Отчёт по лабораторной работе №1.  
Шифры простой замены

Студент: Лапшенкова Любовь Олеговна, 1032217633

Группа: НФИмд-02-21

Преподаватель: Кулябов Дмитрий Сергеевич,

д-р.ф.-м.н., проф.

Москва 2021

Содержание

# 1 Цель работы

Целью данной лабораторной работы является ознакомление с двумя методами шифрования: шифром Цезаря и шифром Атбаш. Также необходимо реализовать оба шифра на одном из известных языков программирования.

# 2 Задание

1. Реализовать шифр Цезаря с произвольным ключом .
2. Реализовать шифр Атбаш.

# 3 Теоретическое введение

## 3.1 Шифр Цезаря

### 3.1.1 Введение

С быстрым развитием обмена цифровыми данными в электронном виде, информационная безопасность приобретает все большее значение при хранении и передаче данных. Поэтому для обмена данными необходимо обеспечить их шифрование. Шифрование - это процесс кодирования сообщения таким образом, чтобы его мог прочитать только предполагаемый получатель [1]. Необходимо принять во внимание одну из простейших систем шифрования - шифр Цезаря. Предполагается, что знаменитый римский император и полководец, живший в 1 веке до нашей эры, использовал этот шифр в своей переписке [2]. Алгоритм шифрования Цезаря заключается в замене каждого символа входящего сообщения на символ, который находится на некотором константном расстоянии с правой или левой стороны. Расстояние при этом называют – ключом[3].

### 3.1.2 Математическая модель

С точки зрения математики шифр Цезаря является частным случаем аффинного шифра [4].Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами:

где - символ открытого текста, - символ шифрованного текста, - мощность алфавита, - ключ[5].

Пример:

Шифрование с использованием ключа . Буква «Е» «сдвигается» на три буквы вперёд и становится буквой «З» [4]. Твёрдый знак, перемещённый на три буквы вперёд, становится буквой «Э», и так далее:

{  
 Исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ  
  
 Шифрованный алфавит: ГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВ  
}

### 3.1.3 Слабые места

У шифра Цезаря есть некоторые слабые места, которые позволяют нам использовать атаку методом грубой силы [6]. 1. Алгоритм шифрования и дешифрования известен. 2. Всего 25 ключей. 3. Язык открытого текста известен и легко узнаваем.

## 3.2 Шифр Атбаш

### 3.2.1 Введение

Атбаш - способ шифрования текста, в котором элементы исходного текста заменяются зашифрованным текстом в соответствии с некоторым правилом [7].

### 3.2.2 Математическая модель

Алгоритм этого шифра прост: первая буква алфавита заменяется на последнюю, вторая на предпоследнюю в алфавите и т.д [8]. Иначе говоря, правило шифрования состоит в замене буквы алфавита буквой с номером , где — число букв в алфавите[9].

Пример:

{  
 Исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ  
  
 Шифрованный алфавит: ЯЮЭЬЫЪЩШЧЦХФУТСРПОНМЛКЙИЗЖЁЕДГВБА  
}

### 3.2.3 Слабые места

Основное слабое место - для успешной дешифрации необходимо знать только алфавит сообщения[8].

# 4 Выполнение лабораторной работы

Реализация шифров производилась на языке Python 3. Через Anaconda-Navigator, Jupyter Notebook. Процесс реализации кода доступен по [ссылке](https://youtu.be/uhLd15AetAc).

# 5 Реализация шифра Цезаря

Реализация шифра Цезаря выглядит следующим образом(рис. 1).

