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 3

Выполнил:

студент гр.121702

Витковская С. И.

Проверил:

Сальников Д.А.

Минск 2023

**Содержание**

[**Цель: 3**](#_10zyi4g1nt1b)

[**Задача: 3**](#_gl8o1xw3chrw)

[**Ход работы: 4**](#)

[**Вывод: 6**](#_y0y3n1dghbe6)

#### **Цель**:

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

#### **Задача:**

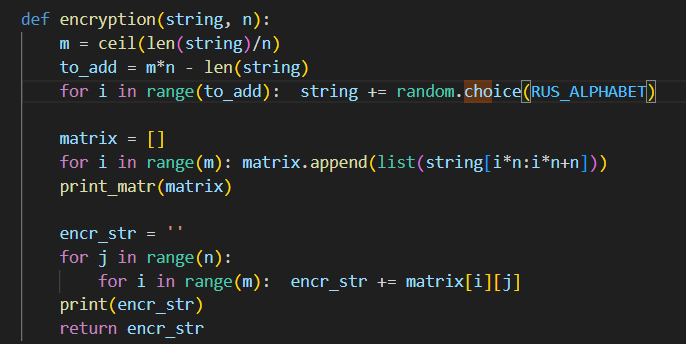
1) Реализовать в виде программы шифр (зашифрование и расшифрование), используя шифр Скитала. Язык исходного текста русский.

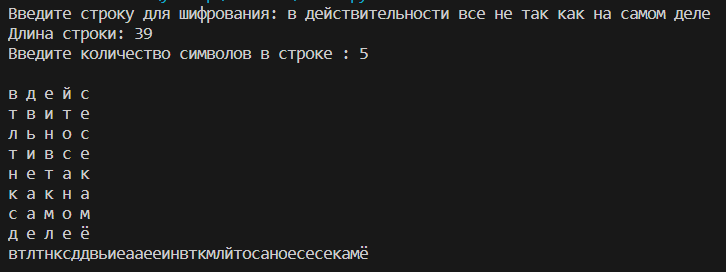
2) Реализовать в виде программы атаку полным перебором ключа, используя для оценки правильности выбора ключа визуальный метод или исходный текст для автоматического сравнения результата дешифрования.

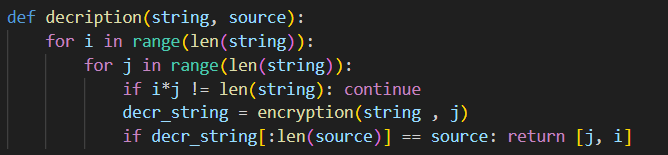
3) Оценить криптографическую стойкость реализованного шифра.

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

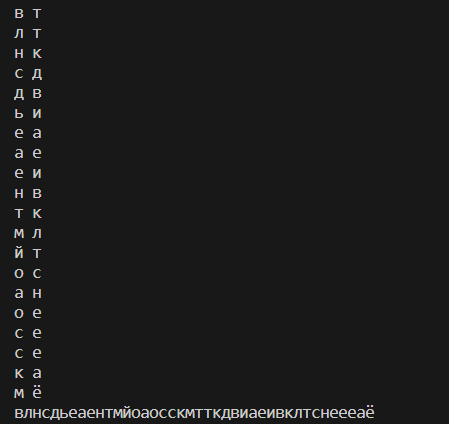
## **Ход работы:**

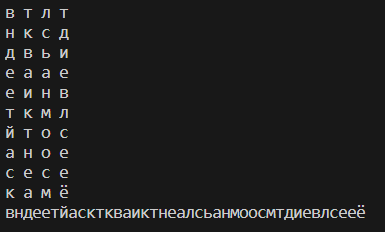
Метод encryption(string, n) подбирает размер матрицы, основываясь на длине текста и количестве символов в строке создаваемой матрицы. Далее заполняет недостающие элементы рандомными символами алфавита. Выводит сгенерированную матрицу и создает строку – зашифрованный текст, считывая столбцы.

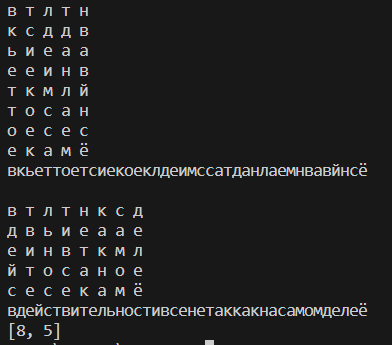




Метод decription(string, source) принимает на вход исходный текст и зашифрованную строку. Далее перебираются всевозможные пары чисел, дающие в произведении длину зашифрованной строки. В метод encryption передается значение строк расшифровывающей матрицы, если это чиссло совпадет с числом столбцов исходной матрицы, то текст будет восстановлен. Будут выведены параметры исходной матрицы.







Для расшифровки текста злоумышленнику понадобится вычислить только два параметра – размеры таблицы. К тому же, если длина зашифрованного текста кратна лишь нескольким значениям, расшифровка займет совсем немного времени, поэтому шифр Скитала нельзя назвать криптографически стойким.

Чтобы усложнить шифр, можно использовать алгоритм поэтапно, например разбивать исходный текст на части и шифровать каждую из частей, используя матрицы с разными параметрами. Так же для усложнения криптограммы можно шифровать текст несколько раз, опять же, используя матрицы разных размеров (главное не использовать противоположные параметры, например 5х3 и 3х5). Можно использовать бОльшие матрицы, которые кратны большому количеству чисел.

#### **Вывод**:

В результате выполнения лабораторной работы была написана программа для шифрования текста русского алфавита с помощью шифра Скитала, и была осуществлена его расшифровка. Были даны рекомендации по увеличению сложности шифрования.