Лабораторная работа №1. Шифры простой замены.

Предмет: Математические основы защиты информации и информационной безопасности

Александр Сергеевич Баклашов

Содержание

# 1 Цель работы

Рассмотреть шифры простой замены, а именно:

Шифр Цезаря

Шифр Атбаш

# 2 Задание

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

# 3 Теоретическое введение

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 вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

Шифр назван в честь римского полководца Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Шифр Атбаш — это простой метод шифрования, при котором буквы сдвигаются на всю длину алфавита.

# 4 Выполнение лабораторной работы

## 4.1 Шифр Цезаря

### 4.1.1 Задача

Реализовать шифр Цезаря с произвольным ключом .

#### 4.1.1.1 Решение

Для начала, инициализируем алфавит (латинские буквы нижнего регистра), затем предложим ввести ключ смещения и фразу. После введения фразы, приступаем к реализации шифрования: проходимся по буквам фразы и алфавита. Если находится совпадение смещаем букву на количество букв алфавита, равное ключу шифрования, и печатаем результат.

Если совпадений нет (например, написаны знаки препинания), печатаем символы без изменений.(рис. [1](#fig:001))



Figure 1: Шифр Цезаря

## 4.2 Шифр Атбаш

### 4.2.1 Задача

Реализовать шифр Атбаш

#### 4.2.1.1 Решение

Для начала, инициализируем алфавит (кириллица нижнего регистра), также добавим пробел в конце алфавита. Затем предложим ввести фразу. После введения фразы, приступаем к реализации шифрования: проходимся по буквам фразы и алфавита. Если находится совпадение смещаем букву на весь алфавит, и печатаем результат.

Если совпадений нет (например, написаны знаки препинания), печатаем символы без изменений. (рис. [2](#fig:002))

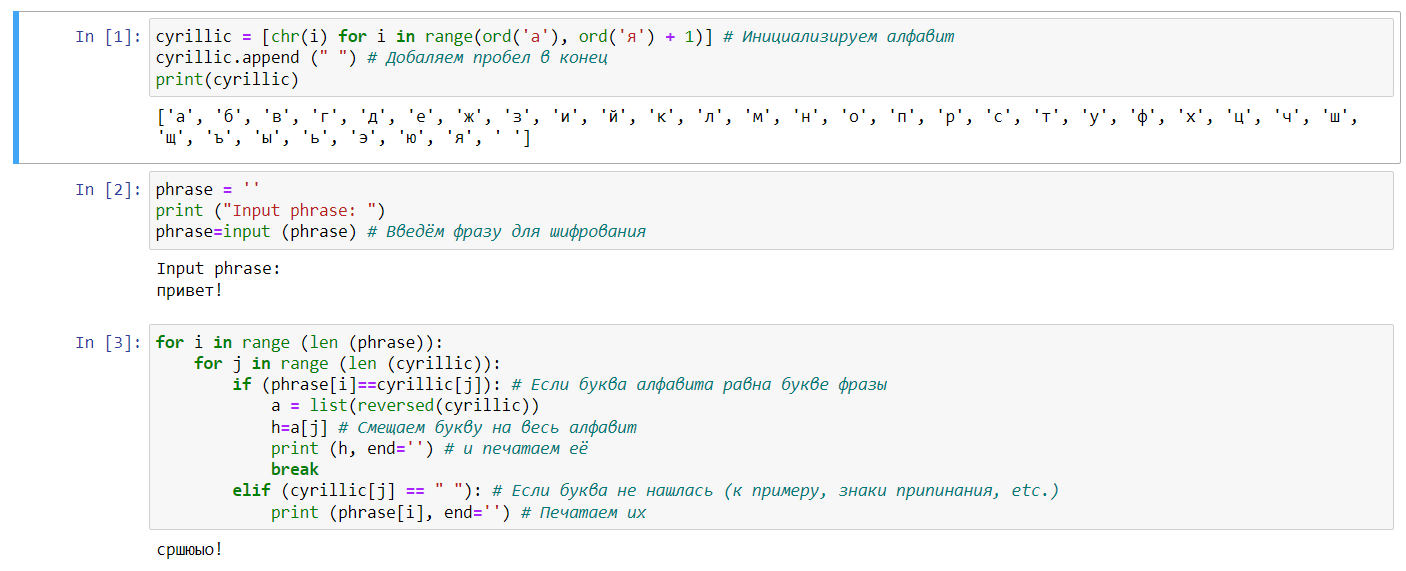


Figure 2: Шифр Атбаш

# 5 Выводы

В ходе данной лабораторной работы я рассмотрел и реализовал такие шифры простой замены, как шифр Цезаря и шифр Атбаш.

# 6 Библиография

1. Python documentation. [Электронный ресурс]. М. URL: [Python documentation](https://docs.python.org/3/index.html) (Дата обращения: 16.09.2023).
2. Лабораторная работа №1. Задача о погоне. - 4 с. [Электронный ресурс]. М. URL: [Лабораторная работа №1. Шифры простой замены.](https://esystem.rudn.ru/pluginfile.php/2089782/mod_folder/content/0/lab01.pdf) (Дата обращения: 16.09.2023).