# РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

### Факультет физико-математических и естественных наук

### Кафедра прикладной информатики и теории вероятностей

# ОТЧЕТ

# ПО ЛАБОРАТОРНОЙ РАБОТЕ № 1

### дисциплина: Математические основы защиты информации и информационной безопасности

### Студент: Пиняева Анна Андреевна

### Группа: НПИмд-01-24

### МОСКВА

### 2025

# Теоретическое введение

**Шифр Цезаря** (также является шифром простой замены ) - это моноалфавитная подстановка, т.е. каждой букве открытого текста ставится в соответствие одна буква шифртекста. На практике при создании шифра простой замены в качестве шифроалфавита берется исходный алфавит, но с нарушенным порядком букв (алфавитная перестановка). Для запоминания нового порядка букв перемешивание алфавита осуществляется с помощью пароля. В качестве пароля могут выступать слово или несколько слов с неповторяющимися буквами. Шифровальная таблица состоит из двух строк: первой записывается стандартный алфавит открытого текста, во второй - начиная с некоторой позиции размещается 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.

**Шифр Атбаш.** Данный шифря является шифром сдвига на всю длину алфавита.

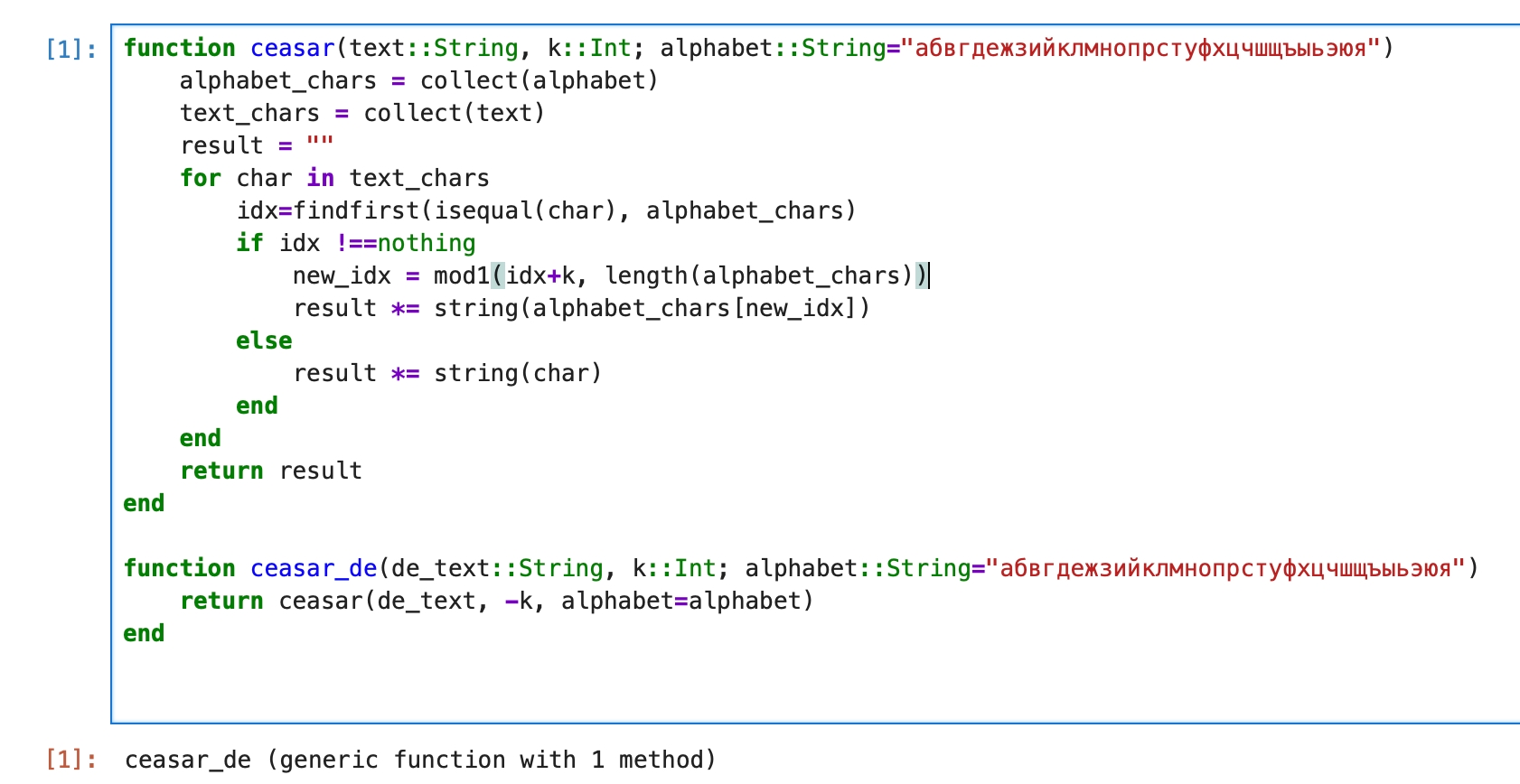
# Цель работы

Знакомство и реализация шифра Цезаря и шифра Атбаш.

# Ход работы

1. Шифр Цезаря. Создаем функцию, которая будет шифровать текст с помощью шифра Цезаря с произвольным ключом k. Функция имеет атрибуты: text - исходный текст для шифрования, k - ключ (величина сдвига), alphabet - используемый алфавит; возвращает зашифрованный текст (рис. 1). Замена происходит путем сдвига каждой буквы на фиксированное число позиций в алфавите. Дешифрование происходит путем сдвига в обратнуб сторону. Результаты тестирования функции можно увидеть на рис.2.

