Лабораторная работа №1

Шифры простой замены

Якушевич Артём Юрьевич

Содержание

# 1 Цель работы

Ознакомиться с шифрами простой замены и обучиться их программной реализации.

# 2 Задание

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

# 3 Теоретическое введение

При подготовке использовалась методичка со страницы курса в ТУИС.[1]

Шифр Цезаря является примером метода подстановки. Дальнейшее усовершенствование оригинального сдвига символа на три позиции в шифре Цезаря состоит в использовании арифметики по модулю двадцать шесть для ключа шифрования, который больше двадцати шести.

,

где - значение открытого текста, - номер сдвига.

Шифр Цезаря со сдвигом 1 (рис. 1):



Рис. 1: Шифр Цезаря со сдвигом 1

Шифр Атбаш – шифр простой замены. Шифрование происходит заменой первой буквы алфавита на последнюю, второй на предпоследнюю, и так далее. По сути, это шифр сдвига на всю длину. Шифр Атбаш для русского алфавита (рис. 2):

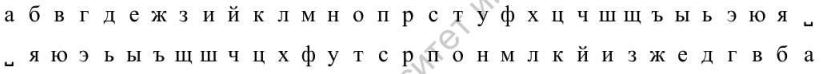


Рис. 2: Шифр Атбаш

# 4 Выполнение лабораторной работы

Работа была выполнена на языке программирования Python.

Сначала реализуем шифр Цезаря (рис. 3):

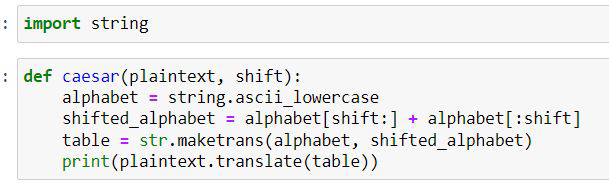


Рис. 3: Программная реализация шифра Цезаря

В переменную alph помещаем латинский алфавит. В переменную shalph задаём алфавит, который начинается с буквы, соответствующей числу сдвига, и прибавляем начало алфавита до этой буквы. Так как в таком случае при числе сдвига больше 26 и меньше -26 программа работать не будет, задаём условие, что в этом случае за число сдвига берется остаток от деления числа на 26. После этого создаём таблицу, в которой каждой букве исходного алфавита сопоставляется буква нового алфавита. В конце выводим зашифрованный текст с помощью метода str.translate, в который передаём таблицу.

Реализация шифра Атбаш (рис. 4):

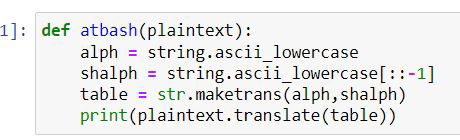


Рис. 4: Программная реализация шифра Атбаш

В переменную alph помещаем алфавит, но в этом случае, опираясь на [1] добавляем к нему пробел. В переменную shalph помещаем тот же алфавит, но перевёрнутый с помощью функционала python. Создаём таблицу и выводим зашифрованный текст.

Ввод исходного текста и числа сдвига (рис. 5):

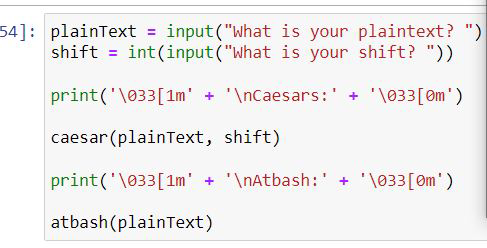


Рис. 5: Программная реализация шифрования

Для ввода исходного текста вводим правило, что не может быть чисел, в противном случае просьба ввести текст будет выведена заново. Для ввода числа сдвига вводим правило, что не может быть букв, в противном случае просьба ввести число сдвига будет выведена заново. Если всё введено правильно, то будет выведен текст, зашифрованный с помощью шифра Цезаря и Атбаш (рис. 6):

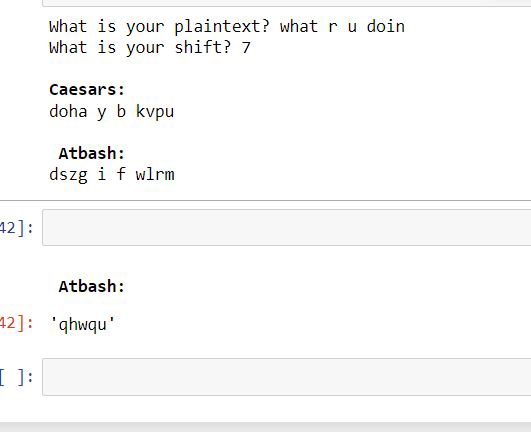


Рис. 6: Вывод программы

# 5 Выводы

Ознакомился с шифрами простой замены и обучился их программной реализации.

# Список литературы

1. ТУИС: Математические основы защиты информации и информационной безопасности (02.04.02) [Электронный ресурс]. РУДН, 2022. URL: <https://esystem.rudn.ru/course/view.php?id=2084>.