данном примере собраны варианты ответа пользователю при некорректном вводе данных.

  
  
Рисунок 15 – Ввод символов из различных языков вперемешку

  
Рисунок 16 – Использование разных языков для ключа и текста

  
  
Рисунок 17 – Пустые исходные данные