Отчёт по лабораторной работе №1.  
Шифры простой замены

Студент: Агеева Анастасия Сергеевна, 1032212304

Группа: НФИмд-02-21

Преподаватель: Кулябов Дмитрий Сергеевич,

д-р.ф.-м.н., проф.

Москва 2021

Содержание

[1 Цель работы 1](#_Toc87890052)

[2 Задание 1](#_Toc87890053)

[3 Теоретическое введение 2](#_Toc87890054)

[3.1 Основные концепции шифрования 2](#_Toc87890055)

[3.2 Шифр Цезаря 2](#_Toc87890056)

[3.2.1 Математическая модель 2](#_Toc87890057)

[3.2.2 Пример 2](#_Toc87890058)

[3.3 Шифр Атбаш 3](#_Toc87890059)

[3.3.1 Пример 3](#_Toc87890060)

[4 Выполнение лабораторной работы 3](#_Toc87890061)

[5 Выводы 5](#_Toc87890062)

[Список литературы 5](#_Toc87890063)

# 1 Цель работы

Цель данной лабораторной работы изучение основ шифрования и реализация двух алгоритмов шифрования: шифра Цезаря и шифра Атбаш.

# 2 Задание

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

# 3 Теоретическое введение

## 3.1 Основные концепции шифрования

**Шифрование** [1] представляет собой сокрытие информации от неавторизованных лиц с предоставлением в это же время авторизованным пользователям доступа к ней. Пользователи называются авторизованными, если у них есть соответствующий ключ для дешифрования информации. Это очень простой принцип. Вся сложность заключается в том, как реализуется весь этот процесс.

Еще одной важной концепцией, о которой необходимо знать, является то, что целью любой системы шифрования является максимальное усложнение получения доступа к информации неавторизованными лицами, даже если у них есть зашифрованный текст и известен алгоритм, использованный для шифрования. Пока неавторизованный пользователь не обладает ключом, секретность и целостность информации не нарушается.

С помощью шифрования обеспечиваются **три состояния безопасности информации**: 1. **Конфиденциальность** - Шифрование используется для сокрытия информации от неавторизованных пользователей при передаче или при хранении. 2. **Целостность** - Шифрование используется для предотвращения изменения информации при передаче или хранении. 3. **Идентифицируемость** - Шифрование используется для аутентификации источника информации и предотвращения отказа отправителя информации от того факта, что данные были отправлены именно им.

## 3.2 Шифр Цезаря

**Шифр Цезаря** [2], также известный как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования. 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.

### 3.2.1 Математическая модель

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики: *y* = (*x* + *k*)mod*n* *x* = (*y* - *k*)mod*n*, где *x* — символ открытого текста, *y* — символ шифрованного текста, *n* — мощность алфавита, а *k* — ключ. С точки зрения математики шифр Цезаря является частным случаем аффинного шифра.

### 3.2.2 Пример

Шифрование с использованием ключа *k* = 3. Буква «Е» «сдвигается» на три буквы вперёд и становится буквой «З». Твёрдый знак, перемещённый на три буквы вперёд, становится буквой «Э», буква «Я», перемещённая на три буквы вперёд, становится буквой «В», и так далее:

Исходный алфавит: А Б В Г Д Е Ё Ж ... Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я  
Шифрованный: Г Д Е Ё Ж З И Й ... Ш Щ Ъ Ы Ь Э Ю Я А Б В

## 3.3 Шифр Атбаш

Атба́ш [3] (ивр. — 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.

Шифр Атбаш можно также рассматривать как частный случай аффинного шифра. Происхождение слова «атбаш» объясняется принципом замены букв. Слово אתבש составлено из букв «алеф», «тав», «бет» и «шин», то есть первой, последней, второй и предпоследней букв еврейского алфавита.

