Государственное учреждение образования

“БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ”

Кафедра: Интеллектуальных информационных технологий

Дисциплина: Средства и методы защиты информации в интеллектуальных системах

**Отчет по лабораторной работе №2**

**“Простейшие криптографические преобразования”**

Вариант 1

Выполнил:

студент гр. 221701

Телица И.Д.

Проверил:

Захаров В.В.

Минск 2024

#### **Цель**:

Получить навыки шифрования текста, изучить теоретические сведения о различных методах шифрования.

#### **Задача:**

1) Реализовать в виде программы шифр (шифрования), используя шифр Цезаря. Язык исходного текста русский.

2) Реализовать в виде программы атаку полным перебором ключа, используя для оценки правильности выбора ключа визуальный метод или исходный текст для автоматического сравнения результата дешифрования.

3) Оценить криптографическую стойкость реализованного шифра.

4) Предложить варианты усложнения шифра. Предложенные варианты оформить в виде алгоритма.

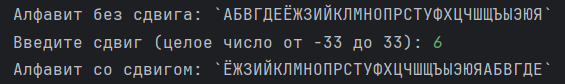
## Шифр Цезаря – это один из шифров подстановки, в котором каждый символ открытого текста заменяется символом, находящимся на некотором, определяемом ключом, постоянном числе позиций левее или правее него в алфавите.

## **Ход работы:**

Задание 1:

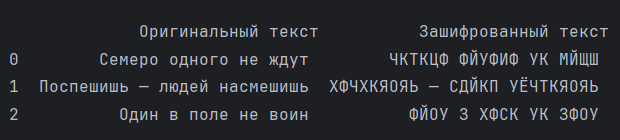
Функция **encrypt\_alphabet(alphabet: str, shift: int)**

Шифрует заданное слово, с заданным сдвигом.

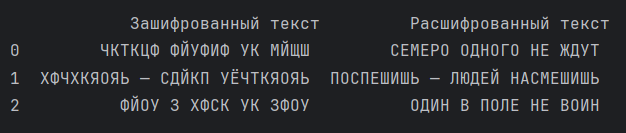


Класс **CaesarEncryptor**

Содержит в себе функционал, связанный с шифрованием текста с заданным сдвигом.

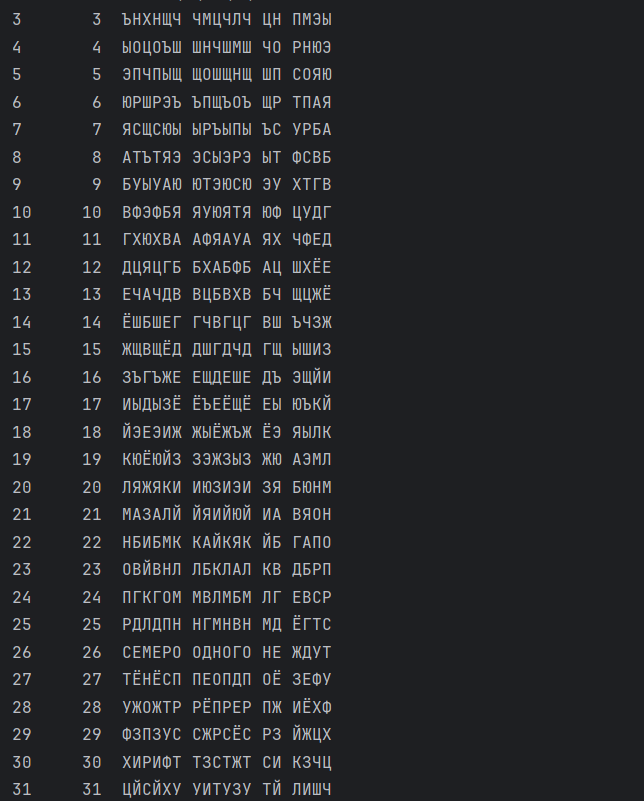


Для расшифрования шифрованного текста необходимо передать сдвиг со знаком ‘-’.



Задание 2:

Зная, что для шифрования текста был использован шифр Цезаря, его расшифрование (взлом шифра, попытка вскрытия сообщения, когда вы НЕ знаете ключ шифрования) не представляет сложности, необходимо лишь перебрать небольшое количество возможных сдвигов.



Задание 3:

В современных реалиях шифр Цезаря невероятно слаб. Во времена жизни Цезаря, ставка делалась на то, что потенциальному взломщику незнаком алгоритм шифрования и уж тем более основы криптографии, что было вполне ожидаемо при уровне образования и развития криптографии того времени.

В наши дни, делать ставку на незнание противником алгоритма нельзя. Также, с учетом доступных ныне вычислительных мощностей, 33 варианта ключа - невероятно маленькое количество, которое любой компьютер способен проверить за доли секунды, именно поэтому шифр Цезаря нельзя считать криптографически стойким.

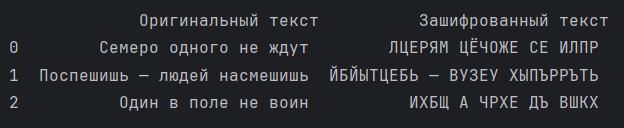
Иной слабостью является однозначность соответствия букв - одна и та же буква оригинального текста всегда соответствует одной и той же букве зашифрованного текста.

Задание 4:

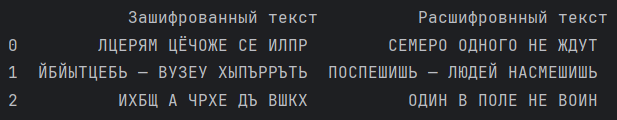
Чтобы усложнить шифр, можно в качестве ключа использовать некоторую математическую функцию, которая для каждого отдельного символа будет определять сдвиг на основании его положения в тексте. Таким образом, для расшифрования текста будет необходимо знать эту самую функцию, число которых запредельно, что не позволит взломать шифр перебором.

Класс **BetterCaesarEncryptor**

Содержит в себе функционал, связанный с шифрованием текста с заданным функцией, которая преобразует по заданной формуле сдвиг.



Для расшифрования шифрованного текста необходимо передать функцию со знаком ‘-’.



#### **Вывод**:

В результате выполнения лабораторной работы была написана программа для шифрования текста русского алфавита с помощью шифра Цезаря, и была осуществлена его расшифровка, а также оценка стойкости алгоритма. Была также реализована программа по усложнению шифра Цезаря.