Первая лабораторная работа. Шифры простой замены

НФИмд-01-23

Асеинова Елизавета Валерьевна

Содержание

# 1 Цель работы

Цель данной работы - ознакомиться с шифрами простой замены: шифр Цезаря и шифр Атбаш, а также научиться применять их на практике.

# 2 Задание

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

# 3 Теоретическое введение

Шифр Цезаря - это моноалфавитная подстановка, т.е каждой букве открытого текста ставится в соответствие одна буква шифртекста. 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.

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

# 4 Выполнение лабораторной работы

1. Произведено ознакомление с шифрами Цезаря и Атбаш по методическим материалам курса
2. Прописан код для шифра Цезаря на языке программирования Python. Код для англоязычных сообщений. Сначала определяем, является ли символ буквой, затем проверяем на верхний и нижний регистр. После этого по формуле определяем символ, полученный в результате сдвига элемента на значение k. Символы, не являющиеся буквами, остаются неизменными.



Рис. 1: Шифр Цезаря

1. Выводим на экран результат применения шифра Цезаря для произвольного текста со сдвигом на значение k = 5.

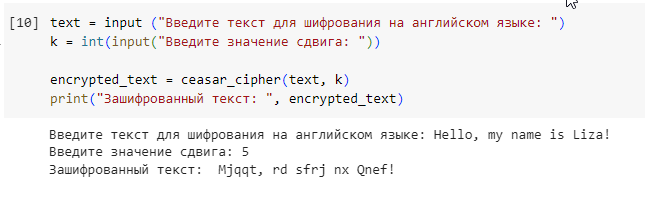


Рис. 2: Результат применения шифра Цезаря

1. Прописан код для шифра Атбаш на языке программирования Python. Код для англоязычных сообщений. Сначала определяем, является ли символ буквой, затем проверяем на верхний и нижний регистр. После этого по формуле определяем символ, полученный в результате отзеркаливание элемента. Символы, не являющиеся буквами, остаются неизменными.



Рис. 3: Шифр Атбаш

1. Выводим на экран результат применения шифра Атбаш.

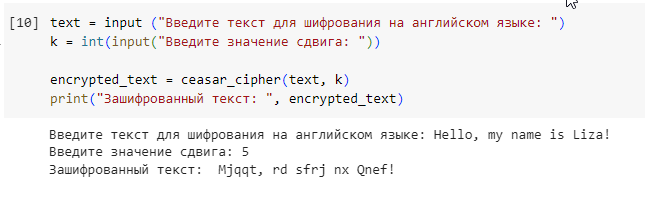


Рис. 4: Результат применения шифра Атбаш

# 5 Выводы

В рамках данной лабораторной работы было произведено ознакомление с шифром Цезаря и шифром Атбаш. Оба шифра были реализованы на языке программирования Python.

# 6 Список литературы

1. Методические материалы курса