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

Шифры простой замены

Выполнил: Махорин Иван Сергеевич,  
НФИмд-02-21, 1032259380

Содержание

[1 Цель работы 1](#_Toc209355511)

[2 Выполнение лабораторной работы 1](#_Toc209355512)

[2.1 Реализация шифра Цезаря с произвольным ключом K 1](#_Toc209355513)

[2.2 Реализация шифра Атбаш 2](#_Toc209355514)

[3 Список литературы. Библиография 3](#_Toc209355515)

# 1 Цель работы

Изучить шифры простой замены и научиться их реализовывать.

# 2 Выполнение лабораторной работы

## 2.1 Реализация шифра Цезаря с произвольным ключом K

Шифр Цезаря — это древнейший шифр подстановки, в котором каждая буква исходного текста заменяется другой буквой, сдвинутой на фиксированное число позиций в алфавите. Этот метод очень прост: например, при сдвиге на 3, А становится Г, Б — Д и так далее. Для восстановления исходного текста нужно сдвинуть буквы в обратном направлении.

Выполним реализацию этого алгоритма на языке Julia (рис. 1):

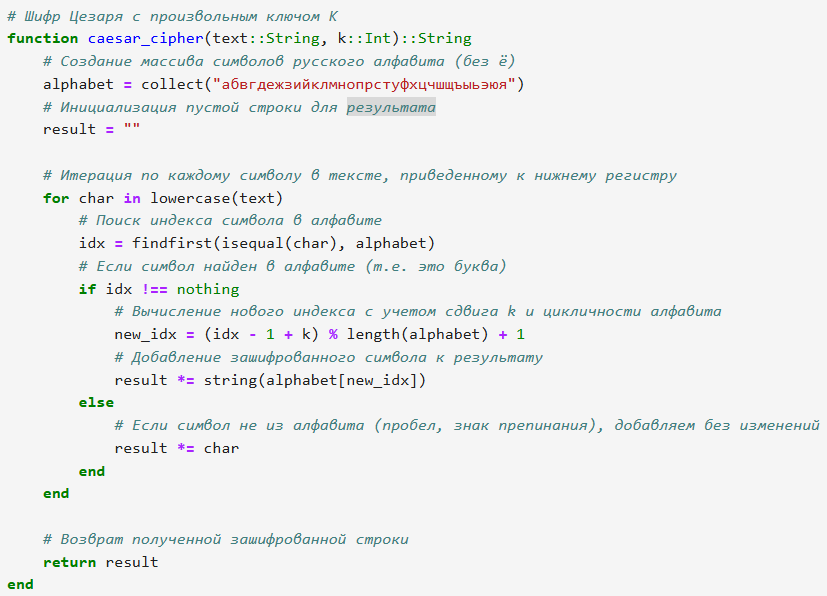


Рис. 1: Реализация шифра цезаря с произвольным ключом K

Проверим работу алгоритма (рис. 2):

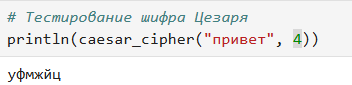


Рис. 2: Проверка

## 2.2 Реализация шифра Атбаш

Шифр Атбаш — это простейший шифр замены, в котором буквы алфавита заменяются в обратном порядке: первая буква становится последней, вторая — предпоследней и так далее. Например, A становится Z, B — Y, а C — X. Этот метод изначально применялся для еврейского алфавита, откуда и получил свое название от первых букв «алеф» и «тав»:

Выполним реализацию этого алгоритма на языке Julia (рис. 3):

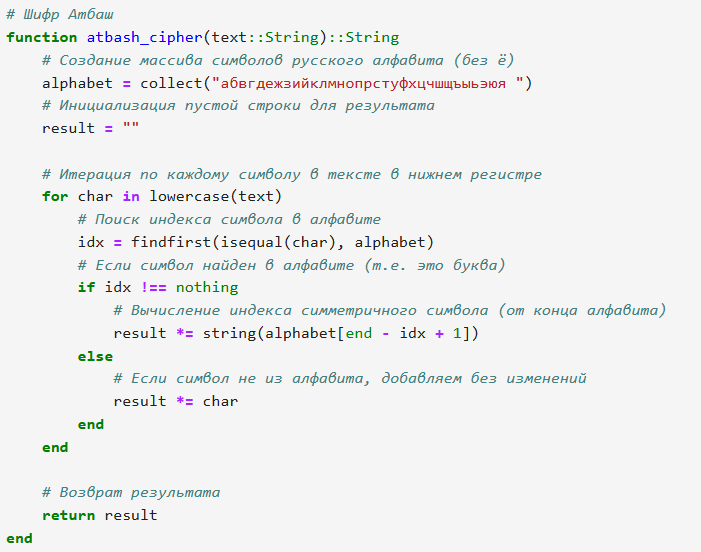


Рис. 3: Реализация шифра Атбаш

Проверим работу алгоритма (рис. 4):

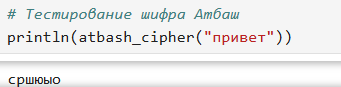


Рис. 4: Проверка

# 3 Список литературы. Библиография

[1] Julia: https://docs.julialang.org/en/v1/