Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет информационный технологий и управления

Кафедра интеллектуальных информационных технологий

Дисциплина: «Средства и методы защиты информации в  
интеллектуальных системах»

Лабораторная работа №2 по теме:  
«Простейшие криптографические преобразования»

Студент гр. 121702

Заломов Р.А.

Проверил:

Сальников Д.А.

Минск 2023

**Тема**

Простейшие криптографические преобразования

**Задание**

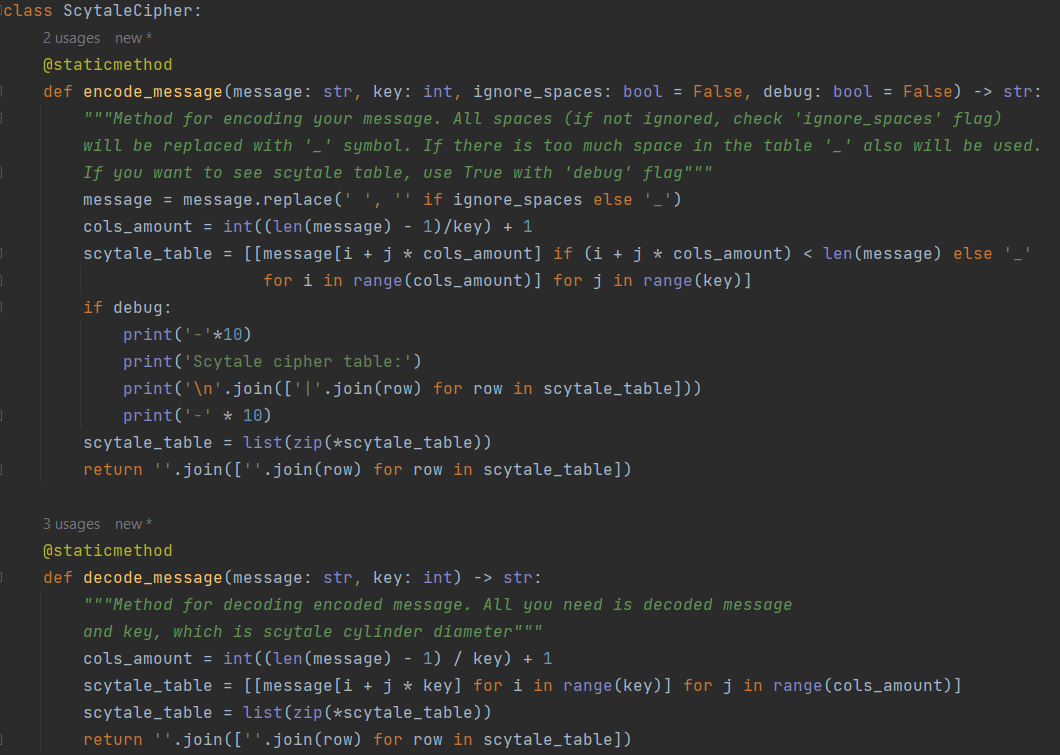
Разработать программу, реализующую следующие функции:

1. Реализовать в виде программы шифр (зашифрование и расшифрование) в соответствии с вариантом. Язык исходного текста русский или английский по выбору исполнителя.
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. Предложить варианты усложнения шифра. Предложенные варианты оформить в виде алгоритма.

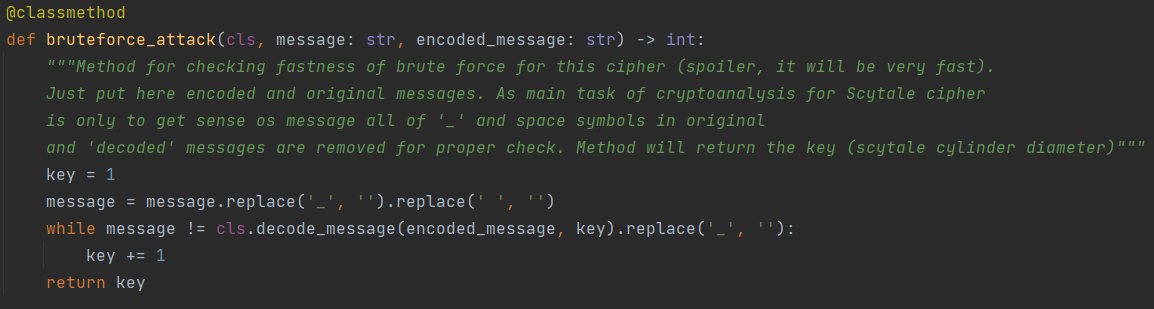
**Выполнение задания**Вариант 3 – шифр Скитала

**Задание 1**

Листинг

  
  
Результат работы  

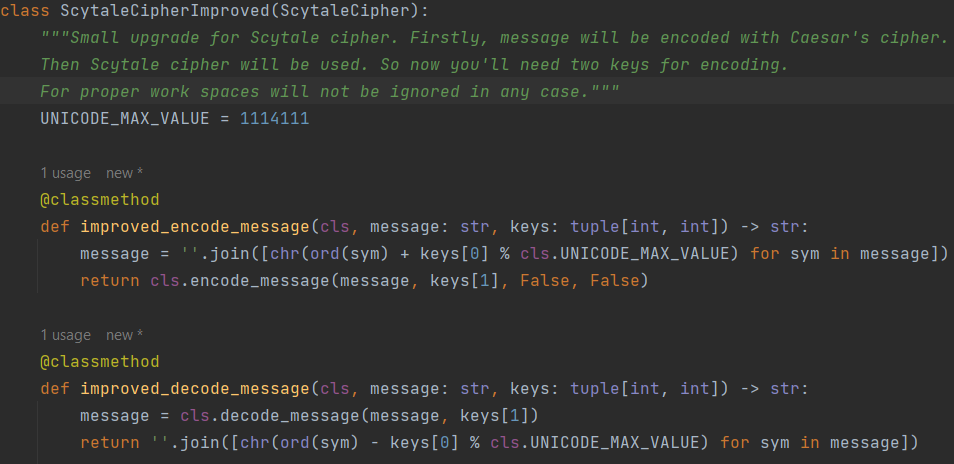

**Задание 2**

Листинг  


Результат работы (для сообщения из задания 1)  


**Задание 3**

Для улучшения стойкости шифра было предложено объединить шифр Скитала с шифром Цезаря: исходное сообщение сначала шифруется методом Цезаря, затем Скитала. Для шифрования требуется два ключа – один для метода Цезаря, второй для Скитала

Листинг  


Результат работы (для сообщения из Задания 1, ключами были числа 10 и 2)  


**Вывод**

В ходе лабораторной работы были реализованы программные средства шифрования и дешифрования текстов при помощи простейших шифров. Стоит отметить, что на данный момент ни один из этих шифров не является стойким, т.к. дешифрование сообщения, зашифрованного при помощи таких шифров, может быть произведено при помощи вычислительной техники за короткое время. Немного повысить стойкость поможет объединение нескольких шифров.