Математические основы защиты информации и информационной безопасности. Отчет по лабораторной работе №1

Шифры простой замены

Юдин Герман Станиславович 1132236901

Содержание

# 1 Цель работы

Освоить на практике шифры простой замены.

# 2 Выполнение лабораторной работы

Требуется реализовать:

1. Шифр Цезаря с произвольным ключом K.
2. Шифр Атбаш.

## 2.1 Шифр цезаря

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 простойзамены в качестве шифроалфавита берется исходный алфавит, но с нарушеннымпорядком букв (алфавитная перестановка). Для запоминания нового порядкабукв перемешивание алфавита осуществляется с помощью пароля. В качествепароля могут выступать слово или несколько слов с неповторяющимися буквами. Шифровальная таблица состоит из двух строк: в первой записывается стандартный алфавит открытого текста, во второй — начиная с некоторой позицииразмещается пароль (пробелы опускаются), а далее идут в алфавитном порядке оставшиеся буквы, не вошедшие в пароль. В случае несовпадения начала пароля с началом строки процесс после ее завершения циклически продолжается с первой позиции. Ключом шифра служит пароль вместе с числом, указывающим положение начальной буквы пароля.

Чтобы реализовать программу был написал след. код на python:

Выписан алфавит с учетом возможного пробела fig. 1.

Алфавит

Figure 1: Алфавит

Вводится число, на которое будет произведен сдвиг. Даже если число слишком большое оно преобразуется в возможный интервал (берётся остаток от деления) fig. 2.

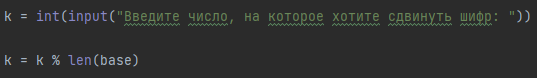


Figure 2: Ввод k

Вводится контрольное слово, у которого берутся только уникальные символы fig. 3.

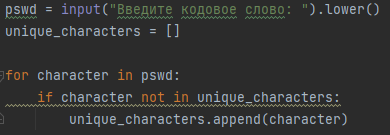


Figure 3: Контрольное слово

После слова добавляется весь оставшийся алфавит fig. 4.

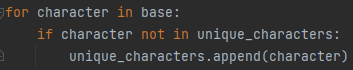


Figure 4: Преобразование зашифрованного алфавита 1

Происходит перемещение k символов в начало fig. 5.

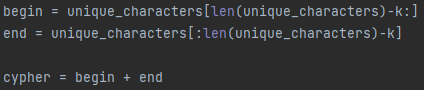


Figure 5: Преобразование зашифрованного алфавита 2

Выводятся оба алфавита. А также происходит ввод фразы, которую хотим зашифровать. Шифрование происходит за счет вычиления индекса символа и выбора символа из зашифрованного алфавита по данному символу fig. 6.

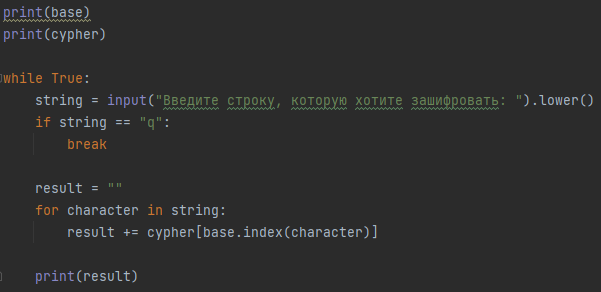


Figure 6: Шифрование фразы

Результат работы алгоритма представлен на рисунке fig. 7.

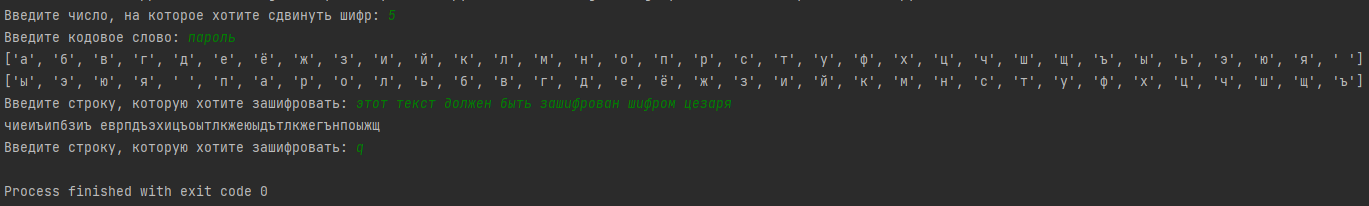


Figure 7: Результат работы алгоритма

## 2.2 Шифр атбаш

Данный шифр является шифром сдвига на всю длину алфавита, состоящего из русских букв и пробела.

Чтобы реализовать программу был написал след. код на python:

Выписан алфавит с учетом возможного пробела fig. 8.

Алфавит

Figure 8: Алфавит

Алфавит разворачивается fig. 9.

Алфавит

Figure 9: Алфавит

Выводятся оба алфавита. А также происходит ввод фразы, которую хотим зашифровать. Шифрование происходит за счет вычиления индекса символа и выбора символа из зашифрованного алфавита по данному символу fig. 10.

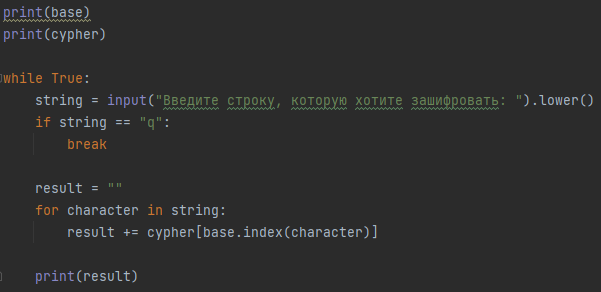


Figure 10: Шифрование фразы

Результат работы алгоритма представлен на рисунке fig. 1.

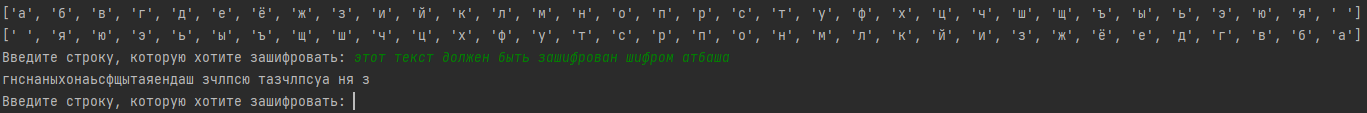


Figure 11: Результат работы алгоритма

# 3 Выводы

В результате выполнения работы я освоил на практике применение шифров простой замены.

# 4 Список литературы

1. Методические материалы курса