Отчёт по лабораторной работе №1

Шифры простой замены

Левкович Константин Анатольевич

Содержание

# 1 Цель работы

Ознакомиться с шифрами простой замены: шифр Цезаря и шифр Атбаш. Реализовать шифры программно.

# 2 Задание

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

# 3 Теоретическое введение

В основе функционирования цифров простой замены лежит следующий принцип: для получения шифртекста отдельные символы или группы символов исходного алфавита заменяются символами или группами символов шифроалфавита.

Шифр Цезаря является примером метода подстановки. Он является моноалфавитной подстановкой, то есть каждой букве открытого текста ставится в соответствие одна буква шифротекста. В оригинальной шифре Цезаря используется свдиг на три символа. Обобщенный вид шифра Цезаря предполает сдвиг символов на произвольное число . Для стандартного алфавита математический вид шифра принимает вид: позиции символа в шифроалфавите есть остаток от деления на кол-во символов в алфавите (26) от позиции символа в исходном алфавите вместе со сдвигом .

,

где - значение открытого текста, - номер сдвига.

Шифр Цезаря со сдвигом 1 (рис. 1):

Рис. 1: Стандартная реализация Шифра Цезаря (сдвиг на 3)

Рис. 1: Стандартная реализация Шифра Цезаря (сдвиг на 3)

Шифр Атбаш - шифр простой замены со сдвигом на всю длину алфавита. Для алфавита, состоящего только из русских букв и пробела, таблица шифрования будет иметь следующий вид: (рис. 2):



Рис. 2: Шифр Атбаш

# 4 Выполнение лабораторной работы

Работа была выполнена на языке программирования Python.

Сначала реализуем шифр Цезаря (рис. 3):

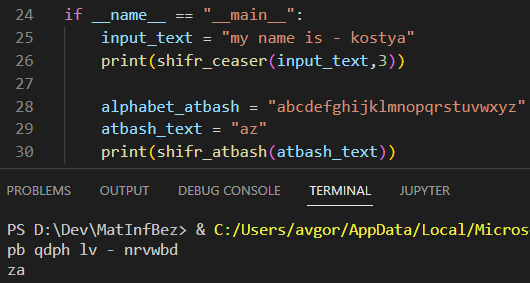


Рис. 3: Программная реализация шифра Цезаря

Задаем алфавит alphabet, состоящий из латинских букв нижнего регистра. Функция shifr\_caeser принимает на вход 2 аргумента: input\_text - входное сообщение, необходимое зашифровать и k - сдвиг алфавита. В цикле для каждого символа проверяется вхождение в исходный алфавит. Для непопавших в алфавит символов замены не требуется, так как сюда попадают спецсимволы. Если символ встретился в алфавите, то из исходного алфавита берется символ, соответующий остатку от деления на 26 исходного символа, сдвинутого на k.

Реализация шифра Атбаш (рис. 4):

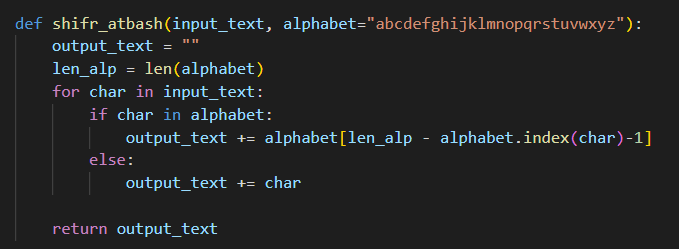


Рис. 4: Программная реализация шифра Атбаш

Функция shifr\_atbash принимает на вход открытый текст и алфавит. По умочанию значение алфавита будут латинские буквы нижнего регистра. Логика для спецсимволов данного шифрования аналогична шифру Цезаря: они не изменяются и попадают в зашифрованное сообщение в исходном виде. Для всех других символов берется зеркально отраженный символ из алфавита: .

Программная реализация шифров Цезаря и Атбаш представлена на рисунке: в обе функции подается один обязательный аргумент - открытый текст и необязательный. Для шифра Цезаря задается сдвиг, для шифра Атбаша задается произвольный алфавит. (рис. 5):

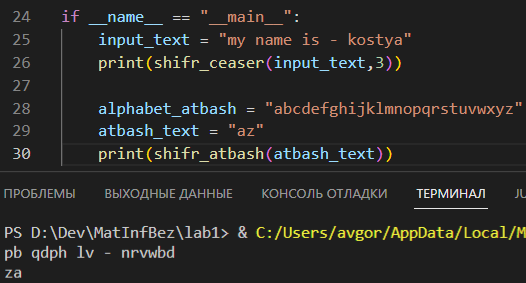


Рис. 5: Вывод программы

# 5 Выводы

Ознакомился с шифрами простой замены: шифр Цезаря и шифр Атбаш. Реализовал шифры программно на языке программирования Python.