Лабораторная работа №1

Шифры простой замены

Ли Тимофей Александрович, НФИмд-02-22

Содержание

[Цель работы 1](#_Toc114340525)

[Задание 1](#_Toc114340526)

[Теоретическое введение 1](#_Toc114340527)

[Шифр Цезаря 2](#_Toc114340528)

[Шифр Атбаш 2](#_Toc114340529)

[Выполнение лабораторной работы 2](#_Toc114340530)

[Реализация шифра Цезаря c произвольным ключом 2](#_Toc114340531)

[Реализация шифра Атбаша 3](#_Toc114340532)

[Тестирование 3](#_Toc114340533)

[Выводы 4](#_Toc114340534)

# Цель работы

Цель данной работы — изучить и программно реализовать шифры простой замены.

# Задание

Заданием является:

* Реализовать шифр Цезаря с произвольным ключом ;
* Реализовать шифр Атбаш.

# Теоретическое введение

Шифр простой замены представляет собой замену каждой буквы в исходном слове на определенное число, которому соответствует данная буква. В основе функционирования шифров простой замены лежит следующий принцип: для получения шифртекста отдельные символы или группы символов исходного алфавита заменяются символами или группами символов шифроалфавита.

## Шифр Цезаря

**Шифр Цезаря** является моноалфавитной подстановкой, т.е. каждой букве открытого текста ставится соответствие одна буква шифротекста.

Математическая процедура шифрования описывается как

где - длина алфавитаа, - произвольный ключ (величина сдвига от изначальной позиции буквы), - текущая позиция буквы в алфавите.

Для латинского алфавита длина составляет 26 символов, а формулу можно привести к виду:

где соответствуют , а .

Сам же Цезарь обычно использовал подстановку .

## Шифр Атбаш

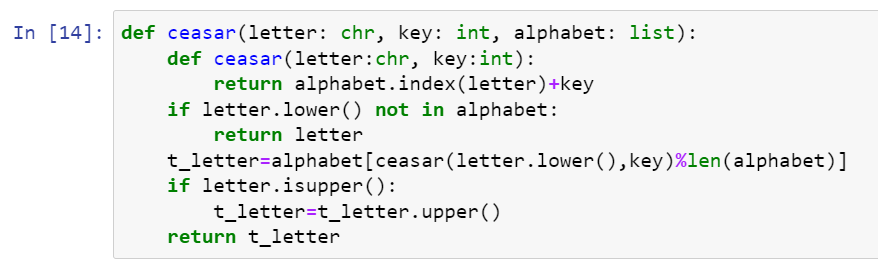
**Шифр Атбаш** является сдвигом на всю длину алфавита. Правило шифрования состоит в замене -й буквы алфавита буквой с номером , где — число букв в алфавите.

# Выполнение лабораторной работы

Для реализации шифров мы будем использовать Python, так как его синтаксис позволяет быстро реализовать необходимые нам алгоритмы.

## Реализация шифра Цезаря c произвольным ключом

Шифр Цезаря реализуем в виде функции ceasar следующего вида:



функция шифра Цезаря

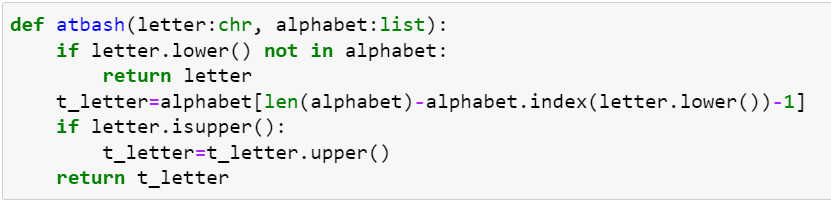
На вход она принимает переменные letter (один символ), key (произвольный ключ), alphabet (алфавит в виде списка).

В ходе обработке мы работаем с индексами элементов массива-строки, предварительно проверяя, является ли символ частью передаваемого алфавита. Если да, то мы вызываем вложенную функцию для расчета сдвига и выполняем к ней операцию деления с остатком (исходя из формулы в теоретическом введении).

В конце мы проверяем, является ли буква заглавной, и, после ситуативной обработки, возвращаем зашифрованную букву.

## Реализация шифра Атбаша

Шифр Атбаш реализуем в виде функции atbash следующего вида:



функция шифра Атбаш

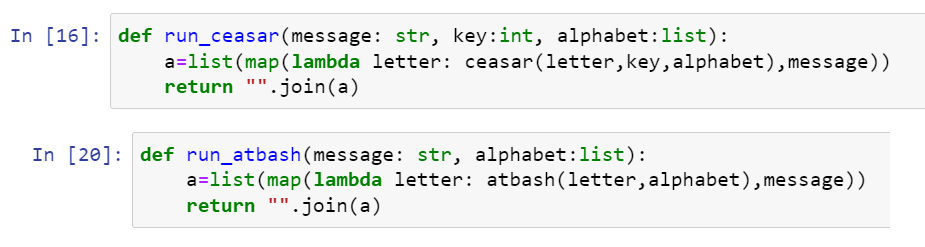
На вход она принимает те же переменные, что и функция Шифра Цезаря, исключая произвольный ключ.

Шифруется символ засчет вычитания из длины алфавита индекс символа, над которым производится шифрование.

Возвращается также зашифрованный символ.

## Тестирование

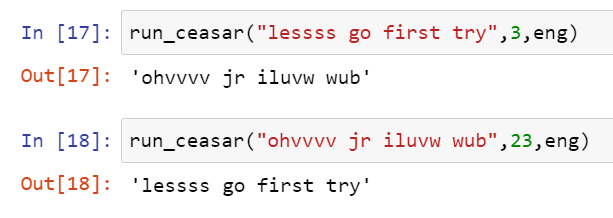
Для запуска шифрования мы создали следующие функции:



функции запуска шифрования

Также создали два вида английского алфавита – без пробела, и с ним – для запуска шифров Цезаря и Атбаш соответственно.

Запустив наш программный код, получим следующие результаты:



результат Цезаря



результат Атбаш

Видим, что шифрование проведено корректно.

# Выводы

В рамках выполненной лабораторной работы мы изучили и реализовали следующие шифры простой замены: шифр Цезаря (с произвольным ключом ) и шифр Атбаш.