Отчёт по лабораторной работе 1

Шифры простой замены

Гурбангельдиев Мухаммет НФИмд-01-22

Содержание

[1 Цель работы 1](#_Toc114342348)

[2 Теоретические сведения 1](#_Toc114342349)

[3 Выполнение лабораторной работы 2](#_Toc114342350)

[4 Выводы 3](#_Toc114342351)

[5 Список литературы 4](#_Toc114342352)

# 1 Цель работы

Приобретение навыков программной реализации простых шифров подстановки и замены.

# 2 Теоретические сведения

Шифр Цезаря (также он является шифром простой замены) - это моноалфавитная подстановка, т.е. каждой букве открытого текста ставится в соответствие одна буква шифртекста. На практике при создании шифра простой замены в качестве шифроалфавита берется исходный алфавит, но с нарушенным порядком букв алфавитная перестановка).

При достижении конца алфавита выполнялся циклический переход к его началу. Таким образом, шифр-алфавит циклически сдвинут влево на K позиций относительно нормативного алфавита.

Цезарь использовал этот шифр замены при смещении. k = 3. Такой шифр можно задать таблицей подстановок, содержащей соответствующие пары букв открытого текста и шифротекста [1]. (рис. -fig. 1)

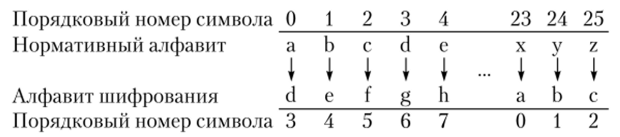


Figure 1: Figure 1: Шифр Цезаря

Шифр Атбаш:

Еще один шифр простой (моноалфавитной) замены. Шифрование осуществляется путем замены первой буквы алфавита на последнюю, второй на предпоследнюю и так далее. (рис. -fig. 2)

Этот шифр использовался для еврейского алфавита и отсюда получил свое название. Первая буква - алеф, заменяется на тау (последнюю), вторая буква - бет, заменяется на шин (предпоследнюю). Из этих букв и сформировалось название. []

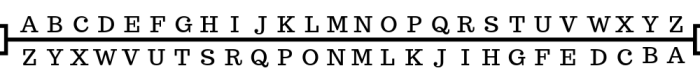


Figure 2: Figure 2: Шифр Атбаш

# 3 Выполнение лабораторной работы

1. Написал функцию caesar для шифрования и расшифровки текста. (рис. -fig. 3)

Сначала написал алфавит в виде списки.

Для расшифровки умножил ключ на -1.

Написал цикл для проверки каждой буквы в нашем слове, а затем определил ее позицию в алфавите с помощью index метода, который возвращает индекс указанного элемента в списке. Как определил позицию, сложил на него ключ (shift). потом распечатал зашифрованный текст.

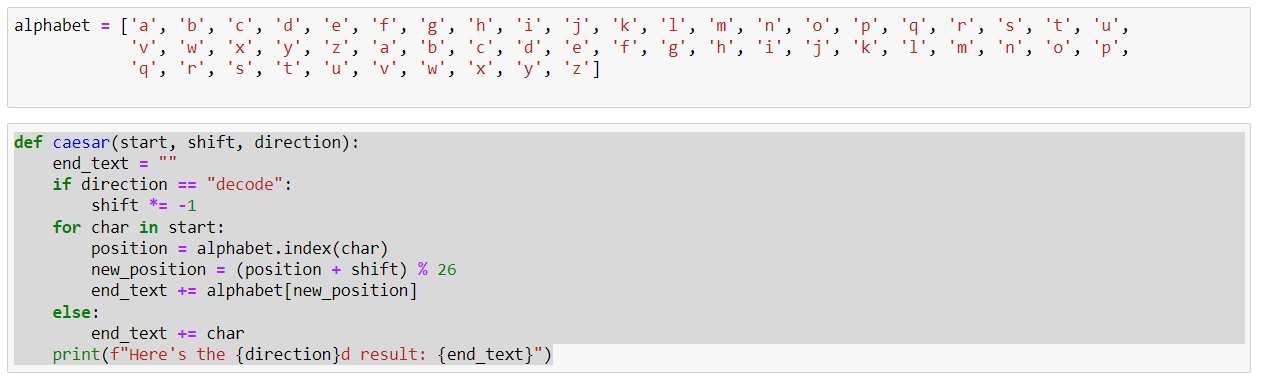


Figure 3: Figure 3: Функция для кодирования текста шифром Цезаря

1. Написал функцию atbash для шифрования и расшифровки текста. (рис. -fig. 4)

Для атбаша сделал аналогично, для сдвига на всю длину алфавита нам нужно умножить позицию на -1.