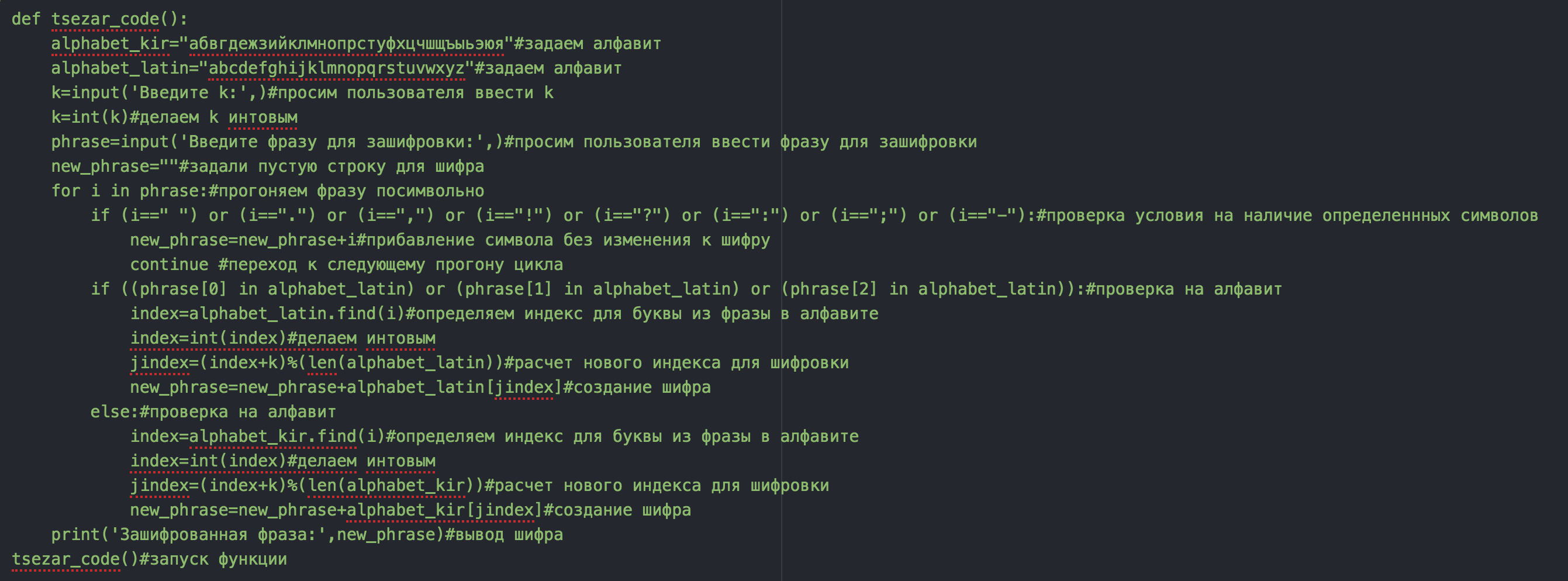


Figure 1: Программа Шифр Цезаря

При запуске функции, получили следующий вывод (рис. 2).

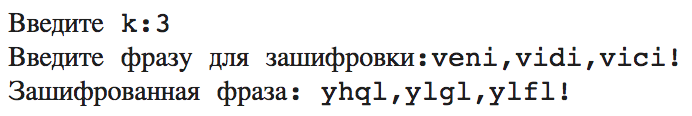


Figure 2: Результат выполнения программы Шифр Цезаря

# 6 Реализация шифра Атбаш

Реализация шифра Атбаш выглядит следующим образом(рис. 3).

