Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет Информационных технологий и управления

Кафедра Интеллектуальных информационных технологий

**ОТЧЁТ**

по дисциплине «Средства и методы защиты информации в интеллектуальных системах»

Лабораторная работа №2

Тема: Простейшие криптографические преобразования

Вариант: 21

Выполнил: Самута Д. В.

гр. 221703

Проверил: Крищенович В. А.

Минск 2024

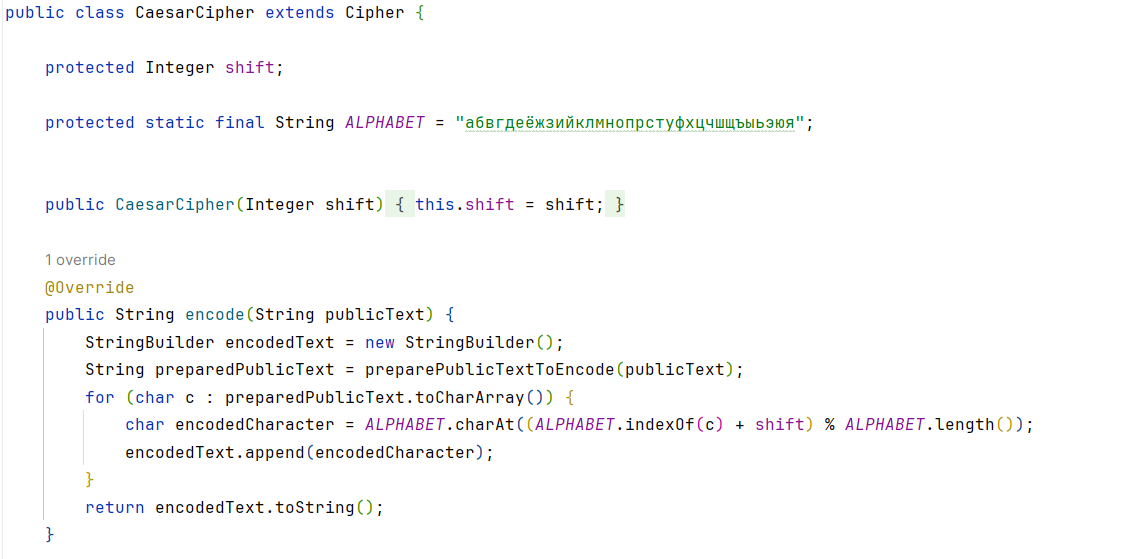
**Задача:** реализовать шифр Цезаря.

**Задание 1 :**

Реализовать в виде программы шифр (зашифрование и расшифрование)

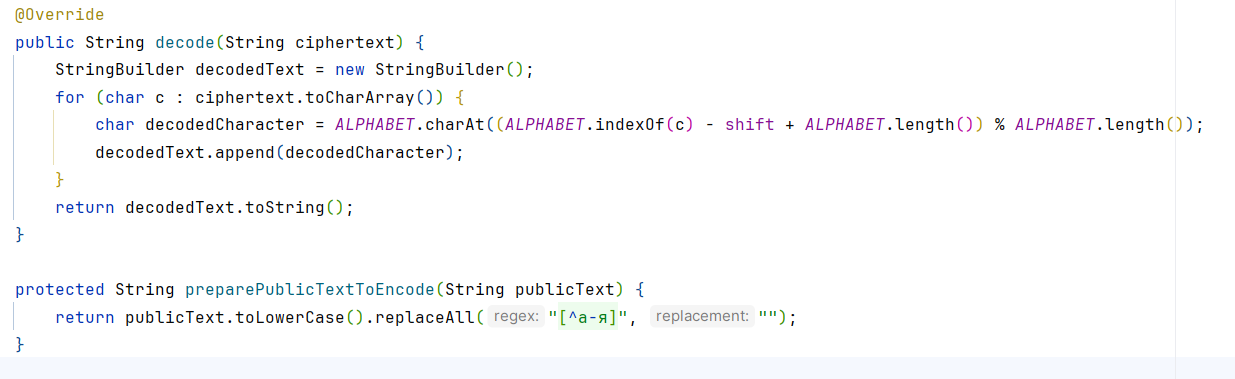
в соответствии с вариантом. Язык исходного текста русский или английский по

выбору исполнителя.



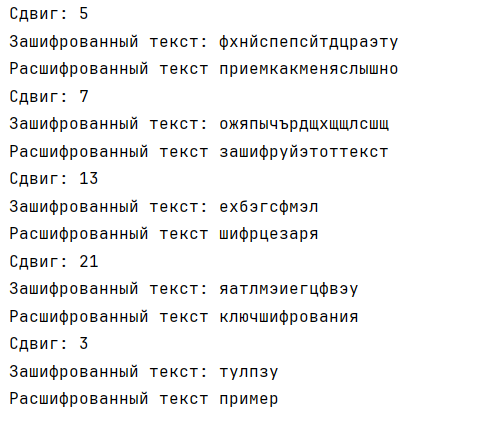
shift – сдвиг по алфавиту для реализации Шифра.

