|  |  |  |
| --- | --- | --- |
| **Дисциплина** | **Лабораторная** | **ФИО** |
| Математические основы защиты информации и информационной безопасности | №2 | Александра Миличевич |

# Цель работы

Познакомиться с шифрами перестановки.

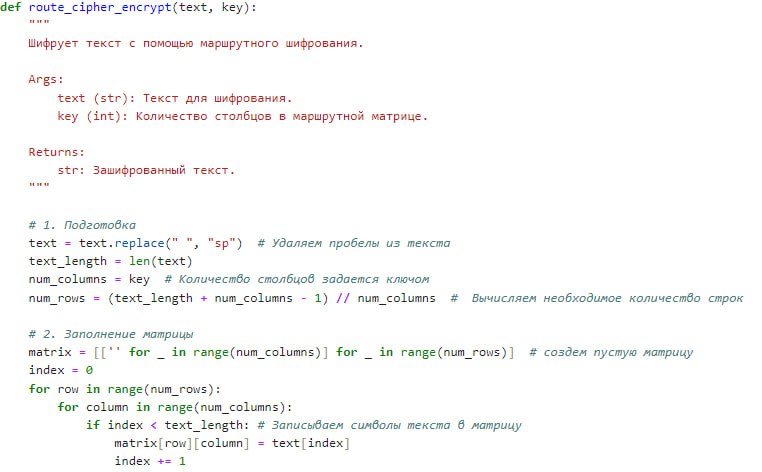
# Задание

1. Программно реализовать маршрутное шифрование.
2. Программно реализовать шифрование с помощью решёток.
3. Программно реализовать шифр Виженера.

# Выполнение лабораторной работы

### Маршрутное шифроваие

1. Код сначала подготавливает текст для шифрования, заменяя пробелы на “sp” и определяя размеры матрицы на основе длины текста и заданного ключа. Затем, символы текста последовательно записываются в матрицу по строкам, заполняя её слева направо и сверху вниз. Эта матрица используется для маршрутного шифрования.

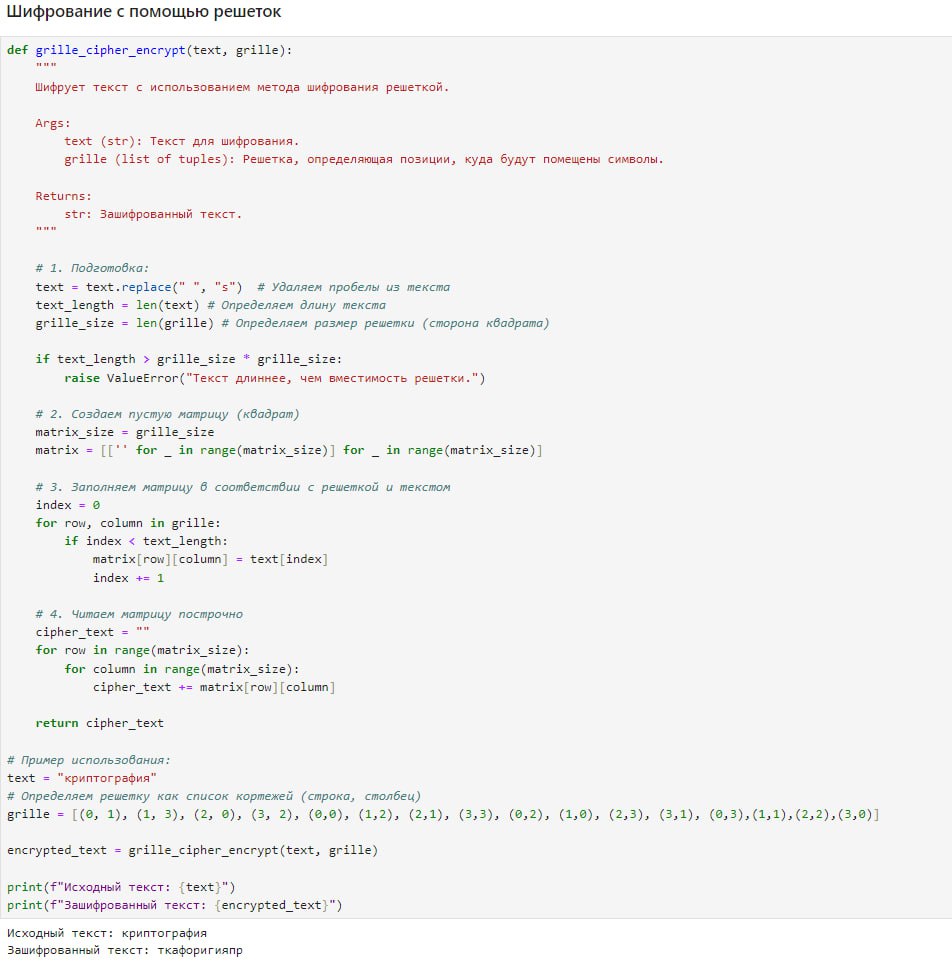


реализация маршрутного шифрования

1.1 # 3. Чтение матрицы по столбцам cipher\_text = "" После заполнения матрицы, код считывает ее по столбцам сверху вниз, формируя зашифрованный текст. Символы каждого столбца добавляются в общий шифрованный текст, который затем возвращается как результат работы алгоритма. Таким образом текст шифруется путем записи по строкам и чтения по столбцам. 

