**Техническое задание**

Разработать программу, позволяющую шифровать и расшифровывать текст с использованием шифра Цезаря. Программа должна поддерживать несколько режимов работы, обеспечивать обработку больших файлов и иметь валидацию входных данных. Опционально можно добавить графический интерфейс пользователя, а также статистический анализ для автоматического взлома шифра.

Основные задачи:

Реализация шифра Цезаря:

Создание и использование алфавита.

Алгоритм сдвига символов в соответствии с заданным ключом.

Обработка файлов:

Функциональность для работы с файлами (чтение, запись).

Обработка больших текстовых файлов.

Валидация входных данных:

Проверка существования файлов.

Допустимость ключей.

Режимы работы:

Шифрование текста:

Функция шифрования, принимающая файл, ключ и записывающая зашифрованный текст в новый файл.

Расшифровка текста:

Функция расшифровки с использованием известного ключа.

Расшифровка методом brute force (опционально):

Реализация метода brute force для перебора всех ключей до успешного расшифрования.

Расшифровка методом статистического анализа (опционально):

Разработка алгоритма статистического анализа для автоматической расшифровки без ключа, используя особенности языка.

Разработка интерфейса пользователя:

Текстовое меню или (опционально) графический интерфейс

Дополнительные задачи:

Обработка ошибок и исключений.

Оптимизация для производительности.

Документация и тестирование.

Криптология, криптография и криптоанализ

Приступим к разбору теории, которая понадобится тебе при написании итогового проекта. Давай узнаем больше о криптологии и ее составляющих. А заодно — больше о шифре, который ты будешь использовать при написании итогового практического проекта.

Задача: написать программу, которая работает с шифром Цезаря.

Это один из самых простых и известных методов шифрования. Назвали его, само собой, в честь императора Гая Юлия Цезаря, который применял его для секретной переписки с генералами.

Шифр Цезаря — это шифр подстановки: в нем каждый символ в открытом тексте заменяется на символ, который находится на некотором постоянном числе позиций левее или правее него в алфавите.

Допустим, мы устанавливаем сдвиг на 3 (ключ = 3). В таком случае А заменится на Г, Б станет Д, и так далее.

Результат

Результат: программа работает в нескольких режимах

Режимы:

Шифровка текста

Расшифровка текста с помощью ключа

Расшифровка текста с помощью brute force (перебор всех вариантов)

(дополнительно) Расшифровка с помощью статистического анализа текста

Программа должна открывать указанный пользователем файл с текстом и проделывать с ним одно из указанных выше действий. После этого создавать новый файл с результатом.

Программа должна выполнять следующие функции:

Шифровка текста из заданного файла. На вход она получает адрес файла с оригинальным текстом, адрес файла в который нужно записать зашифрованный текст, и сдвиг по алфавиту (это является ключом шифра Цезаря). Не забудь проделать проверку того что а) файл оригинала по заданному адресу существует, и б) ключ от 0 и до (размер алфавита - 1) (или можете взять остаток от деления на размер алфавита).

Расшифровка при известном ключе. На входе — адрес зашифрованного файла и адрес куда писать расшифрованный файл, а также сдвиг по алфавиту который использовался при шифровании (ключ).

Расшифровка методом brute force (перебором всех возможных сдвигов); На входе - адрес зашифрованного файла, (опционально) адрес файла с текстом который является примером текста что был зашифрован (например другой труд того же автора) и адрес файла который должен содержать расшифрованный текст.

Расшифровка методом статистического анализа; На входе тоже самое что и для расшифровке перебором.

Не забудь проделать валидацию входных данных.

Исходный текст для шифрования должен быть в файле. Желательно в формате txt. программа должна уметь работать с большими текстами на сотни страниц. Этот файл программа должна уметь зашифровать и записать зашифрованный текст в другой файл.