Метод encode принимает строку пользователя, преобразует ее в нормальную форму, т.е. удаляет знаки препинания, пробелы и др. Далее в цикле проходимся по строке, берем символ, определяем его индекс в афавите, прибавляем к этому индексу shift, берем остаток и берем из алфавите символ по полученному индексу.



Метод decode делает обратное действие аналогично.

Пример работы:

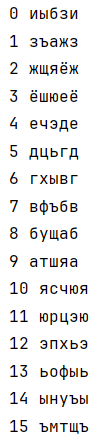
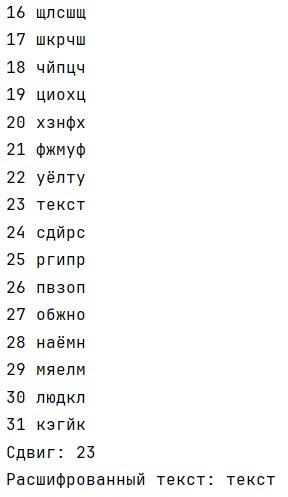


**Задание 2:**

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



Метод просто делает все сдвиги (в данном случае 31 сдвиг, т.к. алфавит русский).

**Задание 3:**

Криптографическая стойкость шифра Цезаря весьма низкая, и его можно легко взломать. Его недостатки:

1. Для русского алфавита он имеет всего лишь 30 ключей, потому что существует всего 30 сдвигов (сдвиг на 0 не считается).
2. Его можно взломать обычным методом перебора, причем это не займет много времени.
3. Шифр Цезаря сохраняет относительную частоту символов, то есть наиболее частые символы исходного текста останутся самыми частыми и в зашифрованном тексте, только сдвинутыми. Это делает шифр уязвимым для **частотного анализа**.

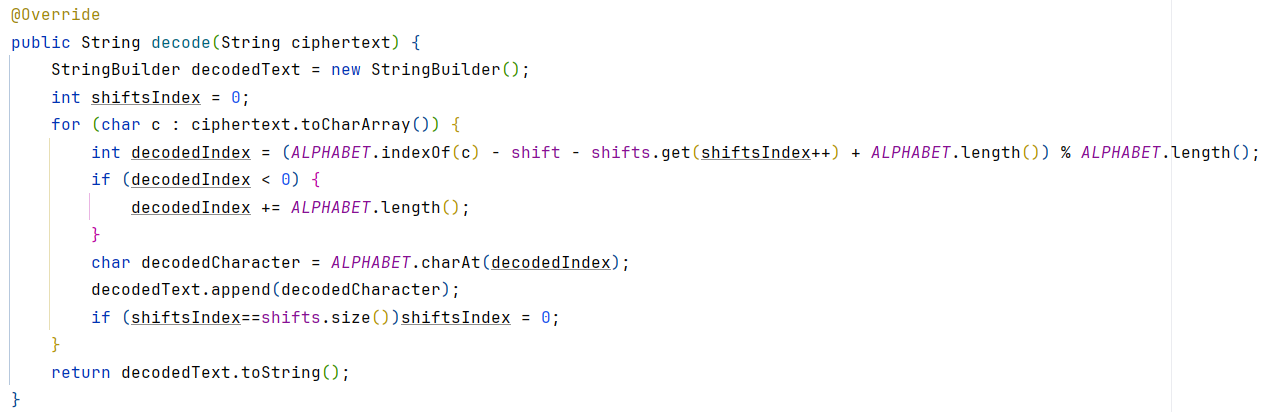
**Задание 4:**

Предложить варианты усложнения шифра. Предложенные варианты

оформить в виде алгоритма.

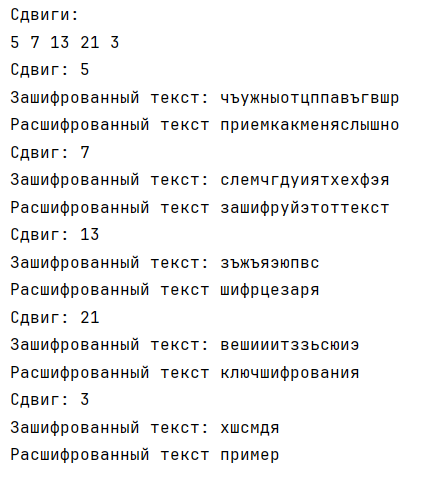


Теперь помимо обычно сдвига shift, передается еще и список сдвигов, элементы которого будут применяться для шифрования. Для первого символа берется первый элемент списка, для второго – второй элемент списка, если список закончился, то берется первый элемент, и далее также.



Расшифрование происходит аналогично.

Пример использования шифра:



Вывод: шифр Цезаря обладает **очень низкой криптографической стойкостью**. Он уязвим к простым атакам методом перебора и частотного анализа. В реальных условиях шифр может быть взломан практически мгновенно, поэтому он не подходит для защиты информации. Для того чтобы шифр было тяжело взломать нужно придерживаться правилам:

1. Использовать длинные и случайные ключи;
2. Решить проблему с относительной частотой символов;
3. Передавать ключи по защищенному каналу;
4. Не хранить ключи в открытом виде.