

## **Разработки криптографической программы на основе шифра Виженера с помощью языка программирования Python и Tkinter**

*Киселева Елизавета Александровна*

*Приамурский государственный университет им. Шолом-Алейхема*

*Студент*

### **Аннотация**

В статье описан метод шифрования Виженера, а также описана разработка программы с графическим интерфейсом на языке программирования Python, которая позволяет кодировать и декодировать текстовые сообщения данным способом.

**Ключевые слова:** Tkinter, Python, декодирование, кодирование.

## **Development of a cryptographic program based on the Vigenère cipher using the Python and Tkinter programming languages**

*Kiseleva Elizaveta Alexandrovna*

*Sholom-Aleichem Priamursky State University*

*Student*

### **Abstract**

The article describes the encryption method, as well as describes the development of programs with a graphical interface in the Python programming language, which allows you to encode and display text messages in this way.

**Keywords:** Tkinter, Python, decoding, coding.

Во все времена высокой актуальностью отличались методы защиты информации. С появлением компьютерных технологий защита информации не только стала активнее развиваться, но и образовалась отдельная ветвь научных исследований. Благодаря современным цифровым устройствам появилась возможность без труда создавать, хранить и передавать информацию любого содержания. На текущий момент имеется несколько методов защиты информации из них самым широко используемым является криптография.

Научными словами криптография - наука о методах обеспечения конфиденциальности, целостности данных, аутентификации, а также невозможности отказа от авторства.

Имеется множество довольно старых и распространённых методов криптографии, таких как: шифр Цезаря, Атбаша, Виженера и т.д. Таким образом, в ходе работы планируется разработать демонстративную программу для демонстрации работы шифра Виженера

Цель данной статьи: разработка программы с графическим интерфейсом для демонстрации работы шифра Виженера.

Ранее вопросами, связанными со стеганографией, интересовался В.А. Волков [1] в своей работе описал суть исторических шифров на примере языка программирования С. Е.А. Жученко [2] описал метод многоалфавитного шифра и работу с символьными данными. Ученные Д.А. Казимова и Т. Орымбай, а также М.Г. Коляда [3, 5] описали методы организации обучения информационной безопасности студентов. Д.В. Карпов, Э.Р. Абузьяров [4] описали реализацию анализ быстрогодействия алгоритма шифрования и дешифрования шифра Цезаря.

Для реализации данной программы для шифрования и дешифрования сообщений в соответствии с шифром Виженера, которое может шифровать сообщение с помощью ключа и дешифровать зашифрованный хэш с помощью того же ключа, было решено за основу использовать язык программирования Python и в связке с библиотекой Tkinter для графического отображения.

К примеру, в шифре Цезаря каждая буква алфавита сдвигается на несколько позиций; например, в шифре Цезаря при сдвиге +3, А стало бы D, В стало бы Е и так далее. 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.

Метод работает таким способом: автор сообщения посылает ключевое слово циклически до тех пор, пока его длина не будет соответствовать длине исходного текста. Чтобы найти значение для смещения, используем позиции каждой буквы нашего ключа в алфавите (от а до z) и считаем с нуля, Каждую букву в оригинальном тексте смещаем на заданное число, как в шифре Цезаря, возвращаясь при надобности после Z в начало алфавита.

Для расшифровки сначала требуется произвести поиск длины ключа. Можно анализировать распределение частот в зашифрованном тексте с различным прореживанием. То есть брать текст, включающий каждую 2-ю букву зашифрованного текста, потом каждую 3-ю и т. д. Как только распределение частот букв будет сильно отличаться от равномерного (например, по энтропии), то можно говорить о найденной длине ключа. Затем произвести обратное действие зашифровки.