### 3.3.1 Пример

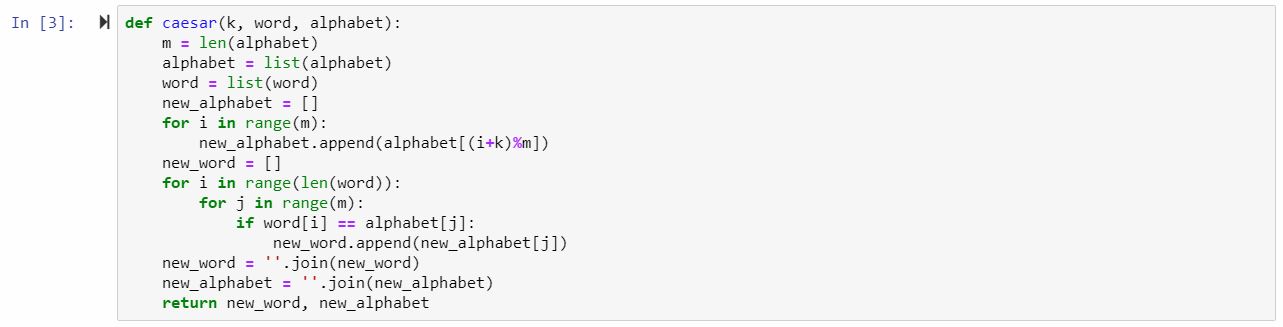
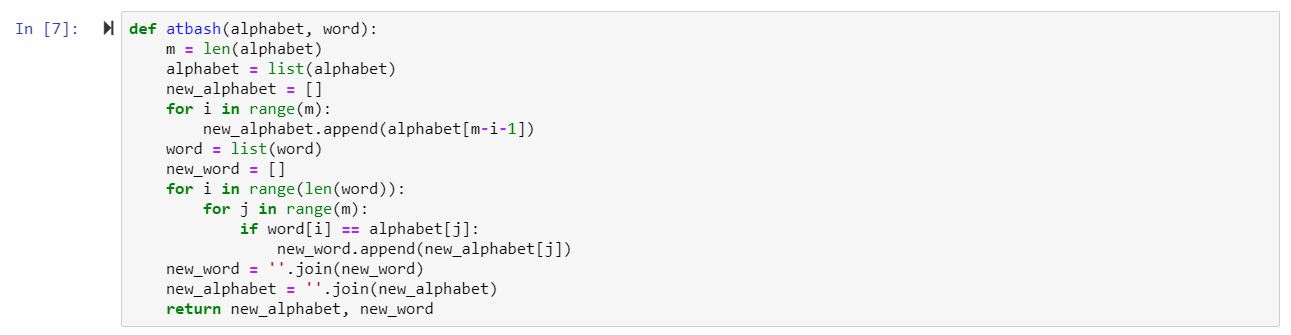
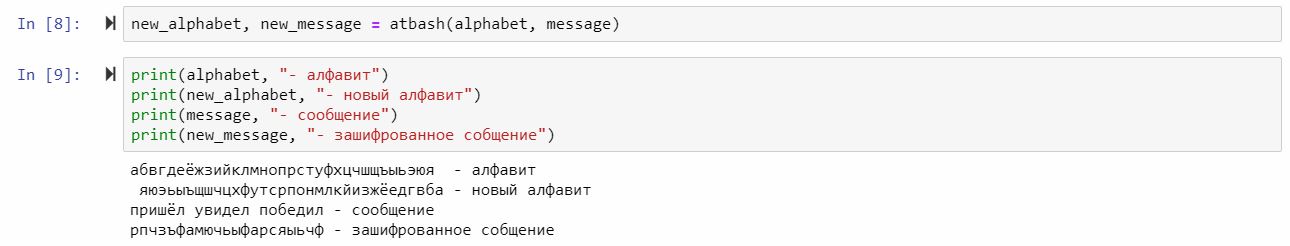
Для русского алфавита реализация шифра Атбаш будет выглядеть следующим образом:

Исходный алфавит: А Б В Г Д Е Ё Ж ... Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я  
Шифрованный: Я Ю Э Ь Ы Ъ Щ Ш ... Й И З Ж Ё Е Д Г В Б А

# 4 Выполнение лабораторной работы

1. Подключение библиотек.

* Figure 1: Подключение библиотеки
* Figure 1: Подключение библиотеки

1. **Реализация шифра Цезаря.**
   1. В качестве начальных значений берется ключ k=3, т.е. алфавит, который также является входным параметром, будет смещаться на три элемента. Алфавитом может быть любая строка неповторяющихся символов. Я использую латинский алфавит. Также задаю строку сообщение, которое будет шифроваться.
   * 
   * Figure 2: Начальные значения для шифра Цезаря
   1. Задам функцию *caesar()*, в качестве параметров передаются заданные начальные данные. Внутри функции высчитывает длина алфавита, а также алфавит и сообщения преобразую в массив. В новый алфавит добавляются элементы заданного алфавита со сдвигом на k. Затем элементы массива сообщения сравниваются с массивом алфавита, и в случае совпадения по найденному индексу добавляется новый элемент в массив зашифрованного сообщения. Новый алфавит и зашифрованное сообщение преобразуются обратно в строку и возвращаются.
   * 
   * Figure 3: Функция шифрования caesar()
   1. Выведу результат работы программы для заданных начальных значений.
   * 
   * Figure 4: Результат выполнения программы
2. **Реализация шифра Атбаш.**
   1. В качестве начальных параметров использую кириллицу с пробелом и сообщение, записанные в строку.
   * 
   * Figure 5: Начальные значения для шифра Атбаш
   1. Задам функцию *atbash()*. Она работает аналогично функции *caesar()*, за исключением формирования нового алфавита: значения старого записываются в новый в обратном порядке.
   * 
   * Figure 6: Функция шифрования atbash()
   1. Выведу результат работы программы для заданных начальных значений.
   * 
   * Figure 7: Результат выполнения программы

# 5 Выводы

В ходе данной лабораторной работы я реализовала два способа шифрования сообщений: при помощи шифра Цезаря и шифра Атбаш.

# Список литературы

1. Лекция 12: Шифрование [Электронный ресурс]. НОУ ИНТУИТ, 2019. URL: <https://intuit.ru/studies/courses/102/102/lecture/2993>.

2. ШИфр Цезаря [Электронный ресурс]. Википедия, 2021. URL: <https://ru.wikipedia.org/wiki/Шифр_Цезаря>.

3. ШИфр Атбаш [Электронный ресурс]. Википедия, 2021. URL: <https://ru.wikipedia.org/wiki/Атбаш>.