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

Шифры простой замены

Терентьев Егор Дмитриевич 1132236902

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:

Функция проверяющая правильность введенного ключа: это значение int и если оно больше значения алфавита, то получаем остаток fig. 1.

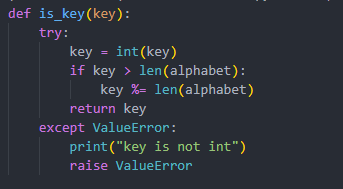


Figure 1: is\_key

Функция проверяющая введенное значения для пароля и слова для шифрования: нужно чтобы каждая буква входила в алфавит fig. 2.

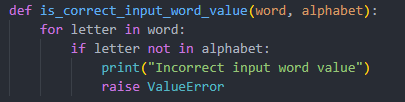


Figure 2: correct\_input\_word

Функция добавляющая только уникальные буквы из слова (нужно для пароля) и функция создающая шифр-алфавит fig. 3.

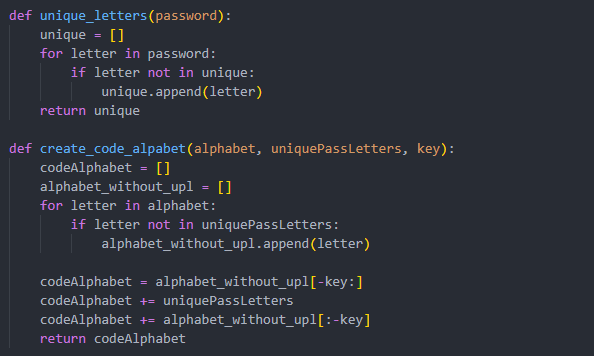


Figure 3: unique\_let\_and\_cipher\_alphabet

Функция шифрующая слово по шифр алфавиту fig. 4

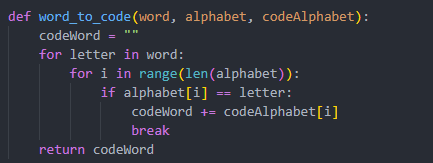


Figure 4: word\_to\_code

Основная фунция запуска где получаем входные значения и шифруем слово fig. 5

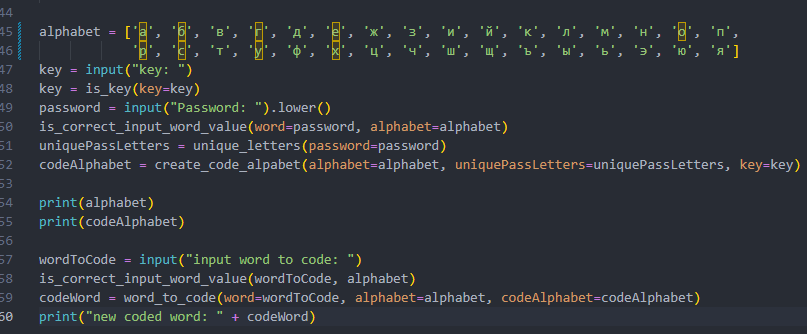


Figure 5: main\_func\_caesar

Пример работы шифра как было показано в материалах к лабораторной работе fig. 6

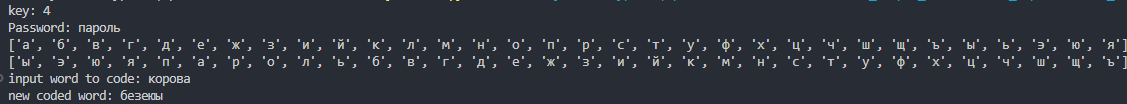


Figure 6: output\_caesar

## 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:

Здесь реализована функция для проверки что каждая буква входит в алфавит (для входных значений), разворот алфавита, и кодировка слова с помощью шифр-алфавита fig. 7

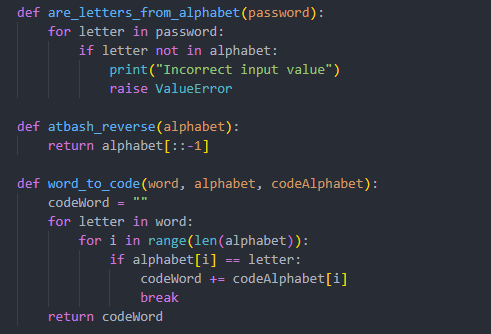


Figure 7: atbash\_func

Основная фунция запуска где получаем входные значения и шифруем слово fig. 8

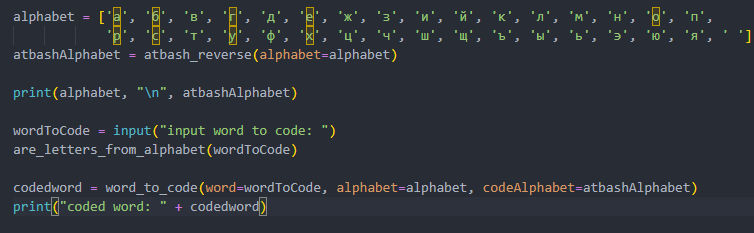


Figure 8: mainFunc\_atbash

Пример работы шифра fig. 9

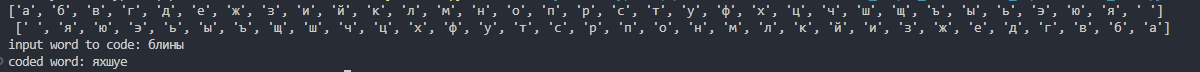


Figure 9: output\_atbash

# 3 Выводы

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

# 4 Список литературы

1. Методические материалы курса