Благодаря библиотеки Base64 значительно облегчается написание программы. На рисунке 1 изображен код кодирования и декодирования.

```
import base64

def encode(key, clear):
    enc = []
    for i in range(len(clear)):
        key_c = key[i % len(key)]
        enc_c = chr((ord(clear[i]) +
                    ord(key_c)) % 256)
        enc.append(enc_c)
    return base64.urlsafe_b64encode("".join(enc).encode()).decode()

def decode(key, enc):
    dec = []
    enc = base64.urlsafe_b64decode(enc).decode()
    for i in range(len(enc)):
        key_c = key[i % len(key)]
        dec_c = chr((256 + ord(enc[i]) -
                    ord(key_c)) % 256)
        dec.append(dec_c)
    return "".join(dec)
```

Рисунок 1 – Код кодирования и декодирования

Затем после написания логики было организовано написание графического интерфейса с помощью библиотеки Tkinter. Благодаря готовым модулям не составляет труда организовать кнопки, поля ввода текста и т.д. Таким образом по результате работы был организован графический интерфейс для взаимодействия со скриптом для кодирования и декодирования. На рисунке 2 изображен внешний вид программы.

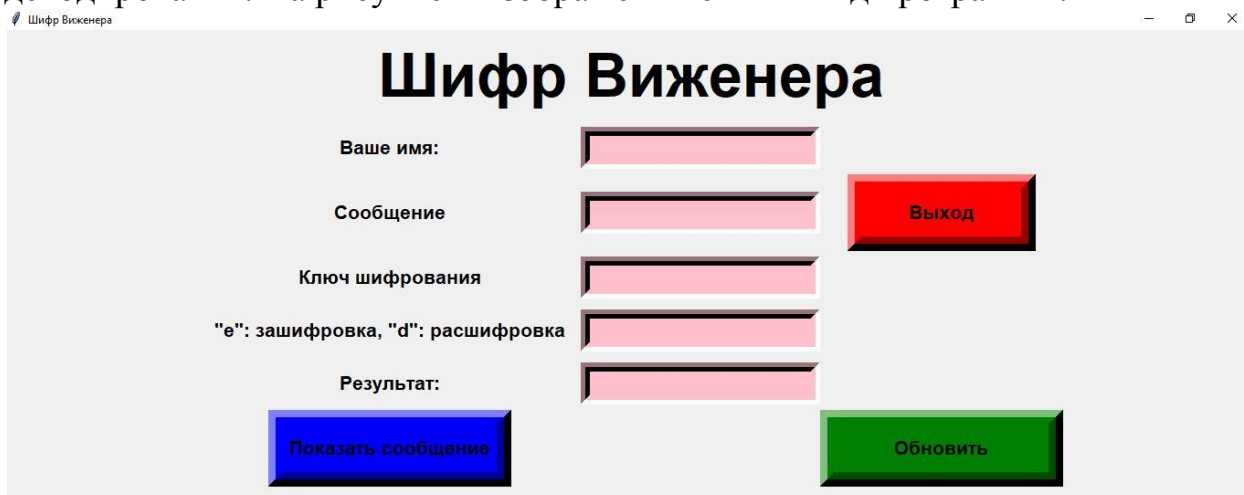



Рисунок 2 – Внешний вид программы

Для кодирования текста требуется ввести имя, сообщение, ключ шифрования и указать мод «е». При нажатии на кнопку «Показать сообщение» в поле «Результат» будет выведен конечный зашифрованный текст. На рисунке 3 изображено кодирование информации.

