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 №1

Вариант 5

Выполнил: Воложинец А.А.

гр. 221703

Проверил: В.А. Крищенович

Минск 2024

**Условие:**

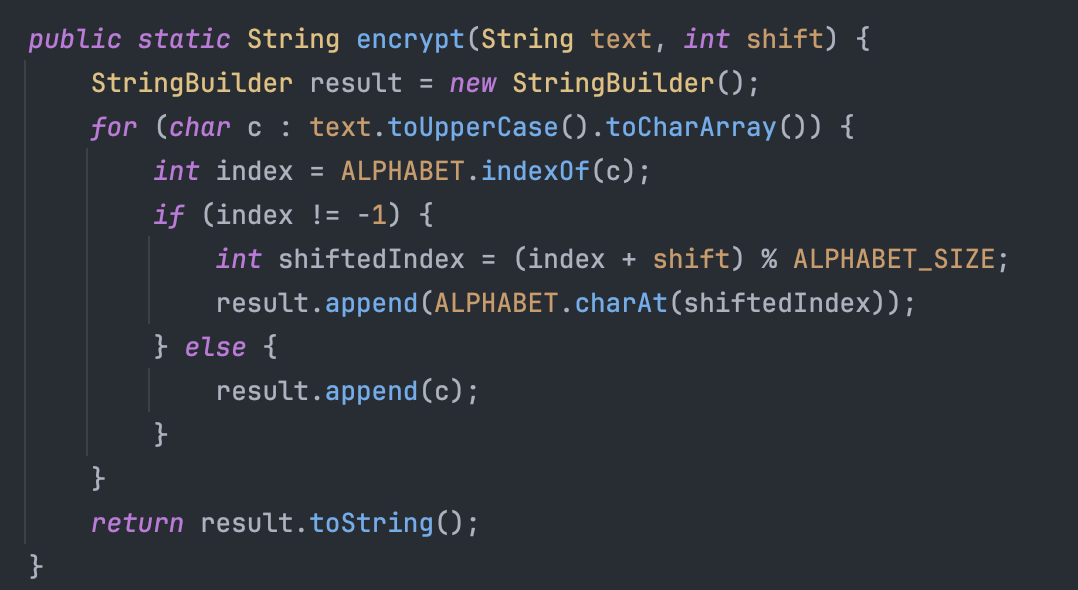
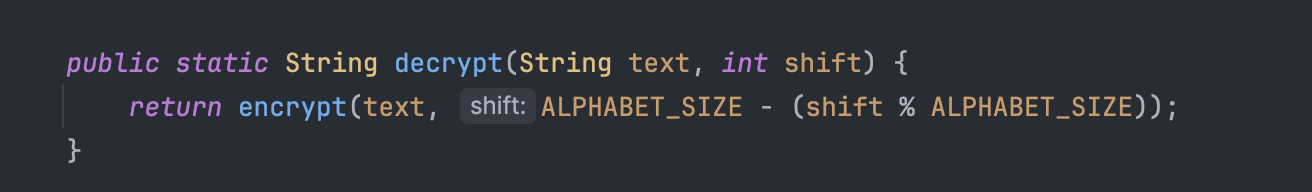
1) Реализовать в виде программы шифр Цезаря (зашифрование и расшифрование). Язык исходного текста русский.

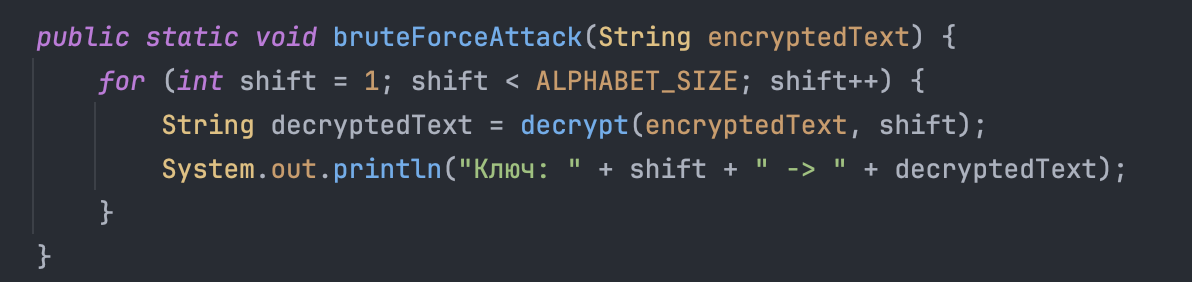
2) Реализовать в виде программы атаку полным перебором ключа, используя для оценки правильности выбора ключа визуальный метод или исходный текст для автоматического сравнения результата дешифрования.

3) Оценить криптографическую стойкость реализованного шифра.

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

**Реализация:**

* Шифровка
* Расшифровка
* Атака полным перебором



**Оценка криптографической стойкости шифра**

Шифр Цезаря является крайне слабым с точки зрения современной криптографии. Вот несколько ключевых моментов:

* **Малое количество ключей**. Для русского алфавита существует всего 33 возможных сдвига, что делает атаку полным перебором чрезвычайно простой и быстрой.
* **Отсутствие сложных математических операций**. Этот шифр не использует никаких математических принципов или сложных операций, что упрощает его взлом.
* **Статистическая атака**. Частотный анализ легко позволяет распознать шифрованный текст, так как частоты символов в естественном языке сохраняются после шифрования.

**Варианты усложнения шифра:**

1. **Множественные алфавиты**: Использовать несколько алфавитов для шифрования текста.
2. **Шифр Виженера**: Это расширение шифра Цезаря, в котором используются разные сдвиги для разных букв исходного текста.
3. **Зависимость от позиции символа**: Изменять сдвиг на основе позиции символа в строке.