Министерство образования Республики Беларусь

Учреждение образования  
БЕЛОРУССКИЙ  ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

                        Факультет      Информационных технологий и управления

                        Кафедра         Интеллектуальных информационных технологий

**ОТЧЁТ**

по лабораторной работе №2

по дисциплине “Средства и методы защиты

информации в интеллектуальных системах”

Вариант 10

Выполнила:

Демидовец Д.В. , гр. 221703

Проверил:

Крищенович В.А.

Минск, 2024

**ПРОСТЕЙШИЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ** Вариант для реализации: Шифр Виженера.

Теоретические сведения:

Шифр Виженера является простой формой многоалфавитной (полиалфавитной) замены. Многоалфавитная замена определяется ключом, содержащим не менее двух вариантов замен. В шифре Виженера в качестве ключа используется секретное слово. При зашифровании вручную может использоваться таблица алфавитов, называемая квадрат Виженера. Для латинского алфавита квадрат Виженера состоит из 26 строк по 26 символов. Каждая следующая строка образуется сдвигом предыдущей на одну позицию. Таким образом, в таблице получается 26 алфавитов. Для зашифрования каждой последующей буквы циклически используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.



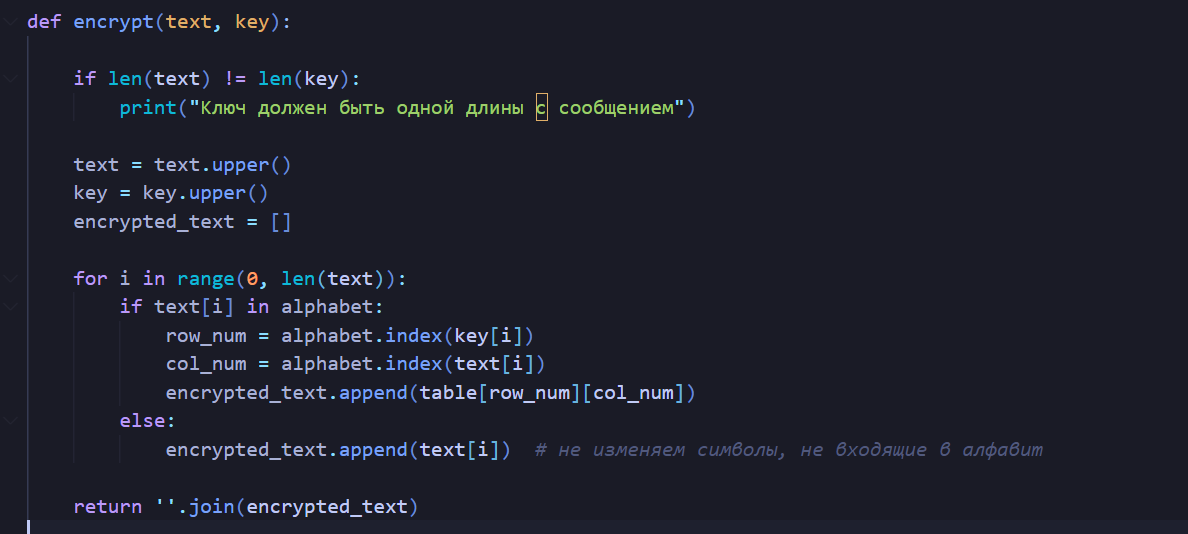
Квадрат Виженера

Задание:

1) Реализовать в виде программы шифр (зашифрование и расшифрование)

в соответствии с вариантом.

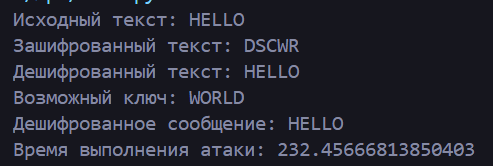
Для шифрования текста методом Виженера реализована функция encrypt. В ней для каждого символа текста находится соответствующий символ в таблице Виженера на пересечении строки (индекс символа ключа в алфавите) и столбца (индекс символа текста в алфавите).



Расшифрованием же занимается метод decrypt, в котором для каждого символа зашифрованного текста определяется индекс символа ключа в алфавите, затем вычисляется исходный символ путем сдвига индекса символа текста назад по алфавиту на количество позиций, соответствующее символу ключа. Если результат выходит за границы алфавита, корректируется отрицательный индекс.



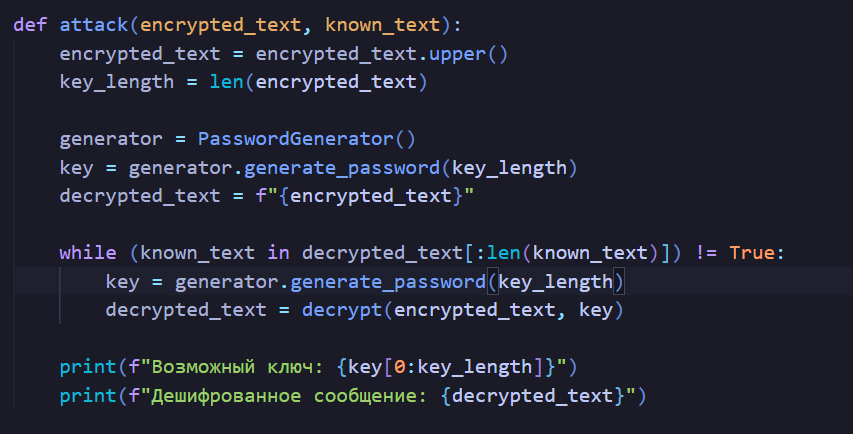
Результат работы программы:



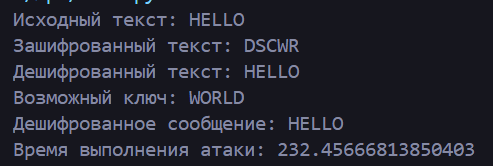
2) Реализовать в виде программы атаку полным перебором ключа,

используя для оценки правильности выбора ключа визуальный метод или

исходный текст для автоматического сравнения результата дешифрования.

В методе attack подбираем ключ из букв английского алфавита с помощью генератора из прошлой лабораторной, продолжая работу цикла, пока текущий ключ не расшифрует заданный текст. После получения искомого ключа выводим результат и время выполнения алгоритма.

Результат работы программы:



3) Криптографическая стойкость шифра Виженера зависит от длины ключа и способов его использования.

При коротких или повторяющихся ключах шифр Виженера не является стойким и может быть взломан с помощью известных методов криптоанализа.

При длинном ключе, используемом один раз, стойкость шифра Виженера значительно возрастает, и он становится достаточно безопасным, однако это усложняет практическую реализацию.

4) Вариант для усложнения шифра:

**Добавление псевдослучайного сдвига к каждому символу**

Алгоритм:

1. У нас на входе текст T длиной n символов и исходный ключ K длиной m символов.
2. Сгенерируем псевдослучайное число r в диапазоне от 1 до длины алфавита (например, для английского языка — от 1 до 26).
3. Применим шифр Виженера для каждого символа текста с исходным ключом K.
4. К каждому зашифрованному символу добавить сдвиг, равный псевдослучайному числу r.

Пример:

-- Начальный текст: **"HELLO"**.

-- Ключ: **"KEY"**.

-- Псевдослучайное число r=3 (будем добавлять сдвиг 3 к каждому зашифрованному символу).

-- Зашифрованный текст: **"ULMYV"**.

-- Результат при обычном шифровании: **"RIJVS"**.

Этот вариант сохраняет простоту алгоритма, но делает шифр Виженера более устойчивым к взлому.