## 6.1 Шифр Атбаш

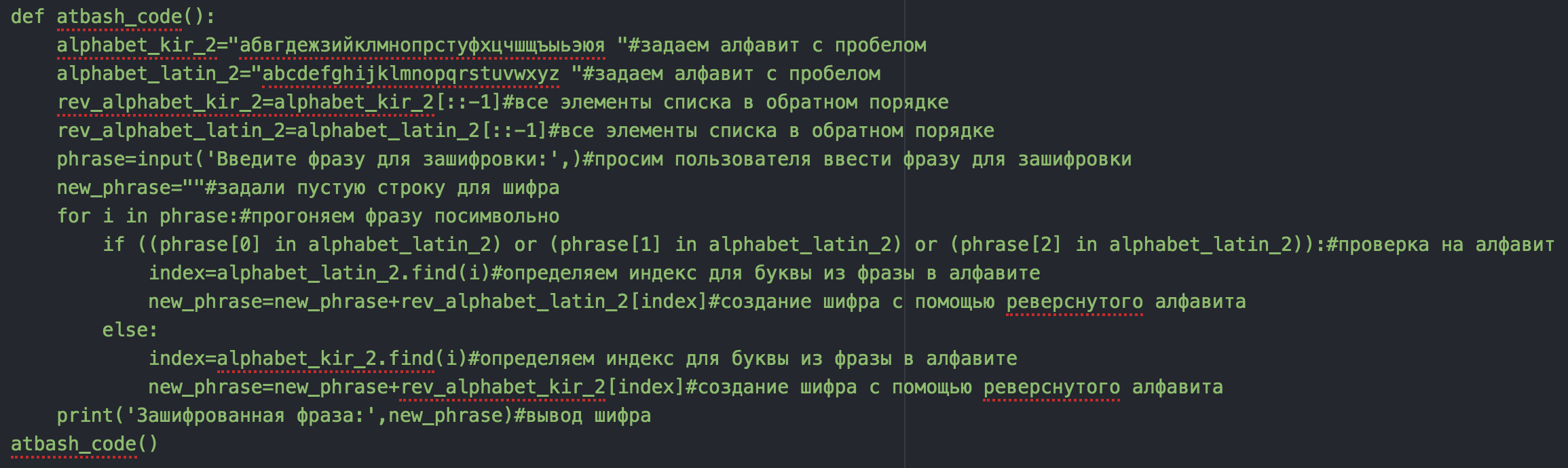


Figure 3: Программа Шифр Атбаш

При запуске функции, получили следующий вывод (рис. 4).

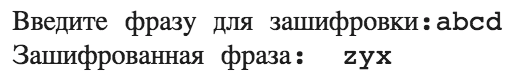


Figure 4: Результат выполнения программы Шифр Атбаш

# 7 Выводы

В процессе выполнения данной лабораторной работы нам удалось ознакомиться с двумя методами шифрования: шифром Цезаря и шифром Атбаш, а также реализовать оба шифра на одном из известных языков программирования (в моем случае на языке Python 3). Код программ был написан в соответствии с теоретическими сведениями, предоставленными в задании к лабораторной работе, а также найденными самостоятельно.

# Список литературы

1. Habr. Шифр Цезаря или как просто зашифровать текст [Электронный ресурс]. Habr, 2020, URL:https://habr.com/ru/post/534058/ (дата обращения 09.11.2021)
2. ИНТУИТ. Лекция 2: Основные понятия криптографии [Электронный ресурс]. ИНТУИТ, 2021, URL:https://intuit.ru/studies/courses/691/547/lecture/12371?page=3 (дата обращения 09.11.2021)
3. Инфоурок. Система шифрования Цезарь. Аффинная система трансплантации Цезаря [Электронный ресурс]. Инфоурок, 2021, URL:https://infourok.ru/sistema-shifrovaniya-cezar-affinnaya-sistema-transplantacii-cezarya-4640938.html (дата обращения 10.11.2021)
4. Google. Криптография. Шифр Цезаря [Электронный ресурс]. Google, 2021, URL:https://www.sites.google.com/site/kriptografics/sifr-cezara (дата обращения 10.11.2021)
5. Mind Control. Шифр Цезаря [Электронный ресурс]. Mind Control, 2021, URL:https://mind-control.fandom.com/wiki/%D0%A8%D0%B8%D1%84%D1%80\_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F (дата обращения 10.11.2021)
6. MySeldon. Шифр Цезаря или как просто зашифровать текст [Электронный ресурс]. MySeldon, 2020, URL:https://news.myseldon.com/ru/news/index/242705590 (дата обращения 11.11.2021)
7. Wiki93. Атбаш [Электронный ресурс]. Wiki93, 2020, URL:http://www.wiki93.ru/index.php?title=%D0%90%D1%82%D0%B1%D0%B0%D1%88 (дата обращения 11.11.2021)
8. Hi-edu. Криптография[Электронный ресурс]. Hi-edu, 2021, URL:http://www.hi-edu.ru/e-books/xbook1019/01/info.pdf (дата обращения 11.11.2021)
9. Academic dictionary. Атбаш [Электронный ресурс]. Academic dictionary, 2020, URL:https://dic.academic.ru/dic.nsf/ruwiki/247899 (дата обращения 12.11.2021)