Отчёт по лабораторной работе №1

Студент: Майорова О.А., НФИмд-02-21

Преподаватель: д.ф.-м.н. Кулябов Д.С.

Москва 2021

Содержание

[1 Цель работы 1](#_Toc87812802)

[2 Задание 1](#_Toc87812803)

[3 Теоретическое введение 1](#_Toc87812804)

[4 Выполнение лабораторной работы 2](#_Toc87812805)

[5 Выводы 4](#_Toc87812806)

[Список литературы 4](#_Toc87812807)

# 1 Цель работы

Цель: Ознакомиться с шифрами простой замены на примере шифров Цезаря и Атбаш.

# 2 Задание

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

# 3 Теоретическое введение

Шифр простой замены — класс методов шифрования, которые сводятся к созданию по определённому алгоритму таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква шифр-текста. Само шифрование заключается в замене букв согласно таблице. Для расшифровки достаточно иметь ту же таблицу, либо знать алгоритм, по которому она генерируется. К шифрам простой замены относятся многие способы шифрования, возникшие в древности или средневековье, как, например, Атбаш или шифр Цезаря [1].

Шифр Цезаря — один из древнейших шифров. При шифровании каждый символ в открытом тексте заменяется другим, отстоящим левее или правее от него в алфавите на фиксированное число позиций. Шифр назван в честь римского полководца Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами. Например, Цезарь использовал в переписке шифр с ключом *k*=3. Такая таблица шифрования имеет вид табл. 1.

Table 1: Шифр Цезаря, используемый Цезарем

| A | B | C | D | E | F | G | H | I | J | … | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| D | E | F | G | H | I | J | K | L | M | … | T | U | V | W | X | Y | Z | A | B | C |

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами:

*y* = (*x - k*) mod *n*

*x* = (*y - k*) mod *n*,

где

* *x* — символ открытого текста
* *y* — символ шифрованного текста
* *n* — мощность (кол-во символов) алфавита
* *k* — ключ.

С точки зрения современного криптоанализа, шифр Цезаря не имеет приемлемой стойкости [2,3].

Шифр Атбаш — простой шифр подстановки для алфавитного письма, использованный для еврейского алфавита и получивший оттуда свое название. Шифрование происходит заменой первой буквы алфавита на последнюю, второй на предпоследнюю, то есть правило шифрования состоит в замене *i*-й буквы алфавита буквой с номером *n*-*i*+1, где *n* — число букв в алфавите [4,5]. Для кириллицы таблица шифрования будет иметь вид табл. 2.

Table 2: Шифр Атбаш для кириллицы

| а | б | в | г | д | е | ё | ж | з | и | … | ц | ч | ш | щ | ъ | ы | ь | э | ю | я |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| я | ю | э | ь | ы | ъ | щ | ш | ч | ц | … | и | з | ж | ё | е | д | г | в | б | а |

# 4 Выполнение лабораторной работы

Для выполнения лабораторной работы был выбрат язык Python. Сначала реализуем шифр Цезаря с произвольным ключом *k* для латинского алфавита нижнего регистра.

# c - буква для шифрования  
# k - ключ  
  
def Caesar(с, k):  
 n = [(i + k) % 26 for i in range(26)][ord(c) - ord('a')]  
 return chr(ord('a') + n)

Проверим работу функции на примере донесения Ю. Цезаря Сенату об одержанной им победе над Понтийским царем: YHQL YLGL YLFL (“Veni, vidi, vici” - лат. “Пришёл, увидел, победил”) для ключа *k*=3 (табл. 1).

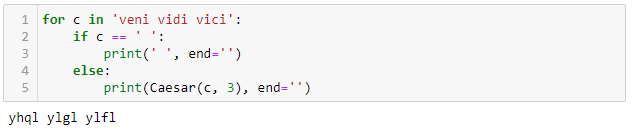


Figure 1: Проверка шифра Цезаря 1

В результате видим, что сообщение было зашифровано корректно (рис. 1).

Ещё раз проверим работу функции уже на любимом изречении императора Августа, который использовал шифр Цезаря с ключом *k*=1 (табл. 3): GFTUJOB MFOUF (“Festina lente” - лат. “Торопись медленно”).

Table 3: Шифр Цезаря, используемый Августом

| A | B | C | D | E | F | G | H | I | J | … | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| B | C | D | E | F | G | H | I | J | K | … | R | S | T | U | V | W | X | Y | Z | A |

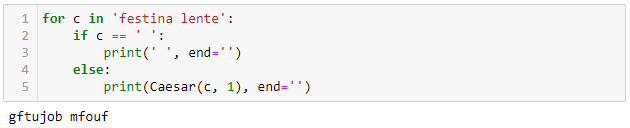


Figure 2: Проверка шифра Цезаря 2

В результате видим, что изречение было зашифровано корректно (рис. 2).

Далее реализуем шифр Атбаш для кириллицы нижнего регистра (табл. 2).

# c - буква для шифрования  
  
def Atbash(c):  
 return chr(ord('а') + (ord('я') - ord(c)))

Проверим работу функции для первой и последней букв алфавита (рис. 3) и для аббревиатуры нашей изучаемой дисциплины (рис. 4).

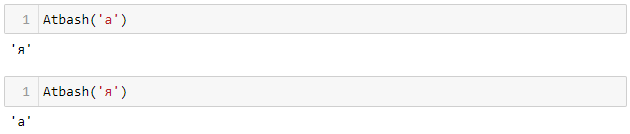


Figure 3: Проверка шифра Атбаш 1

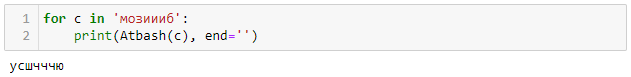


Figure 4: Проверка шифра Атбаш 2

Можно видеть, что шифрование функцией было произведено корректно.

# 5 Выводы

Таким образом, была достигнута цель, поставленная в начале лабораторной работы. Было осуществлено знакомство с шифрами простой замены на примере шифров Цезаря и Атбаш. Также была получена реализация данных шифров на языке Python.

# Список литературы

1. Шифр простой заменыl [Электронный ресурс]. Wikipedia, 2021. URL: <https://ru.wikipedia.org/w/index.php?title=Шифр_простой_замены&oldid=113983740>.

2. Шифр Цезаря [Электронный ресурс]. Wikipedia, 2021. URL: <https://ru.wikipedia.org/w/index.php?title=Шифр_Цезаря&oldid=116640937>.

3. Шифр Цезаря [Электронный ресурс]. Kriptografea, 2009. URL: <http://kriptografea.narod.ru/chezar.html>.

4. Атбаш [Электронный ресурс]. Wikipedia, 2021. URL: <https://ru.wikipedia.org/w/index.php?title=Атбаш&oldid=111452029>.

5. Шифр Атбаш [Электронный ресурс]. Kriptografea, 2009. URL: <http://kriptografea.narod.ru/atbash.html>.