Figure 4: Figure 4: Функция для кодирования текста шифром Атбаша

1. Написал блок выбора нужного метода и ввода текста. (рис. -fig. 5)

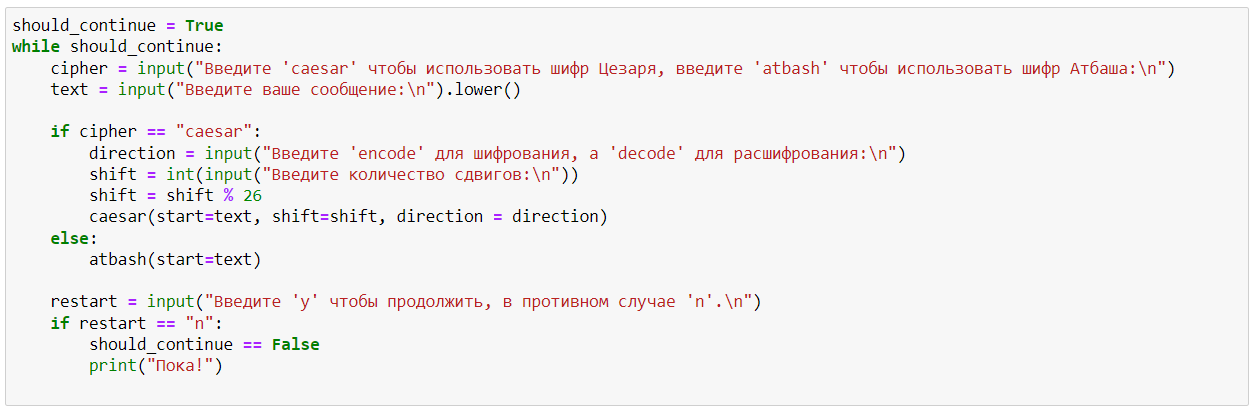


Figure 5: Figure 5: Код для выбора метод шифрования и ввода текста

1. Зашифровал и расшифровал слова password с помощью шифра Цезаря. (рис. -fig. 6) (рис. -fig. 7)

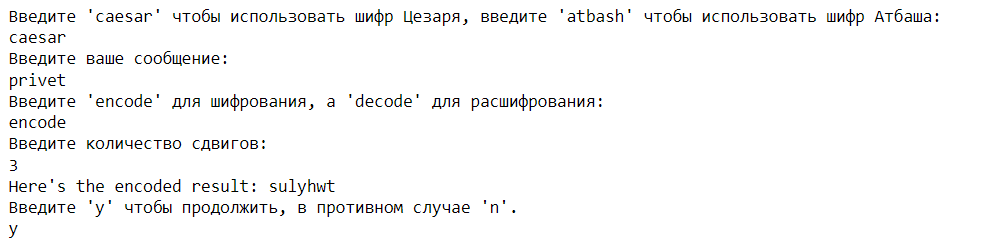


Figure 6: Figure 6: Получение шифрования текста методом Цезаря

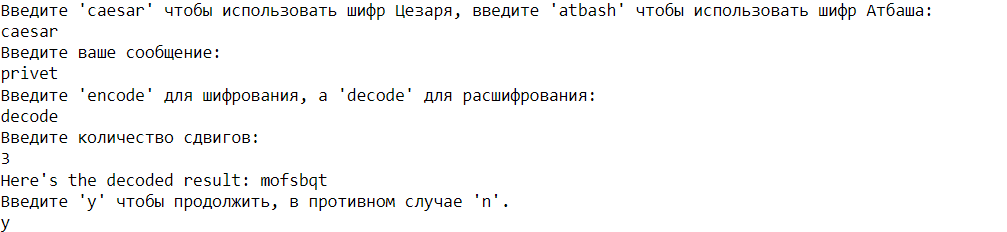


Figure 7: Figure 7: Получение шифрования текста методом Цезаря

1. Зашифровал и расшифровал слова password с помощью Атбаша. (рис. -fig. 8)

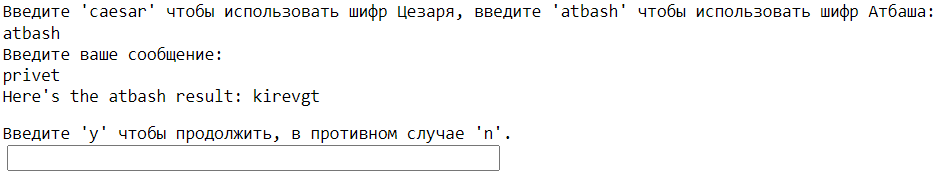


Figure 8: Figure 8: Получение шифрования текста методом Атбаша

# 4 Выводы

Приобрел навыки программной реализации простых шифров подстановки и замены.

# 5 Список литературы

1. Шифры простой замены. — URL: https://studme.org/239550/

informatika/shifry\_prostoy\_zameny.

1. Шифр Атбаш. — URL: https://studbooks.net/2215784/informatika/shifr\_atbash.