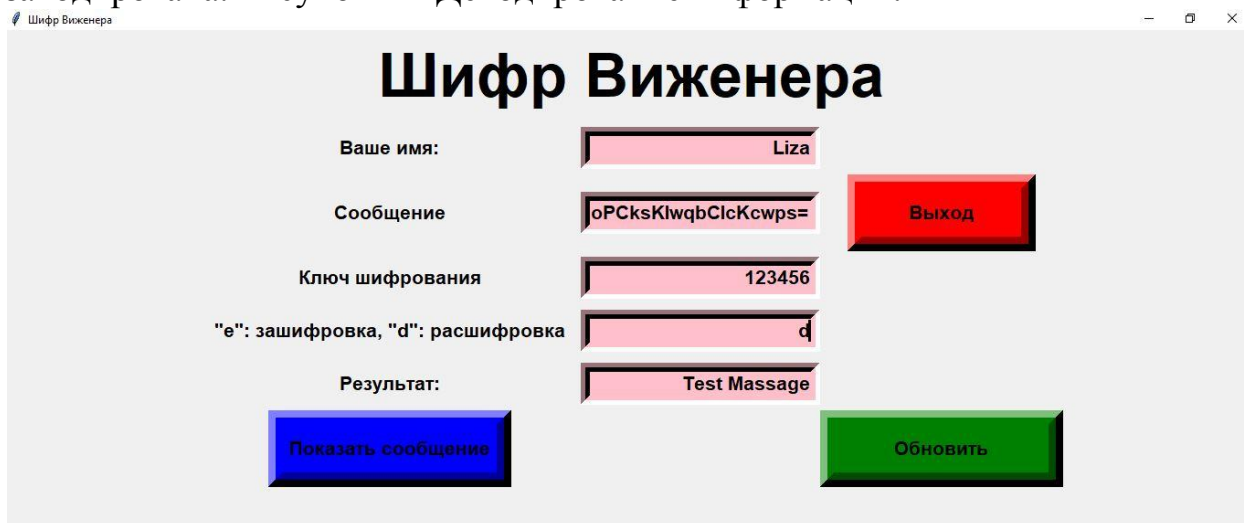


The screenshot shows a web application window titled "Шифр Виженера". The interface includes the following elements:

- Ваше имя:** Input field containing "Liza".
- Сообщение:** Input field containing "Test Massage".
- Ключ шифрования:** Input field containing "123456".
- "e": зашифровка, "d": расшифровка:** Input field containing "e".
- Результат:** Output field containing "woXC18KmwqhVwoPCks".
- Buttons:** A red "Выход" button, a blue "Показать сообщение" button, and a green "Обновить" button.

Рисунок 3 – Кодирование информации

Для декодирования информации требуется результат кодирования вставить в поле «Сообщение», ключ шифрования, указанный при кодировании, указать мод «d» и при нажатии на кнопку «Показать сообщение» в поле «Результат» отобразится информация, которая была закодирована. Рисунок 4 – Декодирование информации.



The screenshot shows the same web application window, but with the following changes:

- Сообщение:** Input field containing the encoded text "oPCksKlwqbClcKcws=".
- "e": зашифровка, "d": расшифровка:** Input field containing "d".
- Результат:** Output field containing the decoded text "Test Massage".
- The other fields and buttons remain the same as in Figure 3.

Рисунок 4 – Декодирование информации

### Заключение

В ходе работы, была разработана программа на языке программирования Python для кодирования и декодирования текста с помощью шифра Виженера. Кроме реализации кодирования был реализован графический интерфейс, который позволил более наглядно увидеть результат. Данная программа удачно протестирована и результат описан в работе.

**Библиографический список**

1. Волков В. А. Исторические шифры на примере языка С //Постулат. – 2017. – №. 4.
2. Жученко Е. А. Реализация на ЭВМ метода многоалфавитного шифра и работа с символьными данными //Современные методы прикладной математики, теории управления и компьютерных технологий (ПМТУКТ-2015). 2015. С. 146-147.
3. Казимова Д. А., Орымбай Т. Формы организации обучения при подготовке студентов к обеспечению информационной безопасности //Форум. Серия: Гуманитарные и экономические науки. 2015. №. 3. С. 74-78.
4. Карпов Д. В., Абузярова Э. Р., Ласкова С. Г. Реализация и анализ быстродействия алгоритма шифрования и дешифрования шифра Цезаря //Евразийский союз ученых. 2015. №. 6-2. С. 120-121.
5. Коляда М. Г. Использование телекоммуникационных мини-проектов в системе подготовки будущих специалистов сферы информационной безопасности //Инновационные образовательные технологии. 2013. №. 3. С. 27-33.