*Рис. 1 Реализация шифра Цезаря:*



N|Solid

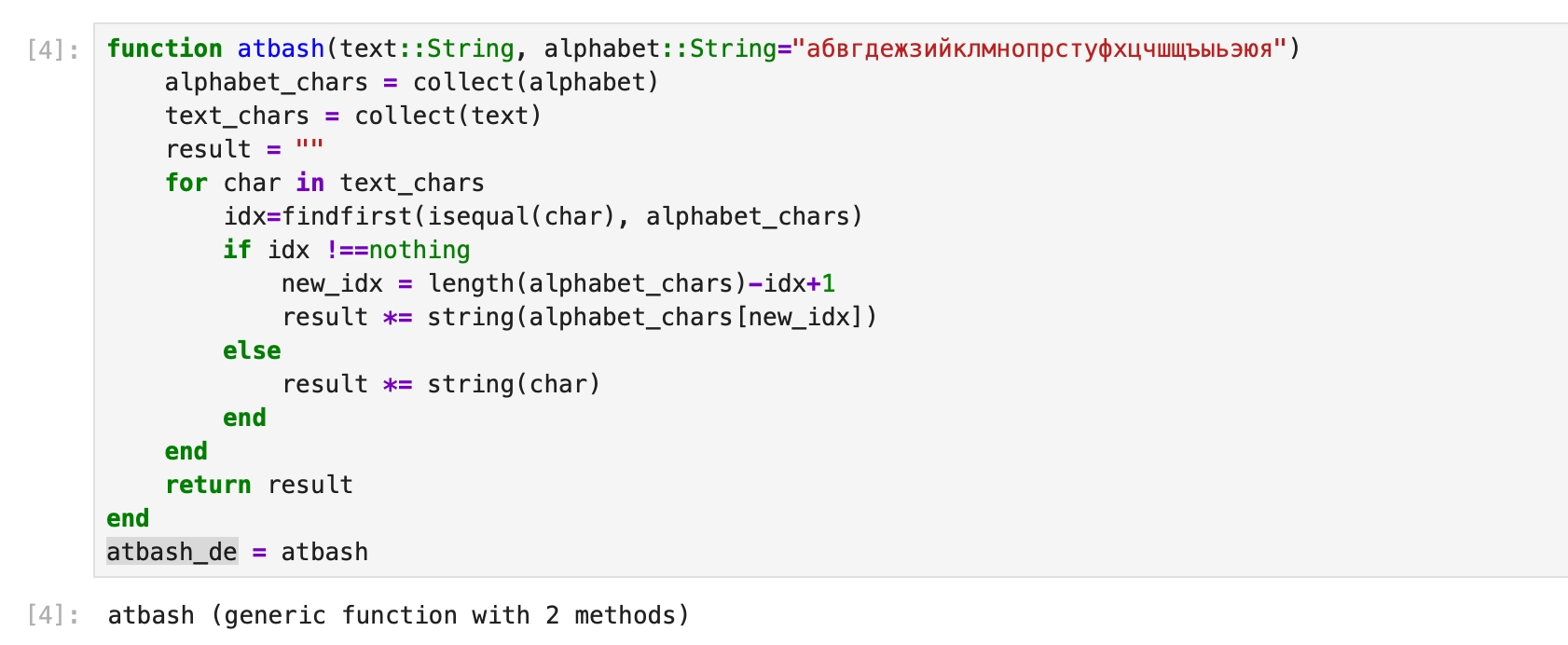
*Рис. 2 Тестирование шифра Цезаря:*



N|Solid

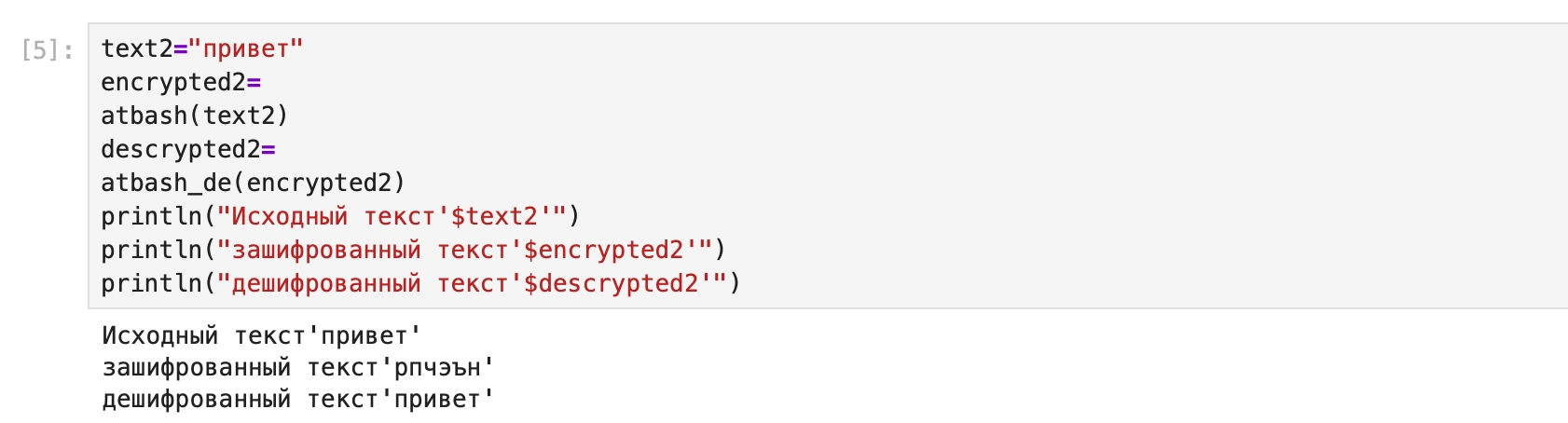
1. Шифр Атбаш. Создаем аналогичную функции Цезаря функцию, но без атрибута k. В функции замена происходит путем “переворачивания” алфавита зеркально. Дешиврование и шифрование одинаковы. Реализация представлена на рис.3. Результаты тестирования функции можно увидеть на рис.4.

*Рис. 3 Реализация шифра Атбаш:*



N|Solid

*Рис. 4 Тестирование шифра Атбаш:*



N|Solid

Вывод: В ходе данной работы мной были изучены шифры простой замены: шифр Цезаря и шифр Атбаш. Были получены теоретические и практические навыки реализации этих шифров. Написан программный код на языке Julia для шифрования, дешифрования и тестирования каждого метода.