Лабораторная работа №1. Шифры простой замены.

Предмет: Математические основы защиты информации и информационной безопасности

Александр Сергеевич Баклашов

Содержание

List of Figures

1 Цель работы

Рассмотреть шифры простой замены, а именно:

— Шифр Цезаря

— Шифр Атбаш

2 Задание

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

3 Теоретическое введение

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.

Шифр Атбаш — это простой метод шифрования, при котором буквы сдвигаются на всю длину алфавита.

4 Выполнение лабораторной работы

4.1 Шифр Цезаря

4.1.1 Задача

Реализовать шифр Цезаря с произвольным ключом k.

4.1.1.1 Решение

Для начала, инициализируем алфавит (латинские буквы нижнего регистра), затем предложим ввести ключ смещения и фразу. После введения фразы, приступаем к реализации шифрования: проходимся по буквам фразы и алфавита. Если находится совпадение — смещаем букву на количество букв алфавита, равное ключу шифрования, и печатаем результат.

Если совпадений нет (например, написаны знаки препинания), печатаем символы без изменений.(рис. 4.1)

Figure 4.1: Шифр Цезаря

4.2 Шифр Атбаш

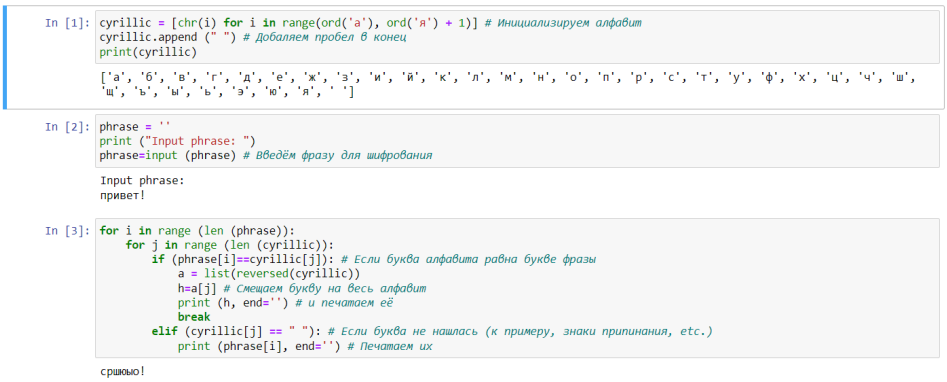
4.2.1 Задача

Реализовать шифр Атбаш

4.2.1.1 Решение

Для начала, инициализируем алфавит (кириллица нижнего регистра), также добавим пробел в конце алфавита. Затем предложим ввести фразу. После введения фразы, приступаем к реализации шифрования: проходимся по буквам фразы и алфавита. Если находится совпадение — смещаем букву на весь алфавит, и печатаем результат.

Если совпадений нет (например, написаны знаки препинания), печатаем символы без изменений. (рис. 4.2)



```
In [1]: cyrillic = [chr(i) for i in range(ord('а'), ord('я') + 1)] # Инициализируем алфавит
        cyrillic.append (" ") # Добаляем пробел в конец
        print(cyrillic)

        ['а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш',
        'щ', 'ъ', 'ы', 'ь', 'э', 'ю', 'я', ' ']

In [2]: phrase = ''
        print ("Input phrase: ")
        phrase=input (phrase) # Введём фразу для шифрования

        Input phrase:
        привет!

In [3]: for i in range (len (phrase)):
            for j in range (len (cyrillic)):
                if (phrase[i]==cyrillic[j]): # Если буква алфавита равна букве фразы
                    a = list(reversed(cyrillic))
                    h=a[j] # Смещаем букву на весь алфавит
                    print (h, end='') # и печатаем её
                    break
                elif (cyrillic[j] == " "): # Если буква не нашлась (к примеру, знаки припинания, etc.)
                    print (phrase[i], end='') # Печатаем их

        сршюю!
```

Figure 4.2: Шифр Атбаш

5 Выводы

В ходе данной лабораторной работы я рассмотрел и реализовал такие шифры простой замены, как шифр Цезаря и шифр Атбаш.

6 Библиография

1. Python documentation. [Электронный ресурс]. М. URL: Python documentation (Дата обращения: 16.09.2023).

2. Лабораторная работа №1. Задача о погоне. - 4 с. [Электронный ресурс]. М. URL: Лабораторная работа №1. Шифры простой замены. (Дата обращения: 16.09.2023).