Лабораторная работа №1

Цель работы

Освоить на практике написание шифров простой замены. Таких как шифр Атбаш и шифр Цезаря.

Задание

1. Реализовать шифр Цезаря с ключем k символов.
2. Реализовать шифр Атбаш.

Теоретическое введение

Атбаш— простой ***шифр*** подстановки для алфавитного письма. Правило ***шифрования*** состоит в замене n -й буквы алфавита буквой с номером m - n + 1 , где m — число букв в алфавите. [1].

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 3 А была бы заменена на Г, Б станет Д, и так далее. Используемое преобразование обычно обозначают как ROTN, где N — сдвиг, ROT — сокращение от слова ROTATE, в данном случае «циклический сдвиг.[3]

Шифр простой замены — один из древнейших. Прежде всего, выбирается нормативный алфавиту т.е. набор символов, которые будут использоваться для составления сообщений. В качестве нормативного алфавита может применяться, например, русский алфавит, исключая буквы «ъ» и «ё», дополненный символом пробела. [2].

Оборудование

Лабораторная работа выполнялась дома со следующими характеристиками техники:

– Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz 2.81GHz
– ОС Майкрософт Windows 10
– VirtualBox верс. 6.1.26

Код был написан на языке Python2.

Демонстрация работы кода проводилась в продукте Google Colaboratory.

Выполнение лабораторной работы

Шифр Цезаря

1. Реализовала Шифр Цезаря. Показала создание нового шифровочного алфавита. В качестве ключа использовала любое слово без повторяющихся букв.

   (рис. -@fig:001)

Н аданном слайде можно увидеть, как для создания шифровочного афавита я использвоала слово **кот**, и как по стандартному методу оно появляется в начале нового алфавита, а вся остальная часть заполняется оставшимися буквами.

2. Зашифровала слово с помощью нового алфавита.

   (рис. -@fig:002)

На слайде видно, как новый алфавит шифруется с помощью шифроалфавита, и слово чебурек превращается в мешанину из символов.

3. Дешифровала символы.

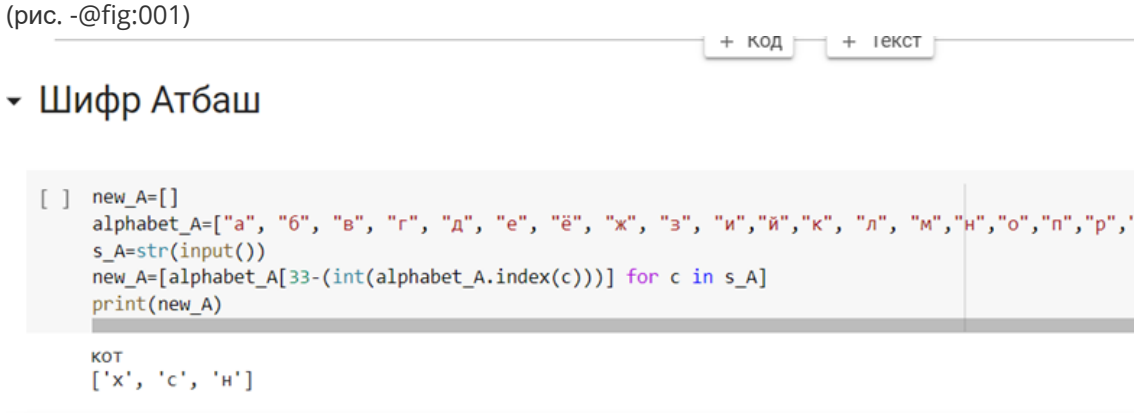
(рис. -@fig:003)

Теперь зашифрованную мешанину из символов рашировала, так как у меня уже было слово-ключ и шифроалфавит. Тем самым я вернула **чебурек** на родину.

Шифр Атбаш

1. Реализовала Шифр Атбаш с попощью обратного алфавита. Зашифровала слово.

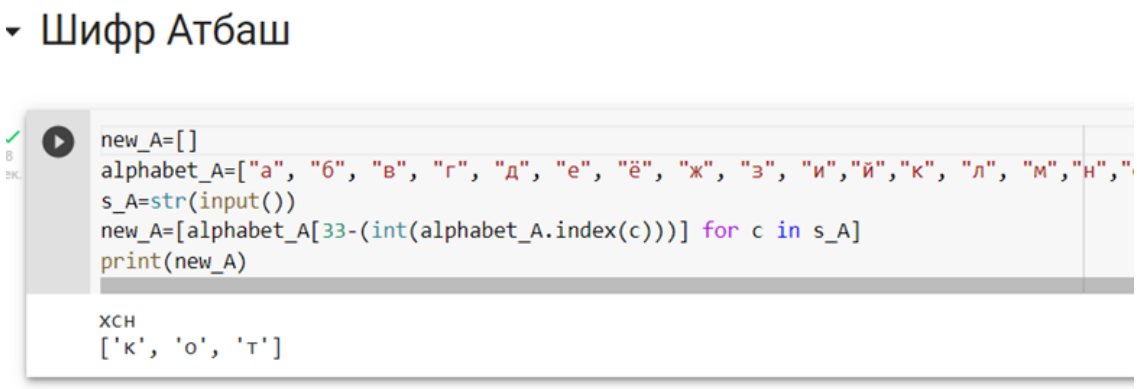
(рис. -@fig:001)



Так как шифрованием методом Атбаш является фактически нахождением букв обратным в алфавите, то для нахождения обратной буквы можно отнять от числа символов в списе место, на котором стоит шифруемая буква. Именно по такому принципу работает программа, которая на слайде зашифровала слово **кот**.

2. Дешифровала шифруемое слово с шифром Атбаш.

(рис. -@fig:001)



Используя ту же программу, с помощью которой мы шифровали слово, можно спокойно дешифровать и вернуть **кота**.

Выводы

В ходе данной лабораторной работы, написала 2 программы для шифров простой замены. Поняла принцип шифрования и осовила написание шифров Атбаш и Цезаря на языке Python.

Список литературы

1. Шифры простой замены// Хабр URL: https://habr.com/ru/post/583616/ (дата обращения: 10.09.2022).
2. Лабораторная работа 1. Шифры простой замены. // Туис URL: https://esystem.rudn.ru/pluginfile.php/1198312/mod_resource/content/2/007-lab_crypto-gamma.pdf (дата обращения: 12.09.2022).
3. Простейшие методы шифрования с закрытым ключом // НОУ ИНТУТ URL: https://intuit.ru/studies/courses/691/547/lecture/12373?page=4 (дата обращения: 12.09.2022).