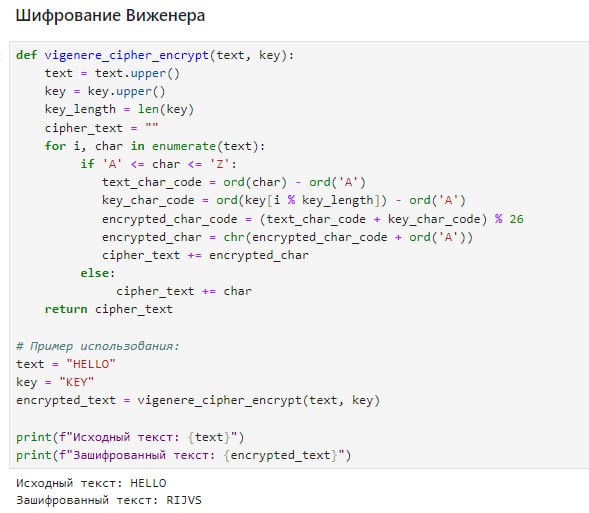
### Шифрование с помощью решеток

Этот код реализует шифрование с использованием решетки (grill e cipher). Сначала он подготавливает текст, удаляя пробелы и проверяя, что текст не превышает размер решетки. Затем, он создает матрицу (решетку) нужного размера, заполняет ее символами текста в порядке, заданном списком grille, и, наконец, считывает матрицу построчно, формируя зашифрованный текст.

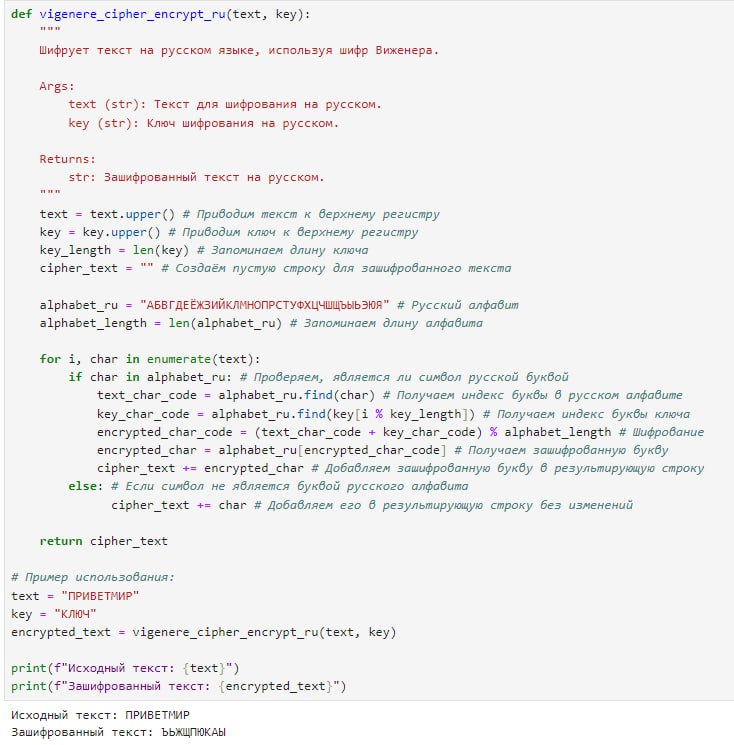
В примере, решетка (grille) задается списком кортежей, где каждый кортеж указывает строку и столбец, куда должен быть помещен соответствующий символ текста. Результат работы алгоритма — зашифрованный текст, сформированный из прочитанных по строкам элементов матрицы. 

### Таблица Виженера

Этот код реализует шифрование Виженера, где каждый символ текста сдвигается на величину, определяемую соответствующим символом ключа, повторяющегося по циклу. Функция vigenere\_cipher\_encrypt сначала приводит текст и ключ к верхнему регистру, а затем для каждой буквы текста вычисляет её сдвиг, используя соответствующую букву ключа и выполняя операцию взятия остатка от деления на 26. Результатом является шифрованный текст, где неалфавитные символы остаются неизменными.В этом конкретном примере текст “HELLO” шифруется с помощью ключа “KEY”, что приводит к зашифрованному тексту, где буквы сдвигаются на величину, задаваемую буквами ключа. Разница между шифрованием Виженера и другими шифрами, например, маршрутным или решеточным, заключается в том, что Виженер использует полиалфавитный шифр с циклическим ключом, в то время как маршрутный и решеточный шифры используют перестановку символов.



реализация шифрования таблица виженера

В коде для шифрования Виженера на русском языке, добавлен русский алфавит (alphabet\_ru) и его длина (alphabet\_length), чтобы обрабатывать символы русского языка. Индексы букв берутся из русского алфавита alphabet\_ru.find(), и для шифрования используется модуль от деления на длину русского алфавита. Если символ не найден в русском алфавите, он добавляется в зашифрованный текст без изменений. 

# Выводы

Программно реализованы шифры перестановки.